送信ドメイン認証技術
導入マニュアル

第２版 2011年８月

迷惑メール対策推進協議会

目　次

第1章 はじめに

第1章　はじめに

1.1　メールの普及と送信者情報偽装の問題

現在のメールシステムは、その仕組みの簡便さによって、多くのコミュニケーションツールの基盤として広く普及しました。その仕組みの簡便さの一方で、送り手が誰であるかを確認する手段が備わっていなかったことにより、現在では、多くの問題が引き起こされています。例えば、第三者のメールアドレスを悪用した匿名の広告宣伝メールの送信行為や、実在するメールアドレスを騙って偽のウェブサイトへ誘導して個人情報などを搾取するフィッシングなどの犯罪行為などが頻繁に行われるようになっています。また、メールシステムでは、受け取ったメールが宛先不明など何らかの原因で配送できない場合には、送信元に対してエラーメールなどの通知文を送信する必要がありますが、これにより送信者情報を詐称された第三者へ大量の通知文が届く問題なども発生するようになっています。

1.2　送信ドメイン認証技術による対応

送信ドメイン認証技術は、受信者が受け取ったメールについて、送信者情報が詐称されているかどうかをドメイン単位で確認可能とする技術です。この技術により、送信者情報が詐称されることによって発生する問題の多くを解決できると期待されています。

送信ドメイン認証技術を利用するためには、メールの送信側と受信側のそれぞれで、新たな設定や機能の導入が必要となります。また、送信ドメイン認証技術には、その手法の違いにより、複数の方式が併存しています。さらに、メールの利用環境や利用局面の多様化により、技術的な課題以外にも、送信ドメイン認証技術を導入する際に考慮すべき事項があります。例えば、仕事に関連したメールを個人が契約した ISP（Internet Service Provider）の回線を利用して自宅から送信する場合に注意すべき点や、自社に関連したキャンペーン情報を顧客に大量送信するために外部の事業者に委託する場合に検討しておくべき点があります。また、メールシステム自体について、ISP など外部事業者のサービスを利用している場合や、専用システムであるものの運用を外部委託している場合など、利用環境の違いによって導入の方法が大きく異なる場合があります。

このため、送信ドメイン認証技術を利用する場合には、どの方式を利用すべきなのか、それぞれの方式にはどのような特徴があるのか、というような具体的な導入の手順や内容について理解することが必要になります。

1.3　本マニュアルの目的

本マニュアルは、主にメールシステムの管理者やメールの仕様の検討や導入を計画する立場にある企画担当者などを対象に、既にメールシステムの構造や概要についてある程度理解していることを前提として、送信ドメイン認証技術の導入にあたって必要な事項をまとめています。また、それらの事項に加え、

メールサービスを他組織へ提供している事業者にとって有益な情報も別にまとめています。

まず、電子メールの仕組みと課題について解説を行います（第２章）。続いて、送信ドメイン認証技術について、導入の前提となる知識を整理する目的で、技術部分の解説を行います（第３章）。次に、送信ドメイン認証技術の導入の手順について解説を行います（第４章）。さらに、他者にメールサービスを提供する事業者での追加的な注意事項について、ISPでの対応（第５章）、ホスティングサービスでの対応（第６章）、配信サービスでの対応（第７章）の順に解説を行います。最後に、利用者への周知一般について、解説を行います（第８章）。また、巻末に、参考情報や用語解説をつけています。

送信ドメイン認証技術は、あくまでドメイン単位で送信者情報が詐称されているかどうかを確認可能とする技術であって、これ自体で送受信されるメールが迷惑メールかどうかを判断できる訳ではありません。しかし、この技術の活用によりドメイン名の詐称ができなくなれば、ドメイン単位で受け取りたいメール、受け取る必要がないメールを決めておけば、それを確実に判断できるようになります。送信ドメイン認証技術が広く普及することにより、このような判断が可能なドメインが増え、それにより、迷惑メール自体も減少することが期待されます。本マニュアルがこのような流れに少しでも貢献できれば幸いです。

MEMO

第2章　メールの仕組みと課題

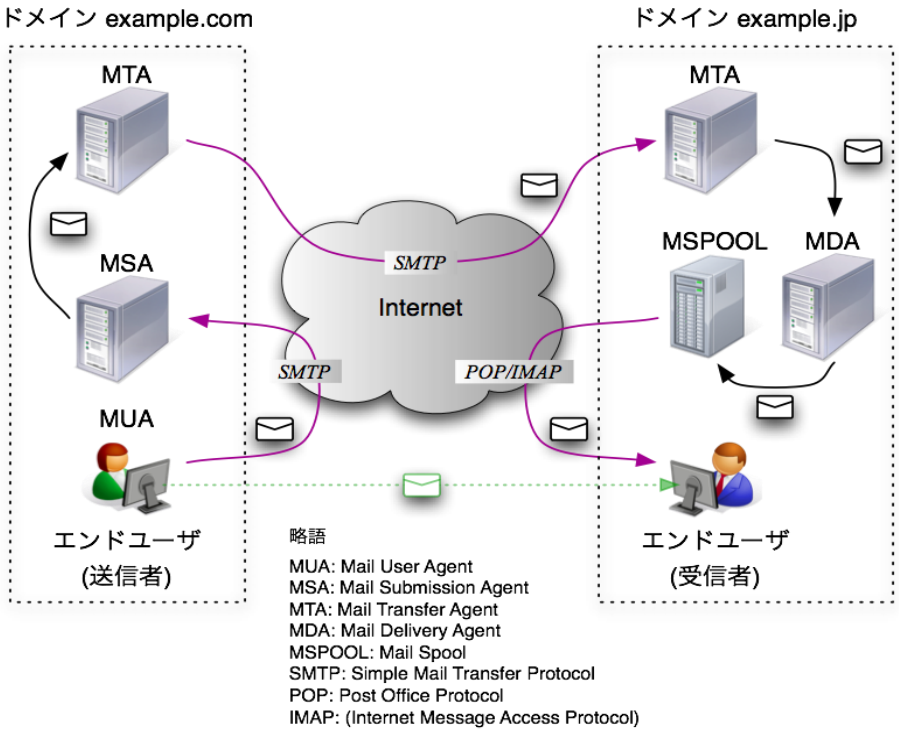
第2章　メールの仕組みと課題

本章では、送信したメールが受信者に届くまでの仕組みについて解説します。また、迷惑メールがなぜ受信者に届いてしまったり、受信側で迷惑メールを防ぐのが難しかったりする原因となっている、メール配送の課題についても解説します。

なお、ここでは、携帯電話で利用する SMS (Short Message Service) など宛先に電話番号を指定する方法ではない、PC で送受信するドメイン名を @（アットマーク）で区切るメールアドレスを宛先に指定するメールを対象とします。

2.1　メールシステムの概要

メールの送信者が作成したメールは、インターネット上の幾つかのサーバを経由して受信者に届けられます。図表２－１ に、example.com ドメインを利用している送信者が、example.jp ドメインを利用している受信者へメールが届けられるまでの流れを示します。



図表２－１　インターネットでのメール送信

図表２－１の説明

1　要素

Mail Transfer Agent　（MTA：メール転送エージェント）

メールを異なるメールシステム間で転送する役割を持ち、他の MTA や MSA と SMTP プロトコルなどを利用してメールの送受信を行う機能を提供します。

メールの宛先に応じて転送する先を振り分ける機能や、受信側のシステムで受信する準備ができていない場合などに一時的にメールを保存（キュー）する機能などを持ちます。

一般にサーバ・アプリケーション・プログラムとして実装されます（例： sendmail 、 Postfix 等）。

Mail User Agent　(MUA：メール・ユーザ・エージェント)

エンドユーザがメールを作成し、送信する（MSA にメールを投稿する）機能や、受信したメールをエンドユーザが読む（メール・スプールから読み出し、表示する）ための機能を提供します。

MUA から MSA へのメールの送信は、一般に SMTP プロトコルを利用して行われます。また、メール・スプールからの読み出しは、 Post Office Protocol 3 （POP 3） や Internet Message Access Protocol 4 （IMAP 4） プロトコルを利用して行われます。

一般的にエンドユーザの端末上で動作するアプリケーションとして実装され、メールクライアント、メールソフト等と呼ばれる場合が多いです（例：Microsoft 社の Outlook や Mozilla の Thunderbird 等）。

Mail Submission Agent　（MSA：メール・サブミッション（投稿）・エージェント）

エンドユーザにより作成されたメールを MUA などから受信し、メールの配送を開始する機能を提供します。

MTA の役割をもつサーバ･アプリケーション･プログラムが MSA を兼ねる場合もあります。MSA から MTA へ SMTP プロトコルを利用してメールを送信すると、 MTA は、次の配送先（他の MTA や MDA ）へメールを転送します。

Mail Delivery Agent　（MDA：メール・配送・エージェント）

メールの受信側（宛先）で、MTA からメールを受信し、メール・スプールへメールを保存する機能を提供します。

MTA の役割をもつサーバ・アプリケーション・プログラムが MDA を兼ねる場合もあります。

Mail Spool　（MSPOOL：メール・スプール）

メールの受信側（宛先）で、エンドユーザが MUA を利用してメールを読み取るためにメールを保存する機能を提供します。Mail Box と呼ぶ場合もあります。

2　処理

① ドメイン example.com のエンドユーザが、 MUA を利用してメールを作成
② エンドユーザは、 MUA を操作し、 MSA にアクセスしてメールを送信（投稿）
③ MSA は、受け取ったメールを MTA へ配送
④ MTA は、宛先ドメインの MTA を見つけ出して、その MTA へメールを配送
⑤ 受け取った宛先ドメインの MTA は、内部の MDA へメールを配送
⑥ MDA は、メール・スプールへメールを届け、メール・スプールでメールを格納
⑦ 宛先のエンドユーザは、MUA を利用してメール・スプールへアクセスし、自分宛のメールを読み出す

③④⑤のメールの配送では、複数の MTA を経由する可能性があります。最近では、アンチウィルスフィルタや迷惑メールフィルタなどを運用しているドメインも多く、そうしたフィルタを用いたフィルタリングは MTA で実施されている場合が多く、１つのドメインの内部であっても複数の MTA を経由してメールが配送されることが一般的になっています。

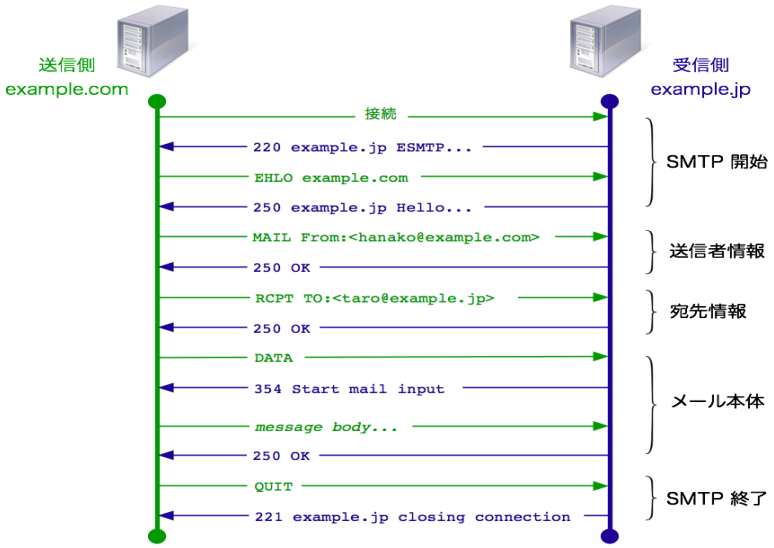
また、④で宛先ドメインの MTA を探すときに、送信元の MTA は、宛先ドメインの DNS 上の MX レコードを参照します。 MX レコードとして登録されているホストは、そのドメインにおいて外部ドメインからのメールを受信する役割をもつホストと解釈されます。

2.2　メール配送の手順

メールを宛先に届けるための配送手順として、SMTP（Simple Mail Transfer Protocol，RFC5321）が使われます。

メール配送では、メールを送りたい側（送信側）が、メールを届けたい先（受信側）にネットワーク的に接続を要求し、受信側が要求を受理することにより、一連の配送手続が開始されます。そして、実行したいコマンド名とその引数を相手方に送信し、相手方がそれに対する応答を返信するやりとりを繰り返すことにより手続が進みます。なお、メール送信は、送信側から受信側へ処理を伝えるので、ほとんどの場合、送信側が受信側に実行したいコマンドを送信することになります。

このときの接続の方法やメールの受け渡し、受信側からの応答の仕方などを決めたものがSMTP です。SMTP での手続の一般的な流れを図表２－２に示します。



図表２－２　SMTP によるメール通信手順

送信側では、処理の内容を示すコマンド（MAIL，RCPT，DATA など）を、引数とともに受信側に伝えます。例えば、MAIL FROM で送信者の情報（メールアドレス）を、RCPT TO で宛先の情報（メールアドレス）を、DATA でメール本体の情報を伝えます。

受信側では、それぞれのコマンドを解釈して応答をします。コマンドに対する応答の種別は、数字（220 や 250 などの３桁の数字）で示されます。例えばメールを受け取れない場合には、否定的な応答番号（500 番台の数字）を返すことになります。受信側は、このようなコマンドに対する応答という形で、受信側の判断や意図を送信側に伝えることができます。

SMTP の規格（RFC5321）では、送信側が指定する各コマンドの形式や順番、それぞれのコマンドに対して受信側が返すことができる応答番号の種類などが定められています。

こうしたメールの配送時に指定される、送信者や宛先のメールアドレスなどは、郵便の手紙になぞらえてエンベロープ（封筒）情報とも呼ばれます。

なお、SMTP は、メールサーバ間の配送時だけでなく、利用者がメールを作成する MUA（メール

ソフト）からメール投稿サーバ（MSA）への送信時にも使われます。

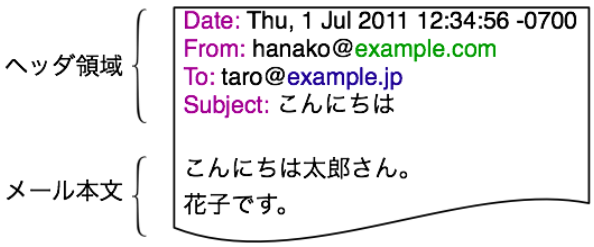
2.3　メール本体の構造

メール本体は、送信側が DATA コマンドを送信し、受信側がその応答として "354" を返した場合に、送信側から送信されます。メール本体の最後に、ドット ('.') 文字だけの行（ドット行）が送信されます。なお、この場合のドット行は、メール本体には含まれません。

メール本体は、ヘッダ領域とメール本文によって構成されます。いずれの領域もテキスト文字列で表現され、専用の区切り記号は決められていませんが、文字列の構成方法によって区別ができるように決められています。

ヘッダ領域は、メール本体の先頭からヘッダ行が連続する領域で、ヘッダ行ではない空行 (改行だけの行) がメール本文との区切りとなります。

メール本文は、ヘッダ領域の区切り(空行)から、メール本体の末尾までとなります。メール本体の例を図表２－３ に示します。



図表２－３　メール本体

ヘッダ行は、ヘッダ名と続くコロン（':'）、ヘッダ本文で構成されます。ヘッダ行はそれぞれ形式や構文が決まっており、ヘッダを追加する場合には、正しく構文に従って記述しなければなりません。

なお、メール本体の構造及びヘッダ行の構文については、SMTP の規格（RFC5321）とは別に、Internet Message Format（RFC5322, インターネットメッセージの形式）で決められています。

2.4　メールの送信者情報

2.4.1　概要

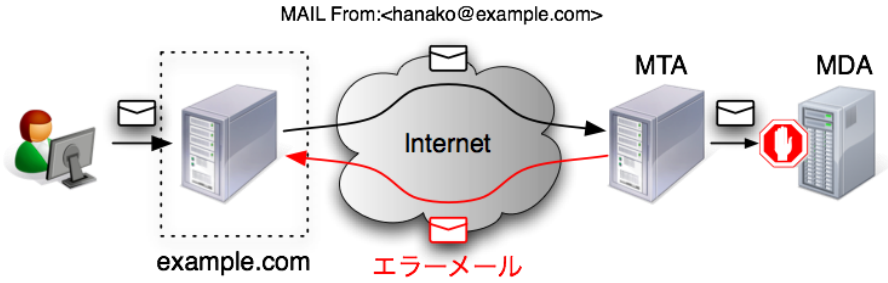
メールの作成者や送信者を示す情報には、メールの配送時に指定される送信者情報（エンベロープ情報に含まれる送信者情報）と、メール本体のヘッダ領域に記述される送信者情報の２種類があります。これらの送信者情報は、メールで利用される情報なので、いずれも、メールアドレスで示されます。

2.4.2　メール配送時に指定される送信者情報

メールの配送時に指定される送信者情報は、図表２－２ で示した MAIL コマンドの引数として指定されるメールアドレスです。このメールアドレスは、配送上で何か問題が発生した場合に送信者に通知を送る際に利用されます。そのため、リバースパス（reverse-path）という

名称が付いています。リバースパスは、SMTP によるメールの配送時に渡される情報なので、一般にはメールの受信者には渡されない情報になります。

なお、受信側の MTA は、この MAIL コマンドに対する応答として、メールを受け取らないことを示すエラーコードを返すことができます。例えば、指定されたメールアドレスが明らかに実在しないものであった場合や、過去に迷惑メールを送信してきた送信者であった場合などには、受け取らないことを応答コードで示すことができます。また、受信側の MTA が、一旦メールを受け取った後で、MDA (Mail Delivery Agent) 上でメールスプールに保存ができなかった場合や宛先が実際には存在しなかった場合など何らかの問題があった場合には、このリバースパス宛にエラーメールを送信することになります。



図表２－４　エラーメールの送信例

2.4.3　ヘッダ領域に記述される送信者情報

ヘッダは、メール本体の一部として受信者に届けられるため、受信者が見ることのできる情報です。しかし、ヘッダにはたくさんの種類があるために、受信者が利用する MUA (Mail User Agent, メールソフトウェア) の多くは、全てのヘッダを表示しません。送信者情報を示すヘッダの仕様としては図表２－５に掲げるものがありますが、MUA が送信者情報として表示する情報は、通常は From ヘッダになっています。

ヘッダ名	用途
Sender	メール送信を実際に行った送信者を示す情報
From	メールの作成者を示す情報
Reply-to	返事を送信する場合の宛先を示す情報

図表２－５　ヘッダ上の送信元アドレス

Sender ヘッダが最も良く使われるケースとしては、メーリングリストがあります。メーリングリストでは、リストへの投稿者が From ヘッダに示されます。しかし、リストメンバへの送信は、実際にはメーリングリスト機能を実現するプログラムなどが配送しています。そのため、Sender ヘッダにはメーリングリストの管理者などのメールアドレスが示されることになります。また、今ではあまり行われないかもしれませんが、例えば実際のメール内容の作成者に

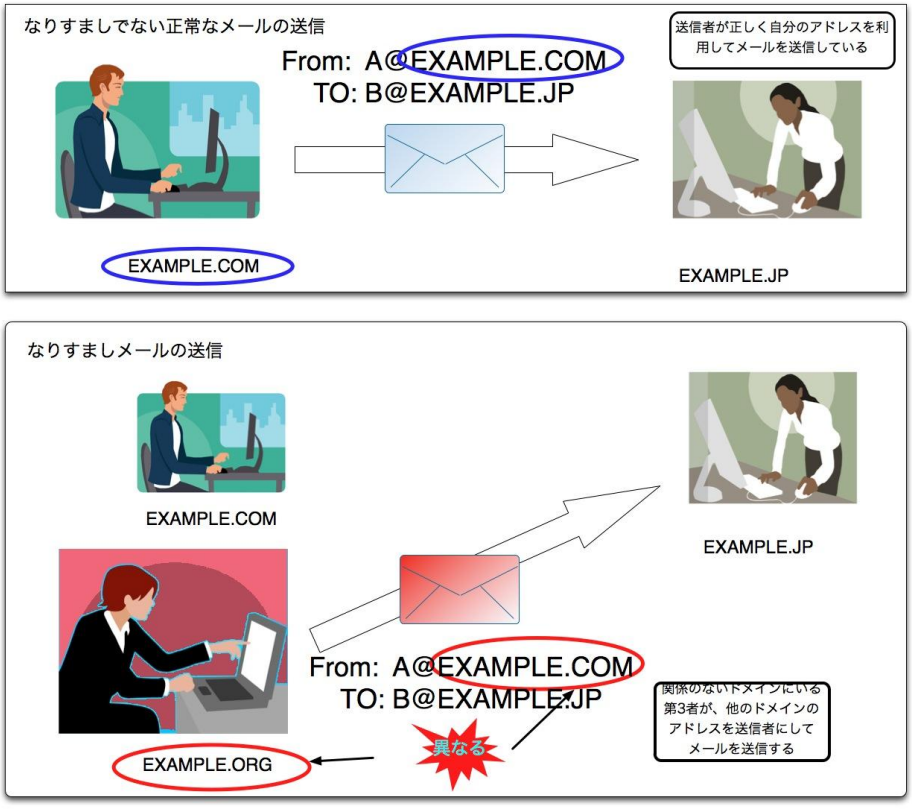
代わって秘書がメール送信するような場合に、送信者のメールアドレスを Sender ヘッダに示されることがあります。

From ヘッダの使われ方にも注意すべき点があります。From ヘッダには、メールアドレス以外にも、補助情報としてディスプレイネーム（display-name）を追加することができます。ディスプレイネームには、任意の文字列を使用できますので、From ヘッダ上に示されたメールアドレスと全く関係の無い名前や文字列が使えます。MUA や Web ブラウザでメールの送受信を行ういわゆるウェブメールシステムの多くは、送信者情報として、このディスプレイネームを優先して表示しますので、送信者情報として表示される文字列は、実際の送信者情報とは全く関係が無いかもしれないものとなっているのです。

2.5　送信者情報詐称の問題

2.5.1　送信者情報詐称を判断する仕組み

メールシステムにおける送信者情報には、2.4 でみたように、用途に応じた複数の種類があります。しかし、これまで、いずれの送信者情報についても、それが正しく名乗られているかを判断する仕組みがありませんでした。もともとの電子メールシステムは、インターネットが現在のような形で普及する以前から存在してきたシステムであり、メールの利用者が限られていた時代から少しずつ拡張されて使われて続けているために、現在のように送信者情報が詐称されることを予め想定していなかったためです。



図表２－６　なりすましメール送信例

そのため、これまで受信側では、経験的な運用方法として、例えば、送信者情報として、存在しないドメイン名が指定された場合や、日本の有名ドメインを名乗っているものの海外など明らかに異なった送信元からのメールだった場合に受信を拒否するなどの工夫をしてきました。

しかし、それらの場合であっても、ドメイン名を管理する DNS(Domain Name System) が単に不調であったり、海外からメール転送をしていたりする場合など、ごくまれに送信者情報を故意に偽装したものではない、正しい送信である場合があります。

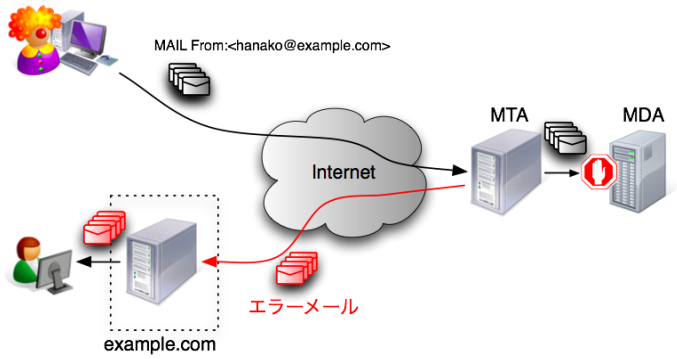
2.5.2　送信者情報詐称の問題点

メールの送信者情報が詐称されることによって、様々な問題が出てきています。

まず、受信側で、迷惑メールを受信しないために、送信者情報をもとに受信を拒絶しようとしても、詐称されていることにより、的確に受信の拒絶ができないことがあります。

また、実在する送信者を詐称し、実物とは異なる偽のウェブサイトに誘導し、個人情報を搾取するなどの犯罪行為（フィッシング）や、信頼性のある送信者を騙り、メールに添付された不正プログラムを実行させ、外部からコントロールされるボットにされたり、PC 内部にある個人情報や操作過程で得られる個人情報を搾取するなどの行為が行われています。

さらに、迷惑メールは宛先が存在するかどうかにかかわらず大量に送信される傾向にあるため、リバースパスを詐称し、実在するメールアドレスを指定している場合に、宛先が不明であることによるエラーメールが、詐称されたメールアドレスに宛てて大量に送信される、バックスキャッタ（backscatter）が大きな問題となってきています。その場合には、そのエラーメールが迷惑メールと判断され、迷惑メール判定機能を提供しているベンダやブラックリストを運営している組織に報告され、正しい処理としてエラーメールを送信している側（最初のメールの受信側）が、迷惑メール送信者として登録され、同じ出口から送信される通常メールまでもが、迷惑メール扱いされて届かなくなる、という 2 次的な問題も発生しています。



図表２－７　バックスキャッタ問題

2.5.3　送信ドメイン認証技術

このように、送信者情報が簡単に詐称できてしまい、それを受信側で簡単に判断することができない現在のメールの仕組みにより、大きな問題が生じています。これに対応するために、送信ドメイン認証技術が開発されており、その普及により、送信者情報詐称の問題点を防ぐことが可能になります。

第３章　送信ドメイン認証技術

第3章　送信ドメイン認証技術

本章では、送信ドメイン認証技術の基礎について解説します。送信ドメイン認証技術は、受信者が受け取ったメールについて、送信者情報が詐称されているかどうかをドメイン単位で確認可能とする技術です。

3.1　送信ドメイン認証技術による対応

送信ドメイン認証技術を利用すると、あるメールを受信したときにそのメールが、From ヘッダアドレスやリバースパスに示されているドメインから本当に送られてきたかどうかを確認することが可能になり、なりすましを見破ることができます。

送信ドメイン認証技術には、ネットワーク方式と電子署名方式という２つの異なる方式があります。

ネットワーク方式の送信ドメイン認証技術は、SMTP プロトコルにおいて、その送信元のホスト（MTA）の IP アドレスをもとにして認証します。この方式では、送信側で、後述するような手段で、自分のドメインで利用しているメールサーバ（MTA）の IP アドレスを公開します。ネットワーク方式の送信ドメイン認証には、Sender Policy Framework（SPF）と Sender ID という 2 つのインターネット標準があります。

電子署名方式の送信ドメイン認証技術は、公開鍵暗号技術を利用します。この方式では、送信側で、公開鍵暗号技術を用いて、公開鍵と秘密鍵を用意し、あらかじめ公開鍵を公開したうえで、秘密鍵を用いて送信するメールから電子署名を作成し、メールに付与した上で送信することで、受信側での電子署名の照合を可能にします。この方式には、Domain Keys Identified Mail（DKIM）という標準規格があります。

いずれの方式も既存のメールシステムの仕組みに大きな変更を加えなくても導入できるように考慮されています。

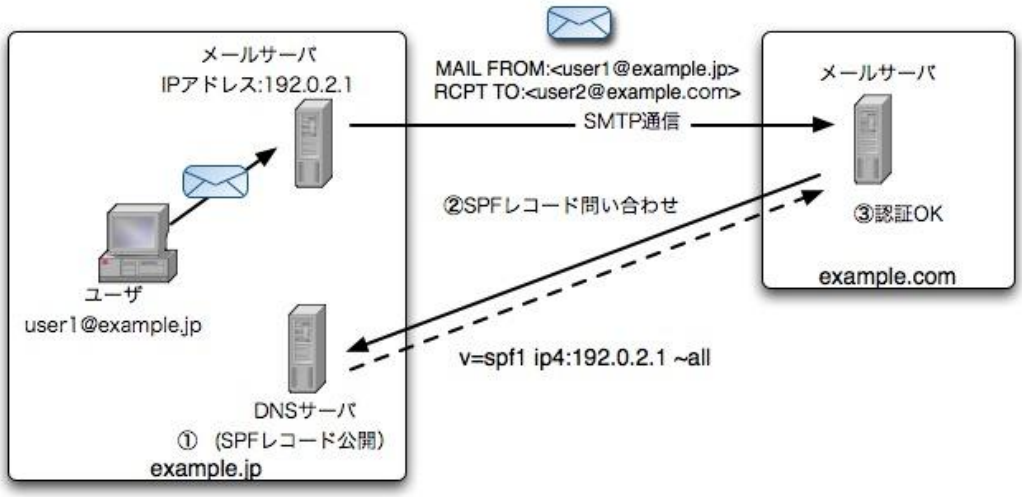
3.2　Sender Policy Framework (SPF)

3.2.1　概要

Sender Policy Framework （SPF）は、元 Pobox 社の Meng Wong 氏により提唱されたネットワーク方式の送信ドメイン認証技術です。SPF は、IETF の MARID WG 等において数々の議論と検討を経て、現在、実験的カテゴリの RFC（RFC4408） として標準化されています。SPF では、リバースパスを元に認証を行います。

3.2.2　SPF の仕組み

SPF の動作の概要を、図表２−４に示します。



図表３－１　SPF による認証の仕組み

送信側では、あらかじめ、自ドメインの DNS サーバ上に、自ドメインの送信者がメールを外部に向けて送出する可能性のあるメールサーバの IP アドレスの一覧を公開します（図表３－１の①）。これを「SPF レコード」と呼びます。

受信側では、メールの受信時に、送信者として指定されたリバースパスのドメイン部分に示されるドメインの DNS サーバより、SPF レコードを取得します（図表３－１の②）。そして、その SPF レコードに指定されている IP アドレスと、 SMTP で接続した先のメールサーバ（認証対象のメールサーバ）の IP アドレスが、一致するか確認することで、認証を実施します（図表３－１の③）。

3.2.3　送信側の設定

メールの送信側では、DNS 上で SPF レコードを公開するだけで SPF の運用を開始できます。RFC4408 では、SPF レコードは、DNS の TXT レコードか SPF RR レコード（以下「SPF 資源レコード」といいます。）として公開することが定められています。た

だし、現時点では、SPF という新しい RR レコード（以下「資源レコード」といいます。）を取り扱えないリゾルバや DNS サーバの実装が存在するため、SPF 資源レコードと TXT レコードの両方を利用して公開します。なお、SPF レコードは、SPF 資源レコードと TXT レコードとの両方を同時に公開可能ですが、SPF 資源レコードが存在する場合には、受信側で、SPF 資源レコードのみを参照すべきとされています。

SPF レコードには、当該ドメインに属するメールアドレスを送信者として、そのドメイン外にメールを送信する可能性のあるメールサーバ（MTA）の、外向けの IP アドレスのリストを記述します。

SPF では、IPv6 を含む IP アドレスを直接記述するほか、簡略に公開可能にする記述法が提供されています。SPF レコードの簡単な例を、図表３－２に示します。

```
例１）　a. example.com.　　IN TXT　"v=spf1 -all"
例２）　b. example.com.　　IN TXT　"v=spf1 +ip4:192.0.2.1 -all"
例３）　b. example.com.　　IN SPF　"v=spf1 +ip4:192.0.2.1 -all"
```

図表３－２　SPF レコード記述例

１つめの例は、a. example.com をドメイン名として持つアドレス（例えば user@a. example.com ）からは、一切メールを送信しないことを意味するものです。

２つめの例は、b. example.com をドメイン名として持つメールアドレス（例えば、user@b.example.com ）からのメールは 192.0.2.1 の IP アドレスを持つホストからのみ送信されるという意味を持ちます。

３つめの例は、SPF 資源レコードとして公開した場合です。

記述方法の詳細は、3.2.4 で解説します。

3.2.4　SPF レコードの記述法

SPF レコードは、最初にバージョンを記述し、空白（半角スペース）を入れて、定義を記述します。定義は、空白（半角スペース）で区切り、複数記述できます。

```
バージョン　空白　定義　空白　定義　・　・　（以下繰り返し）
```

図表３－３　定義

3.2.4.1　バージョン

バージョン（Version）は、その SPF レコードが、SPF のどのバージョンの文法にしたがって記述されているかを示します。

RFC4408 で定義されている SPF レコー

ドの文法はバージョン１のみであり、”v=spf1” と記述することとされています。それ以外の記述（例えば、”v=spf1.0” 等）をすると、その SPF レコードは不正なものとして、受信側で、無視されることになります。

重要な点は、RFC で定められた文法に従わない、誤った SPF レコードを記述すると、受信側ではその SPF レコードを無効として扱うということです（具体的には、3.5.3.2 で解説する ”permerror” として扱われることになります。）。したがって、記述は慎重に行い、公開に際して SPF レコードの記述について試験を行えるサイトなどを利用して試験を行うことなどにより、記述ミスがないことを確認するべきです。

3.2.4.2　定義

定義（terms）は、ディレクティブ（directive）と修飾子（modifier）で構成します。

ディレクティブは、限定子（qualifier）と機構（mechanism）で構成します。

図表３－２の例 2 では、"-all" と "+ip4:192.0.2.1" がディレクティブです。 "-all" のうち、"-" が限定子で、"all"が機構です。また、"+ip4:192.0.2.1" のうち、"+" が限定子で、"ip4:192.0.2.1" が機構です。

修飾子の例としては、"redirect=a.com" 等があります。

受信側での認証の処理では、定義は左から右へと評価します。認証対象のメールサーバの IP アドレスに対して最初にマッチした定義の限定子によって認証結果が決定されます。いずれの定義にもマッチしない場合は、“neutral“ と評価されます（“neutral“ については、3.5.3.2 で解説します。）。

定義　＝　ディレクティブ（directive）（限定子（qualifier）＋機構（mechanism））＋修飾子（modifier）

図表３－４　定義

(a)　限定子

限定子（qualifier）には、認証対象のメールサーバの IP アドレスが、それに続く機構にマッチした場合の認証結果を指定します（図表３－４を参照）。

限定子には、”+” 、”-” 、”~” 、”?” があり、”+” 限定子は省略可能です。それぞれについての認証結果とその意味を、図表３－５に示します。

表記	認証結果	意味
+	pass	当該ドメインの送信メールサーバとして認証する
-	fail	当該ドメインの送信メールサーバとして認証しない
~	softfail	当該ドメインの送信メールサーバとして認証しないが、正当なメールであっても認証失敗する可能性もある
?	neutral	認証されたかどうかを判断されたくない

図表３－５　限定子

(b)　機構

機構（mechanism）には、認証対象のメールサーバの IP アドレスと照合する条件を記述します。機構には、”all”、”include”、”a”、”mx” などがあります。機構の種類と、それぞれの引数及び機能を、図表３－６に示します。

機構	引数	機能
all	なし	・　すべての IP アドレスにマッチする。 ・　SPF レコードの末尾におかれ、デフォルトの動作を定義するために利用される。
include	ドメイン名	・　引数に与えられたドメインの SPF レコードを使って認証処理を実施する。 ・　その結果が pass、temperror 又は permerror の場合にのみ値が採用される。すなわち、include に指定された先のドメインの SPF レコードによって fail の判定が与えられても、それが認証結果としては採用されない。
a	ドメイン名	・　認証対象のメールサーバの IP アドレスが、ドメイン名に与えられた FQDN の A レコードのいずれかであれば、マッチする。
mx	ドメイン名	・　認証対象のメールサーバの IP アドレスが、ドメイン名に対応する MX レコードに指定されているホストの A レコードのいずれかであれば、マッチする。 ・　MX は複数与えられる場合があるが、10 個までの MX ホストに対して検査する。
ptr	ドメイン名	・　認証対象のメールサーバの IP アドレスをリバースルックアップし、得られたホスト名でさらに正引きを実施して IP アドレスを得て、その IP アドレス（複数の IP アドレスが得られる場合がある）が送信元ホストの IP アドレスを含む場合でかつ、リバースルックアップによって得られたホスト名が ptr の引数に与えられたドメイン名と一致するかそのサブドメインである場合に、マッチする。 ・　リバースルックアップに失敗した場合は fail とみなす。負荷の多い処理となるため、あまり利用は推奨されない。
ip4	IP ネットワークアドレス（CIDR 表記可能）又は IP アドレス	・　そのドメインのメールを送信する可能性のあるメールサーバの IP ネットワークアドレス又は IP アドレスを引数に指定する。 ・　認証対象のメールサーバの IP アドレスが、指定された IP ネットワークに含まれているか、IP アドレスに合致する場合に、マッチする。
ip6	IPv6 ネットワークアドレス又は IPv6 アドレス	・　そのドメインのメールを送信する可能性のあるメールサーバの IPv6 ネットワークアドレス又は IPv6 アドレスを引数に指定する。 ・　認証対象のメールサーバの IP アドレスが、IPv6 ネットワークに含まれているか、IPv6 アドレスに合致する場合に、マッチする。
exists	ドメイン名	・　引数であるドメイン名に指定された表記で A レコードのルックアップを実施し、該当の A レコードが存在すればマッチする。 ・　SPF のマクロ機能とあわせての利用を想定する。

図表３－６　機構

(c)　修飾子

修飾子（modifier）は認証についての付加的な情報を与えるものです。機構とは異なり、直接、認証結果を与えませんが、redirect のように認証結果に影響を与えるものもあります。修飾子について、図表３－７に示します。

修飾子	引数	機能
redirect	ドメイン名	・　引数であるドメイン名に指定されたドメインの SPF レコードにより認証処理を実行する。 ・　複数のドメインが１つの SPF 定義を共有するような場合での使用を想定する。 ・　この修飾子を利用する場合には、SPF レコードの末尾に配置することを推奨する。
exp	ドメイン名	・　認証が失敗した場合に、引数であるドメイン名に指定されたドメインの TXT に設定されている文字列を、認証失敗した理由や説明等として利用する。 ・　SMTP セッションでのエラーメッセージなどでの利用を想定する。

図表３－７　修飾子

3.2.4.3　SPF レコード公開時の制限

RFC4408 では、SPF レコードの文字列は DNS 上の制約から 512 オクテットに収まるようにすべきであり、また、UDP を用いた DNS 問合せに対応するためには 480 文字より少なくすべきであることが示されています。また、DNS サーバの負荷や受信側の認証処理を軽減する意味もあり、一度の認証処理で参照する DNS の回数の上限を 10 回に制限しています。

3.2.4.4　認証結果の扱い

認証結果については、3.5 で解説します。

3.3　Sender ID

3.3.1　概要

Sender ID はネットワーク方式の送信ドメイン認証技術です。Microsoft 社が提唱した Caller ID for E-mail と SPF を統合する形で策定されました。Sender ID の仕様は、 SPF の RFC（RFC4408）と同じく実験的カテゴリの RFC（RFC4406 と RFC4407）として、標準化されています。

Sender ID は、SPF の影響を強く受けており、送信側では、SPF （RFC4408）で定義されている SPF レコードを利用して認証情報を公開できます。さらに、 Sender ID 独自で拡張した宣言書式もあります。

SPF と Sender ID の大きな違いは、 SPF がリバースパスを対象に認証するのに対して、Sender ID では、ヘッダ上の送信者アドレスを対象に認証することもできます。実際に受信者が見るヘッダ上のアドレスを検査することで、フィッシィング対策としての効果を強める狙いがあります。

また、複数の送信ヘッダ（Purported Responsible Address。以下「PRA」といいます。）を利用することで、転送時の問題を回避できます。RFC4407 は、この PRA の扱いを定義した RFC です。ヘッダに対して認証処理をするため、SMTP での通信上では、メール本文の内容をある程度読み込んだ上でないと認証が行えません。したがって、MAIL コマンドを受信した段階で認証結果が得られる SPF に比べて、受信側では、運用時に、ややシステム負荷が高くなる場合があります。

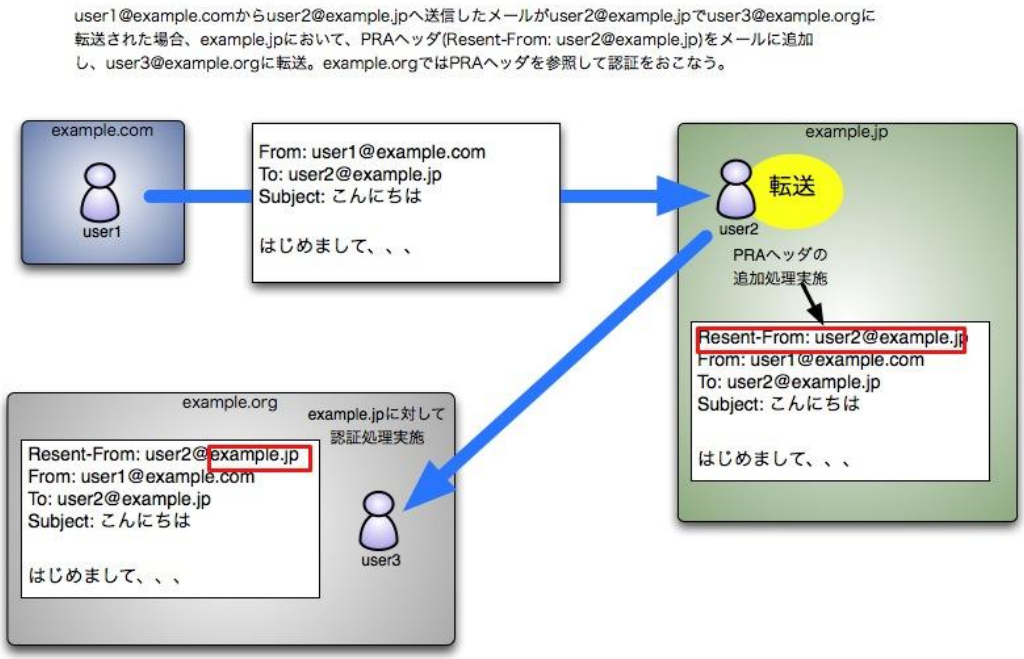
3.3.2　Puported Resposible Adress(PRA)

前述のように、Sender ID では、ヘッダ上の送信者アドレスから送信元のドメインを判断します。このとき、送信者を表す複数のヘッダを利用することで、転送時の問題を回避するように考えられています。一般に、メールの送信者を表すヘッダは ”From” ですが、PRA では、それだけでなく、”Resent-Sender”、”Resent-From”、”Sender”、”From” の各ヘッダについても、この順に優先度が高い者として参照します。図表３－８にそれぞれのヘッダの概要を示します。

ヘッダ	概要
Resent-Sender:	メールを転送したり、メーリングリストで再送する際に、転送等をしようとした者の代理でその転送等を実際に行った者（Resent-From と Resent-Sender が同じアドレスになる場合は Resent-Sender は付与しない）
Resent-From:	メールを転送したり、メーリングリストで再送する際に、その転送等を行った者
Sender:	メールの送信処理者（メールの送信者の代わりにメールの送信処理を実際に行った者）
From:	メールの送信者（メールを実際に作成した者）

図表３－８　PRA（Purported Responsible Address）

なお、メールを転送するときや、メーリングリストで再送するときには、図表３－９で示すように、その転送等を実施するメールボックスにひもづくアドレスを Resent-From ヘッダで指定します。



図表３－９　転送時のＰＲＡ追加

認証時には、まず、Resent-Sender ヘッダが存在する場合には、それを利用して認証を行います。Resent-Sender ヘッダが存在しない場合には、次に、Resent-From ヘッダを探し、存在すれば、それを利用して認証します。Resent-From ヘッダもない場合は、次に、Sender ヘッダ、さらにそれもなければ、From ヘッダという順番で対象を変えます。From ヘッダが複数存在する場合は認証処理に失敗します。

このようにすることで、たとえ、メールの配送時に転送等が行われて、From ヘッダでの認証ができなくても、転送時に、Sender ヘッダや Resent-From ヘッダ、Resent-Sender ヘッダなどのヘッダを追加されていれば、受信側で認証を行うことができます。RFC5322 では再送時には、再送フィールドを入れるべきと記載されており、また、再送ヘッダを入れる場合は、Resent-From を利用するとしているので、メールを再送する場合、Resent-From ヘッダを付与するべきです。なお、直接は関係ありませんが、Resent-From ヘッダを付与した場合は、Resent-Date と再送信時間を付与しなければなりません。

3.3.3　SPF レコードのバージョン

Sender ID では、 SPF で定義されている SPF レコードを spf1 （バージョン 1）とし

て扱い、Sender ID の SPF レコードを spf2.0 （バージョン 2.0）として扱います。

spf2.0 の SPF レコードでは、From ヘッダのアドレスを含む PRA を認証対象とするか、リバースパスを認証対象とするか、またその両方を対象とするかを、 SPF レコード上で指定できます。具体的には、レコードの先頭のバージョンの表記である ”spf2.0” につづけて、認証対象のスコープを記述します。PRA を対象として認証する場合は ”spf2.0/pra” と、リバースパスを指定する場合は ”spf2.0/mfrom” と、両方を対象とする場合は ”spf2.0/mfrom,pra” と記述します。

spf1 のレコードしか公開していないサイトからのメールについても Sender ID では認証対象としており、その場合、リバースパスと PRA を対象として認証します（ ”spf2.0/mfrom,pra” と宣言されているとみなすことになります）。

また、1 つのドメインで、spf1 と spf2.0 の２つの SPF レコードを同時公開できます。

図表３－10 は、spf2.0 と spf1 の SPF レコードの例です。バージョンの記述方法が微妙に異なるので、公開するときは間違えないように気をつけることが必要です。

```
(spf2.0)
   example.org.          IN        TXT       "spf2.0/pra include:example.org -all"

(spf1)
   example.org.          IN        TXT       "v=spf1 include:example.org -all"
```

図表３－１０　spf2.0 と spf1 の SPF レコードの例

3.4　Domainkeys Identified Mail (DKIM)

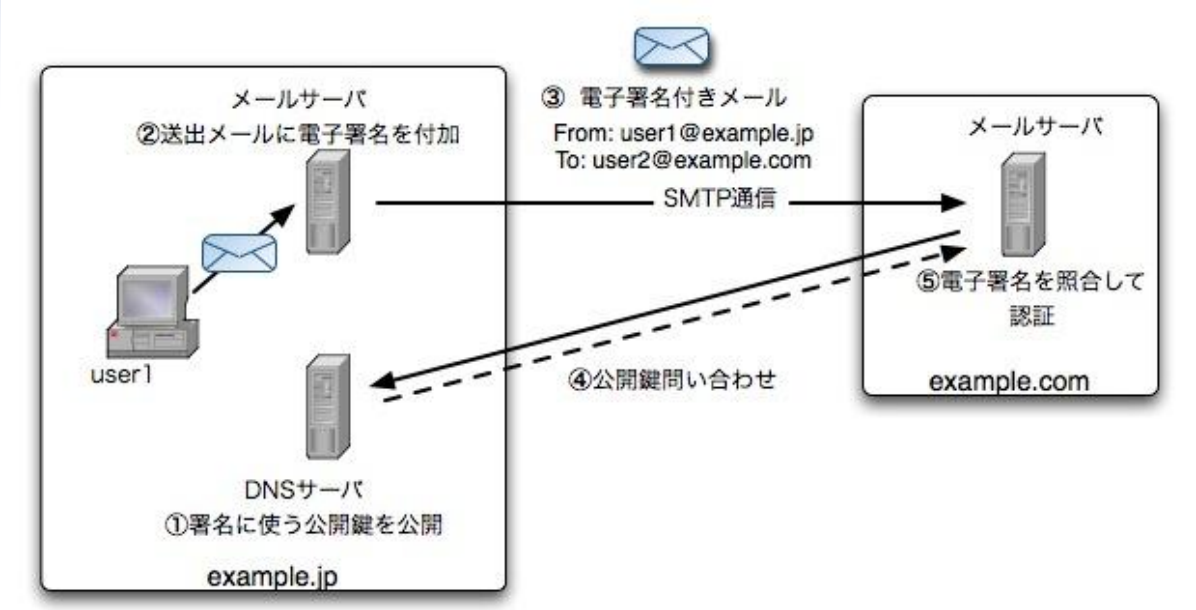
3.4.1　概要

Domainkeys Identified Mail (DKIM) は、電子署名方式の送信ドメイン認証技術です。IETF において、Sendmail 社の Eric Allman 氏等を中心として検討が進められ、RFC4871 及び RFC5672 として標準化されました。さらに、DKIM の標準を補うものとして DKIM-ADSP という標準があり、RFC5617 で標準化されています。

図表３−11 に示すように、DKIM では、送信側でメールから電子署名を作成して付与し、受信側でその電子署名を検証するという方法で送信者のドメインの認証を行います。メール本体（ヘッダ及びメール本文の内容）をもとに電子署名を作成するので、中継メールサーバ（MTA）などで何らかの理由で電子署名又は電子署名の元になったメール本体のデータが変更されなければ、たとえメールが転送されても、転送先で認証が可能です。

図表３−11 では、次のような手順で DKIM 送信ドメイン認証を実施しています。

① example.jp ではあらかじめ DNS に電子署名に使う公開鍵を公開しておく
② example.jp のメールサーバでは送出メールの本文とヘッダを元に電子署名を付与する
③ メールを example.com のサーバに SMTP で送信する
④ example.com のメールサーバは DKIM-Signature の d パラメータに指定されたドメイン部である example.jp の DNS へ公開鍵を問い合わせる
⑤ example.jp から取得した公開鍵により電子署名を照合して OK であれば認証成功



図表３－１１　DKIM による送信ドメイン認証

3.4.2　公開鍵の提供

DKIM では、送信側のドメインの DNS 上に、電子署名の作成に利用した秘密鍵に対応する公開鍵を公開します。公開鍵は、FQDN に対する TXT レコードとして DNS に登録します。

鍵の長さは、512bit から 2048bit までがサポートされています。RFC では 2048bit より大きな鍵を利用する場合もあるとされていますが、同時に、実際には DNS の UDP パケットサイズの 512 バイトにうまく収まる最も長い鍵として 2048bit までが現実的であると説明されています。なお、1024bit より短い鍵では、オフラインでの解読行為に対して脆弱です。

公開鍵を登録する FQDN 及びレコードの例を、図表３－12 に示します。

```
<セレクタ>._domainkey.<ドメイン名>　<タグ>=<値>
例：　sls.dkim._domainkey.smtest.com. 300 IN TXT　　"v=DKIM1; k=rsa; t=y;p=MIGfMA0GCSqGSIb3...<省略>"
```

図表３－１２　公開鍵を登録する FQDN 及びレコードの例

＜セレクタ＞は、3.4.3 で解説する DKIM-Signature ヘッダの s タグに指定したラベルになります。＜ドメイン名＞は、DKIM-Signature ヘッダの d タグに指定されたドメイン名になります。

異なるセレクタを用意することで、同じドメインに対して複数の公開鍵を運用できます。

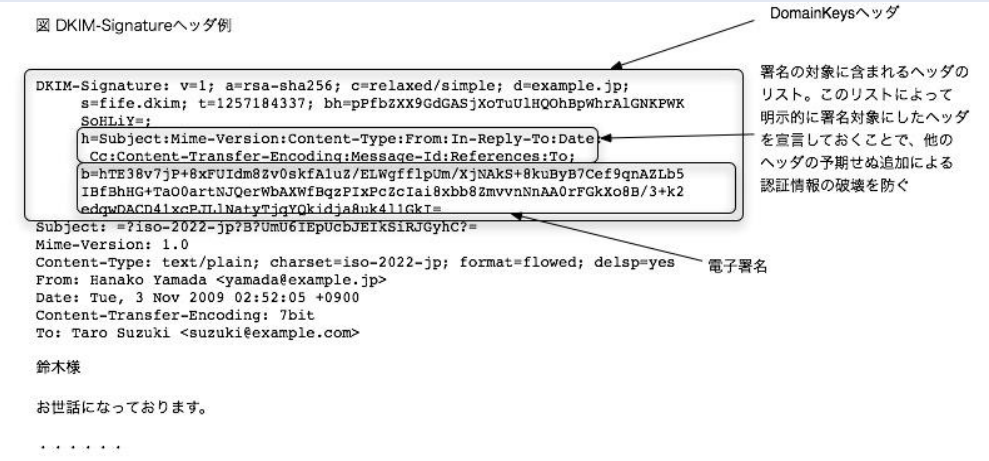
公開鍵のレコードは、「タグ＝値」を ; で列挙することになります。利用できるタグを、図表３－13 に示します。

タグ	値	説明	省略の可否
v	Key レコードのバージョン番号	・　指定する場合は、「DKIM1」になる。省略した場合も、「DKIM1」になる。 ・　指定する場合は、レコードの最初に記述する。	設定することが推奨されるが省略可能
g	鍵の適用条件パターン	・　電子署名の対象とするメールのメールアドレスのローカルパートにマッチする条件パターン。 ・　ワイルドカード文字「*」が利用できる。 ・　この鍵を利用できる送信者のメールアドレスを限定する場合に利用する。省略時は「*」になる。	省略可能
h	利用可能なハッシュ方式	・　電子署名の作成の際に利用できるハッシュ方式を限定する。省略した場合には、すべてのハッシュ方式を許容する。 ・　電子署名の作成者と照合者の両方が sha256 方式をサポートする必要がある。また、照合者は sha1 もサポートする必要がある。	省略可能
k	鍵の形式	・　電子署名の作成の際に利用できる鍵の形式を指定する。省略した場合には、「rsa」になる。	省略可能
n	説明	・　可読な説明文を保持するタグ。省略した場合には、無（長さ０の文字列）になる。	省略可能
p	公開鍵データ	・　公開鍵のデータを保持するタグ。鍵データは base64 でエンコードする。 ・　値が指定されない場合は、該当の鍵が無効になっていることを示す。	必須
s	サービスタイプ	・　当該鍵が有効であるサービスを指定する。 ・　カンマで区切って複数指定できる。現時点で指定できるサービスは、「*」（すべてのサービス）と「email」（電子メール）の２つがある。省略した場合には、「*」となる。	省略可能
t	フラグ	・　フラグを指定する。 ・　「:」で区切って複数指定できる。 ・　指定できるフラグには、「y」と「s」がある。「y」は DKIM の運用が試験モードであることを示す。「y」フラグがある場合は、受信者は認証に成功したメールとそうでないメールを区別して処理してはいけない。「s」が指定されている場合は、i= に指定されたアドレスの @ から右のドメイン名は d= に指定された値と一致する必要がある。省略した場合には、フラグなしとなる。	省略可能

図表３－１３　レコードに利用できるタグ

3.4.3　送信側での電子署名の作成

送信側では、メール本体（ヘッダ及びメール本文の内容）をもとに電子署名を作成します。作成した電子署名を、DKIM-Signature ヘッダとして付与します。DKIM-Signature ヘッダの書式は、「タグ=値」の組を ; で区切って列挙します。DKIM-Signature ヘッダの例を、図表３－14 に示します。また、利用できるタグを、図表３－15 に示します。



図表3－14　DKIM-Signature ヘッダ例

タグ	値	説明	省略の可否
v	バージョン	・　バージョン番号を示す。 ・　現時点では、「1」と指定する。	必須
a	電子署名の作成に利用したアルゴリズム	・　電子署名の作成に利用したアルゴリズムを指定する。 ・　「rsa-sha1」と「rsa-sha256」が利用できる。	必須
b	電子署名データ	・　電子署名データ。base64 にエンコードして指定する。	必須
bh	本体のハッシュ値	・　電子署名の対象とした本体のハッシュ値。	必須
c	メール本文とヘッダの正規化方式	・　電子署名の作成に利用する正規化処理の方法を指定する。「/」で区切って、それぞれメール本文正規化に利用したアルゴリズムを表示する。 ・　「simple」と「relaxe」が指定できる。省略した場合には、「simple/simple」になる	省略可
d	ドメイン名	・　電子署名の作成を行ったドメイン名、すなわち、送信ドメイン名を指定する。公開鍵の取得の際に参照するドメイン名の一部になる。 ・　後述の i タグに与えられるアドレスのドメイン名は、このタグに与えられる値と同じか、又は、サブドメインであることが必要である	必須
h	電子署名の対象としたヘッダ	・　電子署名を作成するデータに含まれたヘッダ。: で区切って複数列挙できる。 ・　送信者を示すヘッダである From や Sender などは、必ず電子署名の対象に含めることが必要である。	必須
i	認証対象送信者アドレス	・　メールの送信者や送信プログラム（メーリングリストなどの場合）のメールアドレス。省略した場合には、 d タグに指定したドメイン名の先頭に @ を追加した値になる。	省略可
l	電子署名の対象とした本文の長さ	・　電子署名の作成を行ったメール本文の先頭からの文字長（バイト長）。省略した場合は、メール本文すべてを電子署名の対象とする。	省略可
q	公開鍵取得方法	・　公開鍵を取得する方法を指定する。現時点では「dns/txt」のみ指定可能。省略した場合には、「dns/txt」となる。	省略可
s	セレクタ	・　公開鍵を取得する際に、クエリを発行する対象のドメイン名の一部に利用する。 ・　複数のセレクタを持つことで、１つのドメインで複数の公開鍵を利用できる。	必須
t	電子署名実施時のタイムスタンプ	・　電子署名を作成した日付を EPOC（1970 年からの秒数）で指定する。省略時は未定義となる。	利用推奨（省略可）
x	有効期限	・　電子署名の有効期限について、有効である日時を EPOC（1970 年からの秒数）で指定する。省略した場合は、無期限になる。	利用推奨（省略可）
z	電子署名の対象としたヘッダのコピー	・　電子署名の対象にしたヘッダの電子署名の作成時の値を保持する。「｜」記号で、複数の指定が可能である。 ・　デバッグ目的であり、認証処理には利用しない。	省略可

図表3－15　DKIM のタグの概要

送信側は、次の手順で電子署名を作成し、DKIM-Signature ヘッダをメールに追加します。

1. 電子署名を作成する対象となるメールか確認する
2. 電子署名を作成する対象となるヘッダを決定し、h タグに列挙する
3. メール本文の内容から l タグに指定した長さを取り出し、正規化処理を実施する
4. ヘッダ、正規化したメール本文の内容、これから追加する DKIM-Signature ヘッダの電子署名のデータを除いた部分をつなげたデータに対して、ハッシュを作成する
5. ハッシュに対して電子署名を作成し、DKIM-Signature ヘッダとして付与したのち、DKIM-Signature 自体をヘッダに追加する

3.4.4　受信側での処理

受信側では、メールに付与された DKIM-Signature ヘッダを取り出し、次の手順で電子署名の検証を行います。

1. DKIM-Signature ヘッダの d タグ、 s タグの値から、公開鍵を取得する FQDN を作成する
2. 公開鍵を取得する。このとき、 i タグに設定してあるメールアドレスのローカルパートが DKIM レコードの g タグの条件パターンにあわない場合は、電子署名の照合を行わない
3. h タグに記述してあるヘッダと、メール本文の内容（ l タグで有効な本文の長さが指定してある場合は、先頭からその長さだけを切り出したもの）及び電子署名データ以外の DKIM-Signature ヘッダの値を併せてハッシュを作成する
4. 公開鍵を利用して、DKIM-Signature ヘッダの電子署名データからハッシュを取り出す（復号する）
5. 電子署名から取り出した（復号した）ハッシュと、受信したメールから作成したハッシュを比較して、同じであれば認証成功

3.4.5　認証結果の扱い

DKIM では、認証する対象の送信ドメインは、メールの From ヘッダから取り出すのではなく、DKIM-Signature ヘッダに指定されているドメインや送信アドレスを対象に認証します。このため、ヘッダ上の送信者である From 行の値と、認証に利用したドメイン名が異なる場合が存在します。DKIM の RFC においては、認証結果に対するメールの扱いについてははっきりと定義されておらず、DKIM-ADSP の RFC において説明されています。

DKIM-ADSP については 3.4.6 で、認証結果の詳細については 3.5 で解説します。

3.4.6　DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)

3.4.6.1　概要

Author Domain Signing Practices（ADSP）とは、 DKIM の認証結果をどのように扱うべきかを示すポリシーを送信側で公開するものです。

3.4.5 で解説したように、DKIM では、メールの DKIM-Signature ヘッダから認証対象のドメインを取り出しますので、From ヘッダに指定されている送信者アドレスのドメインと、電子署名を作成したドメインが異なる場合があります。

まず、DKIM-ADSP では、これを図表３－16 のように整理しています。

分類	原文	意味
認証成功した電子署名	Valid Signature	DKIM の電子署名の認証処理に成功した電子署名（DKIM-Signature ヘッダ）
メール作成者アドレス	Author Address	メールの From ヘッダに指定されている送信者アドレス
メール作成者ドメイン	Author Domain	メール作成者アドレスのドメイン部分
メール作成者ドメイン電子署名	Author Domain Signature	照合が成功した電子署名で、かつ、DKIM-Signature ヘッダの d タグに指定したドメインとメール作成者ドメインが同一である電子署名

図表３－１６　DKIM-ADSP で追加された署名およびメール作成者の整理

DKIM-ADSP では、メール作成者ドメイン電子署名として認証できれば、そのメールの送信ドメインは認証された（pass）と判定します。認証に成功した電子署名がないメール、検証した電子署名のドメインがメール作成者ドメインと異なる場合などにおいて ADSP レコードを参照する必要があります。

3.4.6.2　ADSP レコードの公開

ADSP も DNS 上に TXT レコードで公開します。公開に利用する FQDN は

_adsp._domainkey.<ドメイン名>

となります。

<ドメイン名> は、From ヘッダのアドレスのドメイン名部分となります。電子署名の検証に使う公開鍵を DKIM-Signature ヘッダの d タグや i タグをもとに読み出すのに対して、ADSP は、ヘッダ上の送信ドメインから取り出す点が相違していますので、注意が必要です。

ADSP は、”dkim=値” で記述します。値には、図表３－17 に示すものがあります。

値	概要
all	このドメインから送信されるメールは、すべてメール作成者ドメイン電子署名が与えられる。
unknown	このドメインから送信されるメールのいくつか又はすべてに、メール作成者ドメイン電子署名が得られる。
discardable	このドメインから送信されるメールは、すべてメール作成者ドメイン電子署名が与えられる。そして、もしメール作成者ドメイン電子署名が得られない場合は、受信者はそのメールを破棄することが望まれる。

図表３－１７　DKIM-ADSP の値

3.4.6.3　DKIM-ADSP 利用上の注意点

メール作成者ドメイン電子署名以外のケースの場合、特にメーリングリストに投稿したメールの場合の扱いなどについては、現在も検討中となっており、特に送信側で ADSP レコードを公開する場合には、注意が必要です。

また、受信側では、認証に成功した場合（メール作成者ドメイン電子署名で認証に成功した場合）のみの結果を利用し、それ以外の場合は、その結果だけでなりすましメールであると判断しないようにすることが必要です。

3.5　認証結果のヘッダへの表示

3.5.1　Authentication-Results

送信ドメイン認証技術による認証の結果を該当のメールのヘッダに記録する場合の方法は、RFC5451 で標準化されています。

RFC5451 では、認証結果を記録するヘッダとして、Authentication-Results ヘッダを利用するよう定義されています。

Authentication-Results ヘッダを利用して記録した例を、図表３－18 に示します。

```
Authentication-Results: smtp.example.co.jp;
dkim=pass (1024-bit key) header.i=user@example.com; spf=pass (example.co.jp: domain of user@example.com designates 192.0.2.1 as permitted sender) smtp.mail=user@example.com
```

図表３－１８　Authentication-Results ヘッダを利用して記録した例

3.5.2　ヘッダの詐称

Authentication-Results ヘッダには、認証を実施したメールサーバの ID も同時に記録します。

また、このヘッダの詐称を防ぐために、まったく関係のない外部のドメインから、内部の ID が認証を実施したメールサーバとしてヘッダに記録されたメールを受信した場合には、そのヘッダを削除することが必要です。

3.5.3　認証方法ごとの結果表示

3.5.3.1　概要

１つの Authentication-Results ヘッダで、複数の種類の認証方式による認証の結果を表示できます。図表３－18 の例では、dkim と spf の結果が表示されています。

Authentication-results ヘッダの表示の方法を、図表３－19 に示します。１つの認証方法による認証の結果は、１つの「認証結果情報」に表示します。「認証結果情報」は、「認証結果」、「理由」及び「プロパティ情報」で指定します。

```
Authentication-Results: 認証実施ホスト ID;バージョン; 認証結果情報; 認証結果情報;・・・

※　バージョンは、省略可能
※　認証結果情報は、認証結果 理由 プロパティ情報 が指定されます。
　－　理由は、省略可能
　－　プロパティ情報は、指定されないか、１つ以上指定される場合があります。
```

図表３－１９　Authentication-results ヘッダの表示の方法

「認証結果」は、認証処理の結果を表示するもので、「認証方式ラベル=認証結果の値」で表示されます。「認証方式ラベル」として指定される認証方法の概要を図表３-20 に示します。

認証方法	説明
iprev	RFC5451 にて定義されている接続ホストの IP アドレスの逆引きに基づく認証方法
auth	SMTP 認証 (SMTP AUTH)
dkim	DKIM 送信ドメイン認証
dkim-adsp	DKIM-ADSP 送信ドメイン認証
domainkeys	DomainKeys 送信ドメイン認証
sender-id	Sender ID 送信ドメイン認証
spf	SPF 送信ドメイン認証

図表３－２０　認証結果一覧

「プロパティ情報」では、認証対象が何であったかを表示することが可能です。表示する場合には、認証対象が何であったかを示す認証対象タグと、その実際の値を組として、認証対象タグ=認証対象の値の形で表します。複数の認証方式の結果を表示する場合は、”;”（コロン）で区切って並べます。認証方式ラベルと認証対象タグとして指定されるものを、図表３－21 に示します。

認証方式	認証対象タグ	意味
dkim	header.i	DKIM 認証において i= タグに指定された送信者を元に認証を行った
	header.d	DKIM 認証において d= タグに指定された送信者を元に認証を行った
dkim-adsp	header.from	DKIM-ADSP 認証処理において From ヘッダを元に認証を行った
sender-id	header.ヘッダ名	Sender ID の認証において、表示されたヘッダ名のヘッダに対して認証行った
spf	smtp.mailfrom	SPF 認証においてエンベロープの送信者に対して認証した
	smtp.helo	SPF 認証において HELO コマンドの引数のホスト名を元に認証した

図表３－２１　プロパティ情報一覧

3.5.3.2　SPF 及び Sender ID での結果表示

Authentication-Results ヘッダでは、SPF 及び Sender ID での認証結果の値には、図表３－22 で示すように、”none”、”neutral”、”pass”、”policy”、”hardfail”、”softfail”、”temperror”、”permerror” があります。

値	意味
none	SPF レコードが宣言されていない
neutral	送信元のドメインでは、該当のホストが認証できたかできないかを明らかにしない
pass	認証に成功した
policy	認証は成功したがローカルなポリシーによってその認証結果は受け入れられない
hardfail	認証が失敗した
softfail	認証は失敗であるが、はっきりと認証失敗としては扱ってほしくない
temperror	一時的な問題で認証処理を実行できなかった
permerror	SPF レコードの文法的な誤りなど永続的なエラーで認証処理を実行できなかった

図表３－２２　SPF での認証結果の値

”none” は、SPF レコードが公開されていないため、認証できなかった場合です。この場合、送信ドメイン認証では、送信元についての評価が下せないため、従来どおりスパムフィルタを通すなどしてメールの扱いを決定します。結果が none だった場合には、メールを即座に受信拒否すべきではありません。

”neutral” は、送信ドメインの SPF レコードが、例えば「v=spf1 ?all」のように定義されている場合や、

「v=spf1 +ip4:xxx.xxx.xxx.xxx ?all」

のようにレコードの末尾が「?all」と定義されていて、先立つほかの条件にマッチせず「?all」にマッチした場合です。 RFC には、neutral は none と同じように扱うべきであるとされています。また、softfail よりは正当性が高いものとして扱う可能性があるとも説明されています。結果が neutral だった場合には、メールを即座に受信拒否すべきではありません。

”pass” は、送信元の IP アドレスが SPF レコードにマッチし、認証に成功した場合です。送信ドメインは正当であるので、あとはその送信ドメインの評価に従ってメールを処理します。

“hardfail“ は、SPF レコードが公開されているが、送信元の IP アドレスが「-」クオリファイヤの条件にマッチする場合です。「?all」や「~all」が末尾に設定されている SPF レコードを持つ送信ドメインのメールに対しては、この結果は発生しません。なお、RFC では、「all」の記述が省略された SPF レコードに対して、どの条件にもマッチしない場合は ”neutral” になるとされています。

”softfail” は、SPF レコードが公開されており、送信元の IP アドレスが「~」クオリファイヤの条件にマッチする場合です。RFC では、”fail” と ”neutral” の中間くらいの扱いをすべきであるとされています。結果が ”softfail” である場合には、メールを即座に受信拒否すべきではありません。

”temperror” は、一時的な障害で認証処理が失敗した場合です。対応としてはメールを一時エラー（4XX）で受信拒否するか、そのまま受信することになります。受信した場合は、少し厳しく扱うべきです。

”permerror” は、SPF レコードは公開されているが、SPF レコードの記述に誤りがある場合などです。この結果であっても、永続的な受信拒否をすべきではありません。

3.5.3.3　DKIM での結果表示

DKIM 認証の結果と後述の DKIM-ADSP 認証の結果は、それぞれ別のものとして扱われます。

DKIM での認証結果の値には、図表３－23で示すように、”none”、”neutral”、”pass”、”policy”、” fail”、”temperror”、”permerror” があります。

値	意味
none	メールに DKIM の電子署名が付与されていない
neutral	メールは DKIM の電子署名が付与されていたが、DKIM の電子署名の文法上の誤りなどで、照合処理できなかった
pass	メールに DKIM の電子署名が付与されており、その電子署名は受信者にとって受け入れられるものであり、かつ、電子署名の照合が成功した
policy	メッセージには DKIM の署名が付与されていたが、ローカルなポリシーによってその電子署名は受け入れられない
fail	メールに DKIM の電子署名が付与されており、その電子署名は受信者にとって受け入れられるものであるが、電子署名の照合が失敗し、認証が失敗した
temperror	一時的な問題で認証処理を実行できなかった
permerror	照合に必要なヘッダが存在しない場合など永続的なエラーで認証処理を実行できなかった

図表３－２３　DKIM での認証結果の値

3.5.3.4　DKIM-ADSP での結果表示

DKIM-ADSP での認証結果の値には、図表３－24 で示すように、”none”、”unknown”、”pass”、”discard”、”nxdomain”、” fail”、”temperror”、”permerror” があります。

なお、前述の DKIM 認証の結果はそれぞれ別のものとして扱われます。

値	意味
none	DKIM-ADSP レコードが公開されていない。
unknown	メールにはメール作成者ドメイン電子署名が付与されておらず、かつ、DKIM-ADSP レコードに unknown が公開されている場合
pass	メールが DKIM 電子署名を付与されており、電子署名の照合が成功し、かつ、それがメール作成者ドメイン電子署名である場合
discard	メールにはメール作成者ドメイン電子署名が付与されておらず、かつ、DKIM-ADSP レコードに discardable が公開されている場合
nxdomain	メッセージにはメール作成者ドメイン電子署名が付与されておらず、かつ、メール作成者ドメインが DNS 上に存在しない場合
fail	メールはメール作成者ドメイン電子署名が付与されておらず、かつ、DKIM-ADSP レコードに all が公開されている場合
temperror	一時的な問題で認証処理を実行できなかった
permerror	照合に必要なヘッダが存在しない場合など永続的なエラーで認証処理を実行できなかった。

図表３－２４　DKIM-ADSP での認証結果の値

第4章　送信ドメイン認証技術導入手順

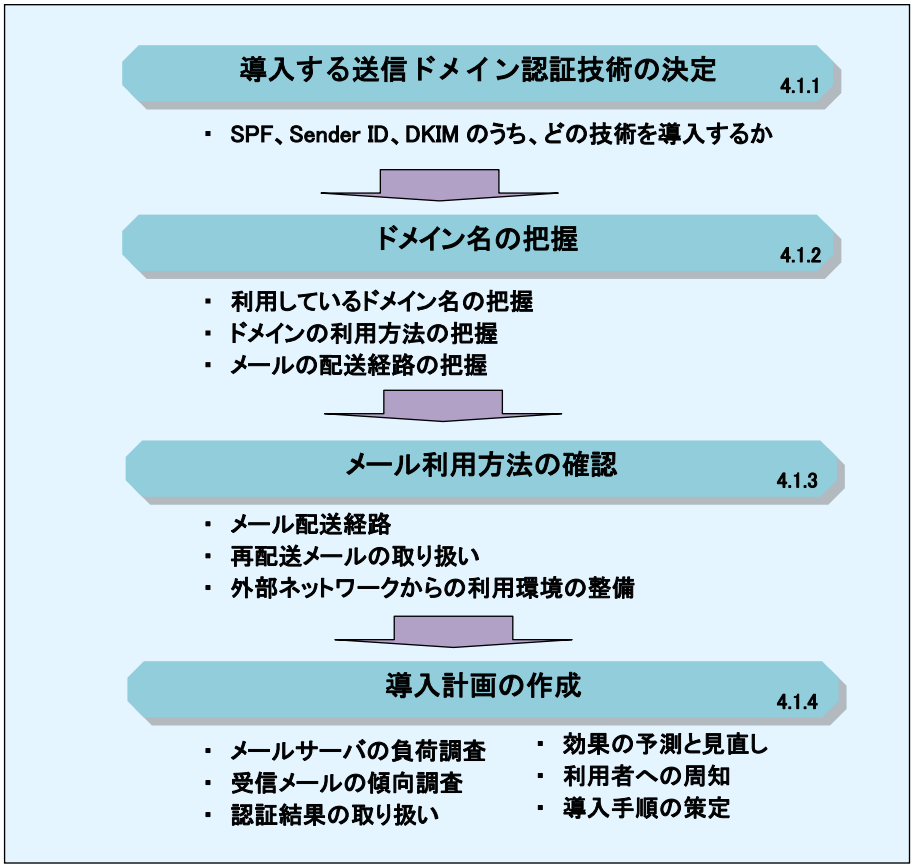
第４章　送信ドメイン認証技術導入手順

送信ドメイン認証技術は、メールの送信側と受信側の双方が協調することによって成り立っています。送信ドメイン認証技術は、既存のメール配送の仕組み (SMTP) に直接影響を与えることなく下位互換的に導入することができますので、メールの送信側と受信側のどちらの立場からでも導入することができます。

本章では、送信ドメイン認証技術の導入に際し、事前に検討しておくべきことや、それぞれの送信ドメイン認証技術について、送信側と受信側のそれぞれの側での実際の作業内容、導入後の運用にあたり注意すべき点などについて解説します。

4.1　事前準備

送信ドメイン認証技術の導入に際し、予め検討しておくべき事項がいくつか存在します。どの技術を導入すべきか、送信側と受信側のどちらから導入すべきか、導入の時期をどう判断するか、という基本的な検討のほか、 送信ドメイン認証技術を正しく機能させるためのメールの運用部分についても検討が必要です。



図表４－１　事前準備

例えば、メール送信側として、送信ドメイン認証技術を導入したにもかかわらず、それが正しく運用されなければ、送信者情報を偽装していないにもかかわらず認証が失敗するようなメールが流通してしまう可能性があります。そのようなメールが多くなれば、そのドメイン名自体の信用も失われてしまう可能性があります。

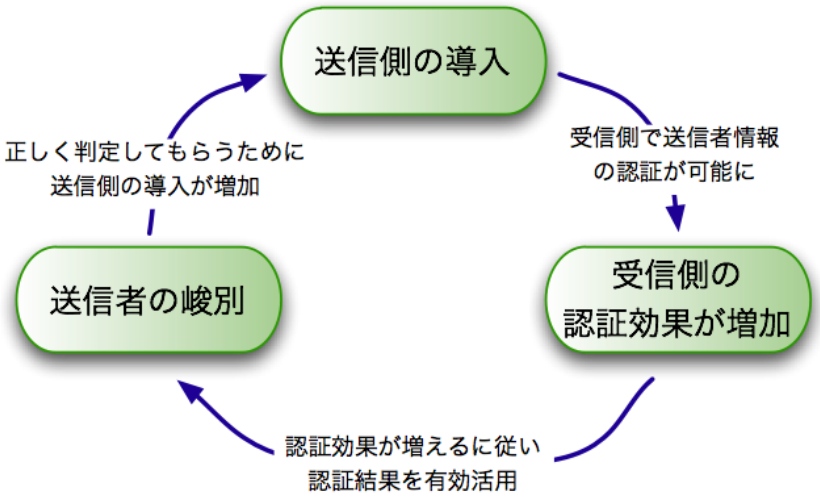
また、メールの受信側では、送信ドメイン認証技術を利用することにより得られた認証結果をどのように利用すべきなのかを考える必要があります。そのためには、実際のメールの配送形態でどのような認証結果が得られる可能性があるのかを正しく理解し、これらメール配送の事情に合わせた検討が予め必要になります。

以下では、送信ドメイン認証技術の導入にあたり、事前に検討すべき内容について具体的に解説するとともに、それらが送信ドメイン認証技術において、どのような意味があるのかについて補足して説明します。

4.1.1　導入する送信ドメイン認証技術の決定

前述のとおり、送信ドメイン認証技術では、メールの送信側と受信側の双方が導入することによって、はじめて認証が可能になるため、送送側と受信側の双方での導入が同程度進むことが望ましいものです。

導入のための費用は導入する技術によって差があり、技術によっては送信側ではほとんど費用がかかりませんが、いずれの技術でも、受信側での導入には受信時に認証するという新たな機能の追加が必要になるので、新たに費用か発生することになります。そのため、まず送信側の導入を増やすことによって、受信側での認証可能なメールの割合を高め、導入効果が得られやすい環境を作ることが普及を進めていくために必要となります。



図表４－２ 普及のサイクル

送信ドメイン認証技術のうち、送信側の導入費用が低い技術は、ドメインを管理するDNS 上に、導入時に SPF レコードを記述すればメールの送信ごとの処理が不要なSPF/SenderID です。そのため、導入費用の低さからも、まず SPF/SenderID の送信側の

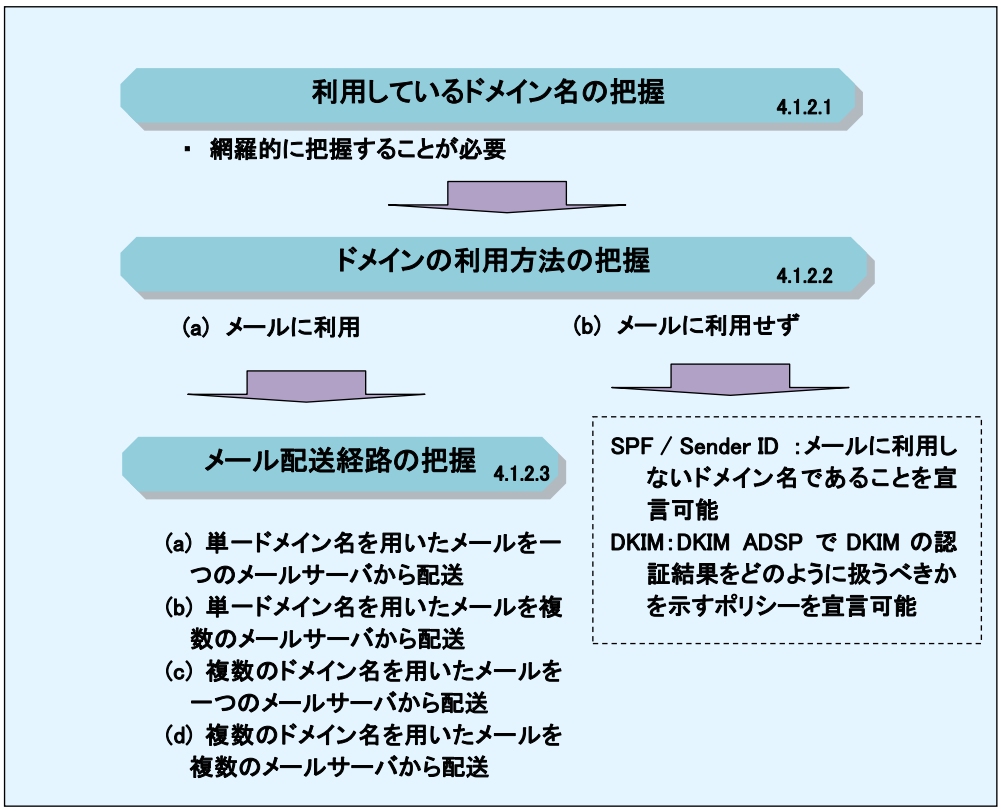
導入は、全てのドメインにおいて実施すべきです。実際に幾つかの導入状況の調査結果からも、SPF レコードの宣言率が高く、SPF/SenderID の送信側の導入が進んでいることが分かります。

受信側については、SPF レコードの宣言率が高いことから、SPF/SenderID の認証機能の導入が効果が得やすいでしょう。SPF と SenderID では、送信者情報の種類に違いがありますが、SPF レコードの形式はバージョン番号を除いて同じですので、可能であれば SPF/SenderID の両方の認証ができる機能の導入が望ましいと考えられます。

DKIM については、送信側の導入にあたっても、 SPF/SenderID に比べて導入のための費用はかかりますが、メールの送信者情報が詐称されているかどうかを認証する以外にも、メール本体が改変されていないことの判別もできること、電子署名というメールの配送経路に依存しない技術を利用するため、配送経路上の各メールシステムに変更を加えることなく多くの利用局面で利用できることなど、SPF/SenderID にはない利点があります。そのため、DKIM の導入については、送信するメールの重要度や受信しているメールに係る送信側での DKIM の導入割合などを考慮し、導入を進めるべきです。

4.1.2　ドメイン名の把握

次に、自組織内で利用しているドメイン名を把握しなければなりません。具体的には、利用しているドメイン名の把握、ドメインの利用方法の把握、メール配送経路の把握が必要です。



図表４－３　ドメイン名の把握

4.1.2.1　利用しているドメイン名の把握

まず、自組織内で利用しているドメイン名自体を正しく把握しなければなりません。

その際、メールに利用しているドメインについて把握することはもちろんですが、それ以外に、ドメイン名の構造上存在する上位ドメインや、メール以外の用途に使っているDNS で参照可能なドメイン名についても確認することが必要です。

4.1.2.2　ドメインの利用方法の把握

ドメイン名を把握したあとは、それぞれのドメインの利用方法を確認しなければなりません。

ドメインの利用方法は、メール利用の観点からは、大きく以下のように分類することができます。

(a) メールに利用しているドメイン名
(b) メールに全く利用していないドメイン名

(a) については、メールの配送経路を把握すること、適切な送信ドメイン認証技術の送信側の設定をすることが必要です。メールの配送経路の把握については、4.1.2.3 を参照して下さい。

(b) については、SPF / Sender ID では、メールに利用しないドメイン名であることをSPF レコードで宣言することができます。この設定方法の詳細については、3.2.3 を参照してください。DKIM では 、DKIM ADSP でDKIM の認証結果をどのように扱うべきかを示すポリシーを宣言できます。例えば、電子署名が付与されていないメールを破棄するような方針 (discardable) を宣言することで、勝手にドメイン名を利用するようなメールを防ぐことができます。DKIM ADSP については、3.4.6 を参照してください。

4.1.2.3　メールの配送経路の把握

次に、メールに利用しているドメインについて、そのドメインを用いて送信されるメールの外部への配送経路を把握しなければなりません。

配送される形態としては、大きく分けて、次の４つが考えられます。

(a) 単一ドメイン名を用いたメールを一つのメールサーバから配送
(b) 単一ドメイン名を用いたメールを複数のメールサーバから配送
(c) 複数のドメイン名を用いたメールを一つのメールサーバから配送
(d) 複数のドメイン名を用いたメールを複数のメールサーバから配送

(a) の場合には、そのドメインを利用するメールの出口（メールサーバ）が一つのメールサーバであることを、利用する送信ドメイン認証技術を用いて設定することになります。

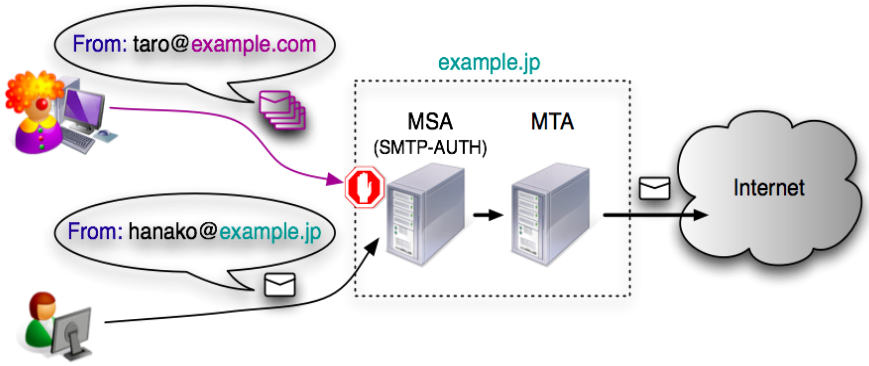
(b) の場合としては、送信効率を上げるために複数のメールサーバを利用しているような場合や、同じドメイン名を利用した特定のメールの配信を外部委託しているような場合があります。この場合にも、利用する送信ドメイン認証技術で、それぞれの送信側のメールサーバが、そのドメインから配送されるメールの正しい出口（メールサーバ）であること

を設定できます。

(c) の場合としては、メールの利用目的別に複数のドメインを併用している場合や、組織ごとにサブドメインを利用しているものの、全体の規模としてそれほど大きくないために、メールサーバを集約している場合などが考えられます。また、メールサービスを外部の複数の組織（ドメイン名）に提供している、いわゆるホスティングサービスの場合などもあります。さらに、(b) のメール配送業務を複数受託し、複数のドメイン名を送信者情報として利用する場合も、この形態に含まれます。

この場合には、それぞれのドメインが同じメールの出口を示すことで、受信側の認証に問題は生じません。

なお、いずれの形態であっても、メールが外部に配送される前に、そのメールで利用されるドメイン名の利用権限を送信者が適切に有しているかを、何らかの方法で確認することが必要です。この確認が適切に行われていないと、利用権限のない者がドメイン名を詐称して不正なメールを外部に配送することができてしまいます。こうしたことが行われると、送信ドメイン認証技術を設定していたことによって、受信側のメールサーバで、詐称されたメールの認証に成功してしまい、かえって問題となってしまいかねません。



図表４－４　送信者情報の利用権限の確認

(d) の場合には、クラウドサービスを用いたホスティングに多く見られる形態で、複数のドメインで複数のサーバを共有している場合があります。また、(b) と (c) の組合せのケースもあります。これらの場合には、(b)、(c) における対応を組み合わせることで正しい設定が可能です。

4.1.3　メールの利用方法の確認

事前準備の最後に、メールの利用方針を決定しなければなりません。

具体的には、メールの配送経路の方針、再配送を行うメールの利用方針、複数のドメインを利用する場合の方針、外部ネットワークから利用する場合の方針のそれぞれについて決定が必要です。

4.1.3.1　方針検討の必要性

メールの送信に利用するドメイン名と、実際のメールの配送経路は、これまで比較的柔軟

に運用されてきました。しかし、迷惑メールがメール流量の大部分を占めるようになってきた現在では、正しいメールが適切に受信できるようにするために、メールの利用方針を適切に決定し、運用することが必要です。

送信ドメイン認証技術が適切に機能するようにするためには、正規に送信されるメールが、送信側で利用するドメイン名に対応した正しい出口（メールサーバ）からのみ配送されるようになっていることが重要になります。

技術革新に伴い、メールの利用形態は多様化してきています。例えば、携帯電話の通信網を利用したデータ通信端末や無線 LAN のアクセスポイントなどモバイル環境は急速に普及してきており、それに伴い、これらの回線を利用したメールの利用も増えてきています。

また、業務として利用するメールや、個人で利用しているメール、ウェブメールなどアクセス端末をあまり選ばずしかも無料で利用可能なメールなど、同一の個人が複数のメールアドレスを利用するようになっています。

こうしたメールの利用形態の多様化を踏まえ、それぞれのドメインごとにメールが適切に受信できるようにするための対応が必要となりますが、それについては、技術的に対応可能な部分や、利用方針に基づく運用によるべき部分もあります。

以下では、メールの利用方針を決定し、それに基づく運用を適切に行う必要がある部分として、次の点について、詳細に検討します。

- メールの配送経路（4.1.3.2）
- 再配送メールの取り扱い（4.1.3.3）
- 外部ネットワークからの利用環境の整備（4.1.3.4）

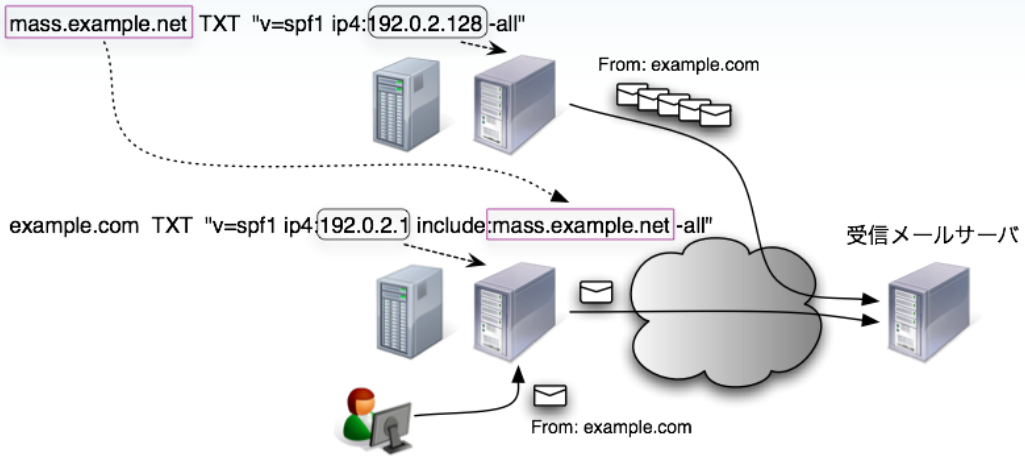
4.1.3.2　メールの配送経路

メールの利用形態としては、（典型的なものとして）１対１のコミュニケーションを目的としたものがあります。そのような場合には、送信に用いられるメールサーバが特定できますので、送信ドメイン認証技術の導入にあたっても、そのメールサーバを利用ドメイン名の出口（メールサーバ）として設定することになります。

メールの利用形態には、そのような一般的なメール配送以外にも、顧客へのアナウンスや特定の参加者への連絡網といった多数の宛先への一斉送信などがあります。メールの大規模配信を行う場合には、送信中に通常のメールが阻害されたりすることがないように専用のメールサーバを利用することがあります。また、こうした配送処理を効率よく行うために、専門の外部事業者へ委託することがあります。これらの場合に利用する送信者情報のドメイン名については、次の２つの考え方があります。

(a) 大量送信用の専用ドメイン名を利用
(b) 通常のメールと同じドメイン名を利用

(a) としては、サブドメインを新たに作成する場合や、別のドメイン名を取得する場合などが考えられます。この場合には、専用ドメイン名を使って配送する出口（メールサーバ）を特定し、それぞれのメールサーバで適切な送信ドメイン認証技術を導入することになります。



図表４－５　大量送信用の専用ドメインを利用する例

(b) には、メールの受信側にとって同じ組織からのメールであるという印象を強く受けるため、信用度が比較的高くなるといった利点があります。その場合には、大量送信されるメールは、通常のメールとは配送出口（メールサーバ）が異なりますので、そのドメイン名に対する送信ドメイン認証技術の設定に、これら大量送信を行うメールサーバを追加する必要があります。

例えば、SPF / Sender ID の場合には、SPF レコードに、これら大量送信を行うメールサーバを追加することになります。大量送信を行うメールサーバの管理が別組織で行われていたり、外部委託されたりしている場合には、それら実際の管理元で別のドメイン名で SPF レコードを宣言してもらい、それを "include" などの機構を使って取り込むことができます。これにより、大量送信を行うメールサーバが追加されたり、何らかの事情で IP アドレスが変更されたりした場合でも、通常のメールサーバのドメイン名の管理側にその都度連絡をすることなく、独立して運用することができます。

DKIM の場合には、電子署名の作成に利用する秘密鍵の管理の問題がありますので、外部委託している場合で秘密鍵を共有できる関係にないときなどには、(b) の方法を採ることはできず、署名ドメイン自体を別ドメインとし、それぞれで鍵の管理と運用を行うことが必要になります。

4.1.3.3　再配送メールの取り扱い

これまで利用されてきたメール利用形態の一つに、メールを一旦受信した後、外部へ再配送するような場合があります。具体的には、メールを転送するときやメーリングリストで再送するときなどです。これらの再配送処理にあたっては、送信ドメイン認証技術として考慮しなければならない事項があります。これらは、それぞれの送信ドメイン認証技術で、影響の受け方や対処方法が異なりますので、4.2 で解説します。

いずれの技術を利用する場合でも、再配送を行う際には、メール受信時に事前に認証を行い、その認証結果をメールヘッダに記録し

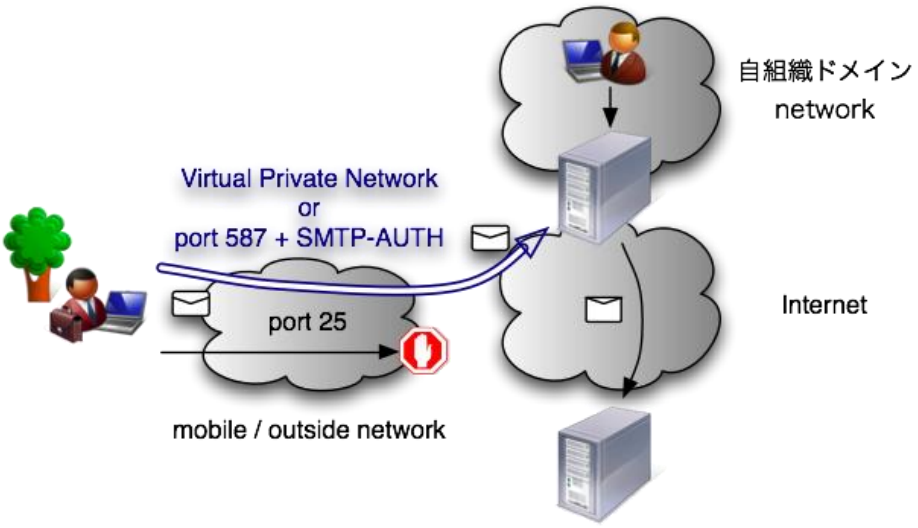
た上で再配送したり、正しく認証できたメールだけを再配送したりするなどの考慮が必要です。

4.1.3.4　外部ネットワークからの利用環境の整備

モバイル環境や社外滞在先など、外部ネットワークからメールを送信することがあります。

自組織で運営している送信用のメールサーバは、通常、セキュリティ上の観点からファイアーウォールなどを用意し、インターネット側から直接通信ができないような内部ネットワークに設置されています。そのため、外部ネットワーク上からメール送信を行うことを可能とするためには、別途 VPN などの通信手段を用意し、内部ネットワークにアクセス可能にする方法や、外部ネットワークからアクセスできる位置に送信メールサーバを用意する方法などがあります。

このような場合には、ネットワーク接続に利用している回線が OP25B を実施している可能性がありますので、メール配送に使われる 25 番ポートではなく、メール投稿用の 587 番ポートを使えるように設定することが必要です。また、送信者を正しく識別するために、SMTP AUTH (送信者認証) による認証を行うべきであり、認証方式についても、パスワードがそのままネットワークに流れない方式 (例えば CRAM-MD5 など) を利用すべきです。



図表４－６　SMTP AUTH による認証

最近では、ホテルなどの環境でもインターネット接続サービスが提供されるようになってきていますが、これらの環境では特に注意が必要です。

特に、欧米のホテルなどでは、ネットワークの不正利用を防ぐ目的で、メール配送に使われる 25 番ポートを用いて直接インターネットへの通信ができず、一度アプリケーション型のファイアーウォールなどで通信が終端されていることがあります。そのため、外部からアクセス可能な送信用メールサーバを用意している場合で、MUA からは通常どおり送

信が行われたように見えても、実際には自組織の送信用メールサーバを経由せず、ホテルなどが用意しているファイアーウォールから送信される場合があります。この場合には、メールの受信側では、受信したメールが、そのメールのドメインの本来の出口（メールサーバ）から送信されているメールではないために、認証が失敗することがありますので、注意が必要です。

4.1.4　導入計画の作成

送信ドメイン認証技術の導入に際しては、技術自体の違いやそれに関連した運用上の特徴以外に、より実際的な側面についても検討し、具体的な導入計画を作成することが必要です。

その検討の際には、以下に挙げた観点が参考になるでしょう。

(a) メールサーバの負荷調査
(b) 受信メールの傾向調査
(c) 認証結果の取り扱い
(d) 効果の予測と見直し
(e) 利用者への周知
(f) 導入手順の策定

4.1.4.1　メールサーバの負荷調査

メール送信側に DKIM を導入する場合や、メール受信側で認証を行う場合には、メールサーバに新たな機能を追加することが必要です。この機能追加により、メールサーバの負荷が高くなりますので、導入前には既存のメールサーバの負荷状態を把握することが必要です。CPU などのリソースの負荷は、いずれの技術を導入する場合でも高くなります。また、受信側で認証を行うことにより DNS の参照回数が増えるため、ネットワーク帯域や DNS のキャッシュサーバの負荷などの考慮も必要になります。

一般にメールの流量は、時間帯によってばらつきがありますし、ピーク時に極端に負荷が高くなる場合もあります。導入に際しては、予め一定の期間の負荷状況を計測し、予想される負荷の上昇分を重ねた上で、設備設計を行うことが必要です。

4.1.4.2　受信メールの傾向調査

受信側では、広く受信メールの傾向を調査することによって、導入する技術の判断に役立てることができます。例えば、既に送信者情報を詐称したメールに困っている場合や、取引先など受け取るべきメールが把握できている場合には、認証の効果を予め予測することができます。予め受け取るべきメールが明確である場合は、それらのメールの送信側で導入している技術を受信側でも導入するべきです。

送信側についても、受信側で認証している技術が予め分かる場合には、導入に際して、参考となるでしょう。

4.1.4.3　認証結果の取り扱い

受信側では、認証の結果の利用方法も予め決めておくことが必要です。メールヘッダに認証結果を示すだけなのか、認証が成功した特定のドメインをホワイトリスト的に優先的に配送するのか、誤認証の可能性がないドメインで認証が失敗した場合に隔離するのかなど、認証結果を有効利用する方法はいくつか

あります。受信メールの傾向調査と合わせて、それぞれの認証結果と送信元のドメインに応じた、効果的な取り扱いの方針を決めることになります。

また、メールは多様な用途で用いられるため、メールシステム全体で一律に適用できない認証結果に基づいた処理も、個々のメール受信者が MUA などで個別に設定することにより、認証結果を有効に利用できる場合があります。メールサービス提供者やメールシステムの管理者は、こうした設定例などをマニュアル等で利用者に周知すると良いでしょう。

4.1.4.4　効果の予測と見直し

受信側では、事前に受信メールの調査を行うことにより、認証による効果を予測することができます。また、送信ドメイン認証技術を導入するメールサーバは、今後も増えてくることが予想されますので、導入時だけでなく、継続してメールの傾向を把握することが有効です。これは、導入時には見送った技術がより機能するようになっていたり、認証結果をより効果的に活用できるようになっていたりするなどによるものです。

4.1.4.5　利用者への周知と導入手順の策定

送信ドメイン認証技術を導入する際には、予めメールの利用者に対して、送信側及び受信側での運用ポリシーを事前に説明しておくことも必要です。特に送信側の利用ポリシーについては、送信ドメイン認証技術の対象としているドメイン以外のドメインを送信者情報として利用しないよう周知しておくことが重要です。メールの受信側で認証が失敗するような使い方をしてしまうことによって、そのドメインやメールの送信元の評価が低下してしまう可能性があります。

また、メールは絶え間なく送受信されていることから、メールシステムへの送信ドメイン認証技術の導入やそれに基づく新たな機能追加、仕様変更などは、頻繁にできない場合もあります。このため、手順を決めて、計画的に導入を進めることが必要です。

さらに、メールを送受信している相手の導入状況も変化していきますので、日頃のメール送受信の状況の把握とともに、その結果に基づいた新たな機能追加や仕様変更などの見直しについて、予め計画を立てることも必要となります。

4.2　一般的な導入手順

送信ドメイン認証技術には、ネットワーク方式の SPF/SenderID と、電子署名方式の DKIM の二つの技術があります。それぞれの技術についての概要、導入に際しての注意点については、第 3 章で解説しています。

ここでは、一般的な導入手順について、送信側での対応を中心に、それぞれの技術ごとに解説します。また、導入に際して既存のメールの使われ方との関係や、問題が生じる場合の対処方法について解説します。

4.2.1 SPF/SenderID

SPF と SenderID は、送信者を認証するために送信元の IP アドレスを利用するネットワーク方式であること、認証のために送信側のドメイン (DNS) 上にある SPF レコードを利用するなど、多くの共通点があります。ここでは、両方の技術について、導入手順のほか、そのままでは認証がうまくできない課題と対処方法などについて解説します。

4.2.1.1 SPF/SenderID の導入手順

SPF/SenderID を送信側に導入するためには、対象とする送信者情報のドメインに対して SPF レコードを宣言することが必要になります。

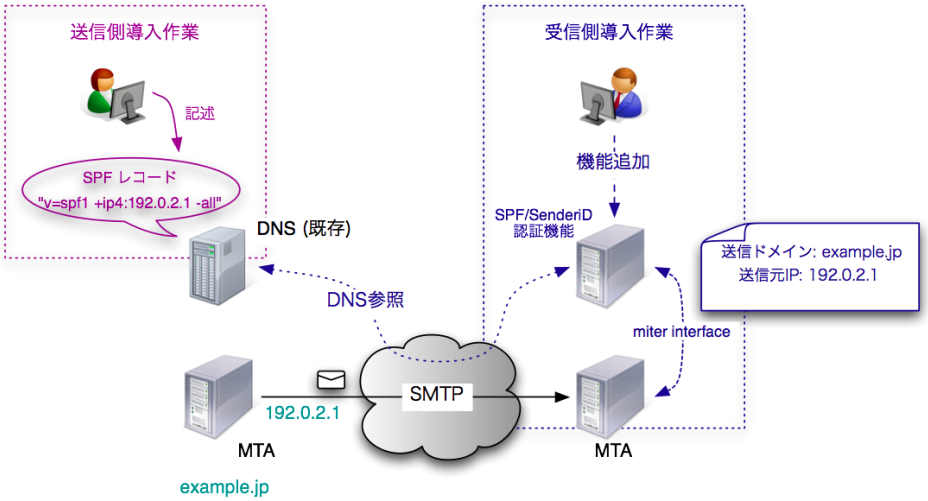
DNS サーバを自組織で管理している場合や、運用を委託しているサービスで、DNS の資源レコードをある程度自由に編集できるような場合には、4.1.3.2 で示したようにメールの配送経路 (出口) を正しく把握した後、それをもとに SPF レコードを記述することになります。この場合、送信側の導入に際して特別な費用は発生しません。

メールの運用自体を外部委託している場合や ISP のメールサービスを利用している場合には、第 5 章以降を参考に、それぞれ設定して下さい。なお、DNS の運用を外部委託していて、自由に編集が行えないような場合には、委託先に SPF レコードの設定依頼が必要になりますので、送信側の導入に際し、費用が発生する場合があります。

SPF/SenderID を受信側に導入し、メールの受信時に認証するためには、受信メールサーバへの新たな機能追加が必要になります。すなわち、受信側での認証を行うためには、送信元の IP アドレスが必要になりますので、原則として、外部から直接メールを受けるサーバ上に認証機能を追加する必要があります。例えば、迷惑メールフィルタ機能を提供するサーバで、送信ドメイン認証機能も提供するものがありますが、その機能を用いるためには、そのサーバが外部からのメールを直接受ける位置にあるかどうかの確認が必要です。

オープンソースの MTA として広く使われている Sendmail や Postfix では、MTA の拡張機能を外部プログラムとして追加できるように、milter インターフェースが標準で提供されています。この milter インターフェースを利用した認証機能を実現するものが、同様にオープンソースとして公開されていますので、それを利用することもできます。

商用のメールサーバを利用している場合や外部のメールサービスを利用している場合には、その開発元やサービス提供元に問い合わせて下さい。その場合には、認証機能の追加には、新たに費用が発生する可能性がありますので、確認が必要です。

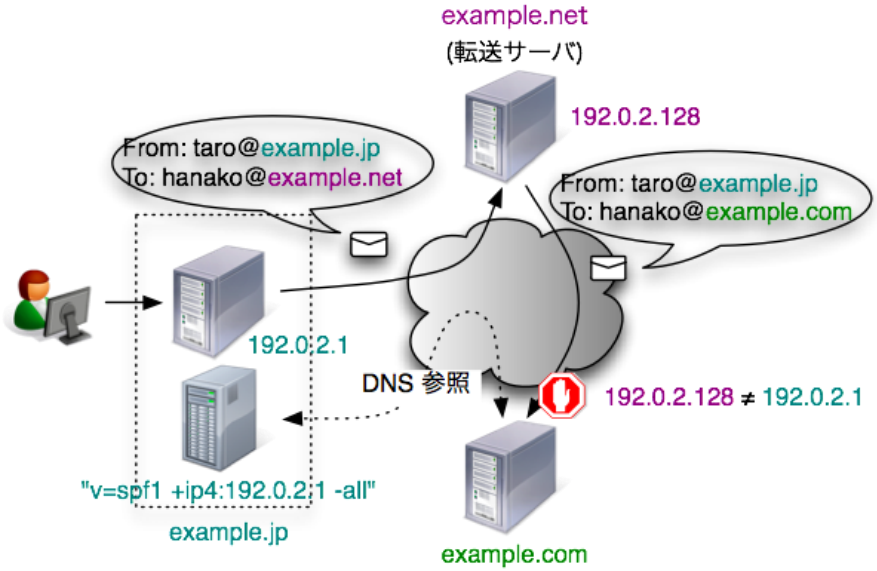


図表４－７ SPF/SenderID の導入

4.2.1.2 課題と対策

ネットワーク方式の送信ドメイン認証技術は、メールの再配送時に認証が失敗してしまうという問題があります。これは、メールの再配送時に、メールを一旦受け取った後、送信者情報をそのままにして、新たな受信者へメールを再配送してしまうことに起因する問題です。

具体的な事例としては、メール転送や古い実装のメーリングリストサーバで発生することがわかっています。



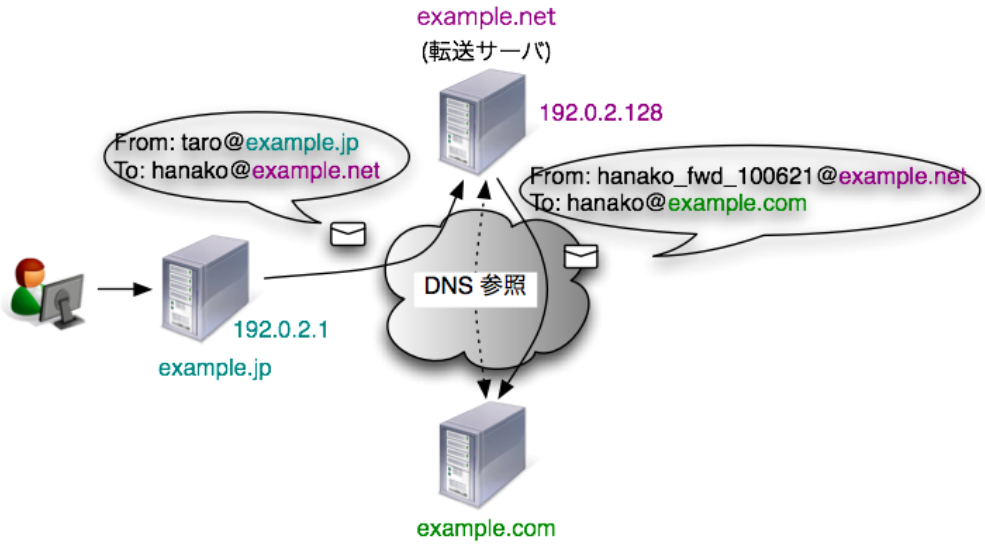
図表４－８ メール再配送による認証失敗の例

この問題を回避するには、メールの再配送時に、送信者情報をメールの再配送元のドメインに書き換える必要があります。

現時点でそれほど広く運用されているものではありませんが、メールの転送に関しては、以下の方法を用いることで、転送先でも正しく認証を行うことができるようになります。

まず、SPF の場合には、リバースパスを送信者情報として認証しますので、転送時に認証が失敗しないようにするために、転送を行う際のリバースパスとして、元の送信者のリバースパスを利用するのではなく、転送元（転送者）のドメインを含むメールアドレスを利用する方法があります。

この場合、転送時にすべてのメールのリバースパスを単純に書き換えてしまうと、メールがループする可能性がありますので、転送時に利用するリバースパスは、転送者のメールアドレスをそのまま利用するのではなく、例えば、図表４-9 のように、メールアドレスのローカルパート部分を工夫して、エラーメールとして戻ってきた場合や、さらに再転送されてきた場合に区別ができるようにすることが必要となります。このようにすることで、転送したメールが何らかの事情で戻ってきた場合に、さらに転送を繰り返さないことにより、不要なループを防ぐことができます。



図表４－９　メール転送への対応の例

Sender ID の場合には、送信者情報として PRA を用いて認証しますので、メールの転送時に、PRA で優先的に使われるヘッダ(Sender ヘッダなど)に、転送元のドメインを含んだメールアドレスを送信者情報として付加すれば問題ありません。

メーリングリストに関しては、リストメンバの管理のために、エラーメールの送信先を示すリバースパスには、メーリングリストの管理用のメールアドレスを指定するようになっています。そのため、SPF では、リストメ

ンバ側で認証が失敗するようなケースはほとんどなくなっています。

しかし、一部の古い実装のサーバプログラムのメーリングリスト機能では、PRA として From ヘッダより優先度の高いヘッダを付けないものがあり、そうした実装では、SenderID では、リストメンバ側で認証が失敗してしまいます。

このため、メーリングリスト機能を使う場合には、メーリングリスト側からメンバへの送信時に、Sender ヘッダなどにメーリングリスト管理用のメールアドレスを追加する機能を持った、最近の実装のサーバプログラムを利用することが推奨されます。

4.2.2 DKIM

DKIM では、送信者情報が正しく表明されているかどうかを、公開鍵暗号方式を利用した電子署名を検証することによって認証します。このため、ネットワーク方式とは異なり、メールの配送経路に影響を受けないという大きな利点があります。その反面、メールの送信側にも電子署名を作成して添付する負担が生じます。

ここでは、DKIM の導入手順のほか、運用上課題となる点について解説します。

4.2.2.1 DKIM の導入手順

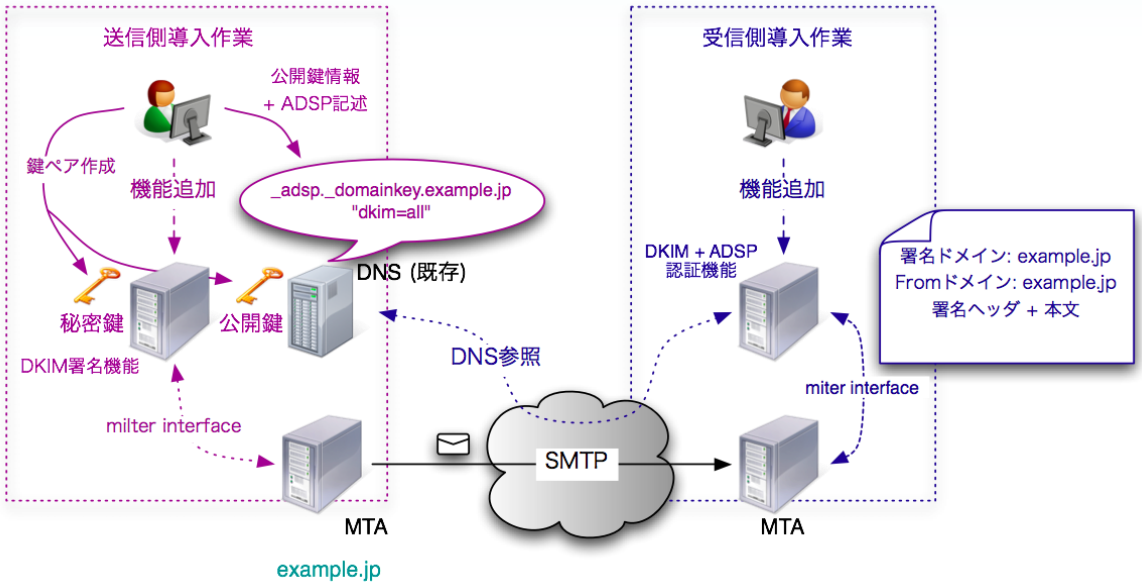
DKIM を送信側に導入するためには、メールの送信時に電子署名を作成し、それをメールヘッダ(DKIM-Signature) として追加する機能が必要になります。

SPF/SenderID と同様に、オープンソースの MTA である Sendmail や Postfix の milter インターフェースを利用することにより、DKIM の電子署名の作成機能を追加することができます。

DKIM では、電子署名の作成に公開鍵暗号技術を使いますので、予め電子署名を作成するときに利用する秘密鍵と、電子署名を検証するために利用する公開鍵を用意する必要があります。オープンソースの OpenDKIM プロジェクトでは、これら鍵のペアを作成するスクリプトプログラムもソースコード一式の中に含まれていますので、これを利用して鍵ペアを生成することもできます。商用のメールサーバを利用している場合や外部のメールサービスを利用している場合には、その開発元やサービス提供元に問い合わせて下さい。DKIM を送信側に導入するためには、新たに費用が発生する可能性がありますので、確認が必要です。

DKIM を受信側に導入する場合には、メールサーバに対して、電子署名を検証し、認証処理を行う機能の追加が必要になります。

この受信側の認証機能も OpenDKIM プロジェクトで提供されています。商用のメールサーバやメールサービスを利用している場合で導入を検討している場合には、提供元に確認が必要です。送信側への導入と同様に、新たに費用が発生する可能性がありますので、確認が必要です。

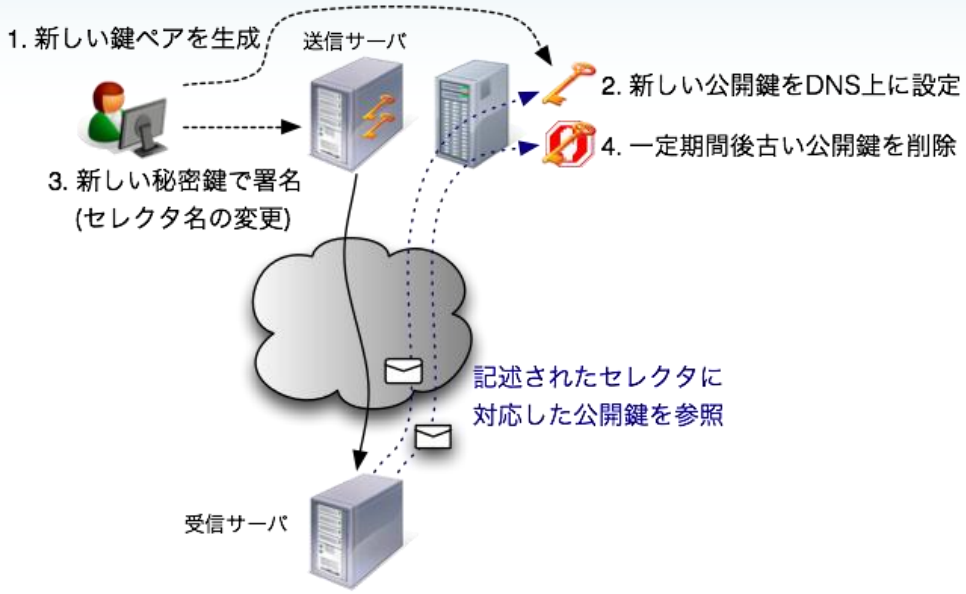


図表４－１０　メール転送への対応の例

4.2.2.2 鍵の管理と運用

DKIM の電子署名を作成するために必要な秘密鍵は、外部に漏れないようにきちんと管理しなければなりません。秘密鍵がわかってしまうと、認証に成功する DKIM の電子署名を第三者が勝手に作成できてしまうことになり、そのドメインに対する認証の意味がなくなってしまいます。

また、DKIM で利用する鍵のペアは、セキュリティ上の観点から、定期的に変更することが望ましいとされています。鍵のペアの変更にあたっては、公開鍵は、DNS の仕組みを利用してメール受信側に渡されますので、ある時期を境に鍵ペアを変更しても、 DNS の伝播の問題で正しい鍵の組み合わせにならない可能性があることに注意が必要です。この点については、DKIM では、3.4.2 で解説したように、同一ドメイン上に、セレクタを利用して複数の鍵を DNS 上に同時に公開することができますので、この仕組みを利用し、セレクタ値と、それが指し示す公開鍵に対応した秘密鍵を切り替えることにより、電子署名の作成に利用する鍵を見かけ上瞬時に切り替えることができます。以下に、鍵を切り替える手順を示します。



図表４－１１　鍵の切替え手順

新たに利用するセレクタ名は、予め取得できないように、なるべく予測しづらい名称 (例えば、番号や続きが連想される名称は避ける) を利用すると良いでしょう。予め公開鍵がわかると、解読のための時間が増えることになり、危険性も増すおそれがあるからです。また、特別な事情がない限り、古いセレクタ名 (鍵ペア) に戻すことはせずに、常に新しいセレクタを用意し続けるべきです。

このセレクタの仕組みをうまく活用すれば、例えば、ハッシュ長が短い SHA-1 を利用している場合でも、頻繁に鍵を変更していくことによって、ある程度のセキュリティを保つことができます。これにより、送受信側ともに、電子署名の作成・検証に必要となる処理能力を抑えることもできます。しかし、絶対に詐称されては困るような大事なメールには SHA-1 は利用すべきではありませんし、新たな攻撃手段が開発されて、より脆弱性が高まった場合にも利用すべきではありません。

4.2.2.3 課題と対策

DKIM では、メール本体の電子署名の対象となっている部分が改変されない限り、認証が失敗することはありません。逆にいえば、Subject ヘッダやメール本文にフッタ情報などを追加するようなメーリングリスト機能では、リストメンバでのメール受信時に認証が失敗する可能性があります。このような場合には、メーリングリスト側で投稿者からのメールを受け取るときに認証を行い、その結果も含めて DKIM で再署名するなどの対応が必要になります。

DKIM の課題として、もっとも難しいものは、電子署名のポリシーの問題です。DKIM では、認証の対象となるのは、正確には、送信者情報ではなく、署名者の情報になります。つまり、電子署名がないメール（署名者の情報がないメール）に対しては、認証が全くで

きないことになります。その結果として、受け取ったメールがたまたま電子署名の対象としていないメールだったのか、誰かが詐称して送ってきたメールなのかの判断ができないことになります。この点は、メールにもともと備わっている送信者情報を利用する SPF/SenderID と DKIM の大きな違いの１つです。

この問題に対応するため、DKIM には、3.4.6 で解説した DKIM ADSP の仕組みが追加されました。送信側で ADSP を表明することにより、送信する全てのメールに電子署名が添付されているはずなのか (dkim=all) 、一部だけなのか（dkim=unknown)を送信側が示すことができます。

しかし、この対応策については、まだ問題が残っています。3.4.6.2 で解説したとおり、ADSP を表明するのは、From ヘッダ上のメールアドレスのドメイン名のサブドメインですので、メール配信を請け負う事業者が、顧客のドメインを From ヘッダに利用し、実際の電子署名の作成を事業者側が行うような、いわゆる第三者署名をどう認証するのか、が問題となります。また、同様のケースとして、メーリングリストの問題もあります。

DKIM は、ドメインを自ら管理し、そのドメインを送信者情報及び署名者情報として使う場合には、とてもうまく機能しますが、メールの利用形態は多様化していますので、それぞれの使い方にうまく適合させるための工夫も必要になってきています。現在もこうした議論は続いておりますので、こうした問題をうまく解決し、適合できるようになることが期待されます。

4.3 運用

送信ドメイン認証技術を導入後にも、その効果を維持するために、日々正しく運用することが必要です。メールシステムの管理者は、受信側に必要とされるメールを正しく送信することにより、そのドメインの信頼性を高めていくことができます。また、送信ドメイン認証技術では、メールサーバだけでなく DNS も重要な役割になっていますので、DNS が正しく機能するような運用が必要になってきます。

4.3.1 メールサーバの運用

送信ドメイン認証技術は、送信者情報が詐称されているかどうかを認証する技術ですが、認証されたドメインが、必要なメールを送信しているドメインなのか、迷惑メールを送信するドメインなのかまでは判断しません。

そのため、受信側での迷惑メール対策としては、送信ドメイン認証技術による認証に加え、ドメイン自体を評価する仕組みが別途必要になります。

また、送信側では、送信ドメイン認証技術を導入しても、そのメールサーバから実際に迷惑メールが送信されてしまえば、ドメインの信用は低下してしまいます。そのため、せっかく送信ドメイン認証技術を導入したにもかかわらず、評判の悪いドメインだと判断されないように、関係のない第三者が勝手にメールサーバを利用できないようにきちんと設定し、管理することが必要になります。例えば、SMTP-AUTH のパスワードに安易な文字列を設定できないようにしたり、自らのメールサーバを利用するメール送信者の PC に不正プログラム (マルウェア) が混入されて

パスワードが漏洩しないようにしたりという対策を講じなければなりません。また、業務的なものを除いて短時間で大量にメールが送信されていないか、短時間で地理的に離れた場所からメール送信されていないかなどの監視等も必要になる場合もあります。

4.3.2 DNS の運用

送信ドメイン認証技術では、送信側から受信側へ伝える、認証に必要な各種情報を DNS を利用して受け渡しします。そのため、メールの送信側ドメインの DNS が常に正しく動作していることが必要です。

4.3.2.1 DNS の状態監視

送信側の DNS に何らかの問題があり、受信側で、SPF レコードや DKIM の公開鍵の情報が取得できなかった場合には、認証結果は temperror (一時的な失敗) となり、正しく認証できません。認証結果の temperror を受信側でどのように扱うかにもよりますが、送信側で送信ドメイン認証技術に関する情報を正しく設定していたとしても、利用している DNS が不安定だったり、何らかの問題があって正しく情報が引き出せない状態にあったりすると、場合によっては受信側で受け取ってもらえないことになり、送信ドメイン認証技術を導入していない場合よりも悪い結果となる可能性もあります。

また、送信側の DNS からの応答が遅かったり、応答を返さないなど不安定な状態にあったりする場合には、受信側での認証処理に負荷がかかる原因になります。特に、大量のメールを受けているメールの受信者には、深刻な問題となる可能性があります。 3.2.4.3 で解説したとおり、SPF や Sender ID での SPF レコードの記述方法で、DNS の参照回数に上限が決められているのも、受信側での認証時の処理を軽減させる意味が含まれています。

送信側のドメインの管理元は、DNS の状態を監視したり、きちんと運用体制が整っている外部のサービスプロバイダを利用したりするなど、 DNS の維持管理を心がけるべきです。

4.3.2.2 DNS の TTL

DNS では、問合せを高速に処理するために、キャッシュの仕組みがあります。このキャッシュの仕組みとその TTL は、SPF レコードや DKIM の公開鍵の変更時の伝播時間と密接な関係があります。TTL の値を大きくすることで、送信側ドメインの DNS へのアクセス回数を少なくする ことができますが、一方で SPF レコードや DKIM の公開鍵や DSP レコードを変更した場合に、受信側のメールサーバに反映されるまでに時間が長くなってしまいます。

送信側のドメインで、これら DNS 上の情報を変更する場合には、予め利用している DNS の TTL 値を把握したうえで、その時間に合わせて十分情報が伝播した後に、システムの変更や鍵の変更をする必要があります。DNS の TTL 値の変更が可能な場合には、前もって TTL 値を短い時間に設定しておくと、変更作業までの時間を短くすることができます。

第５章　ISP での対応

第 5 章　ISP での対応

本章では、ISP が送信ドメイン認証技術を導入する場合に考慮すべき事項について解説します。

ISP が運用するメールシステムは、2.1 で解説したような構成となっており、提供するサービスの規模にもよりますが、概ねメールの送信側と受信側でそれぞれのメールの流れがあります。ここでは、送信ドメイン認証技術の導入に際し、ISP として、メールの送信側及び受信側のそれぞれで行うべき作業や検討すべき事項について解説します。

5.1　ISP のメールサービスの概要

ISP のメールサービスは、ISP が管理する固定的なドメイン名を用いたメールアドレスを顧客に提供し、インターネットへのメールの送信と顧客宛のメールを受信します。受信したメールは、メールアドレスごとにメールスプールに格納されます。メールスプール上の受信メールは、顧客が MUA や、ウェブメール機能を提供している場合はウェブブラウザなどを利用して閲覧します。

ISP はドメインを管理している場合が多いので、SPF レコードの設定や DKIM の公開鍵の設定など、DNS 上に必要となる作業を自社で行えるため、送信ドメイン認証技術の導入が比較的容易であるといえます。また、メールスプールも管理していますので、例えば送信ドメイン認証技術で認証が失敗したメールを通常閲覧できる領域と別の場所に保管したり、認証が成功した特定のドメインからのメールを優先的に受信させるなど、フィルタサービスの機能拡充に応用することも可能です。

5.2　送信側の対応

5.2.1　概要

ISP が送信するメールは、一般の企業や各種組織のドメイン名を利用して送信されるメールに比べて、その規模が大きかったり、利用目的が多様であることにより様々な種類のメールが送受信される、という特徴があります。送信ドメイン認証技術を送信側で導入し、ISP を経由しない詐称されたメールを区別できるようにすることは、ISP のドメイン名の信頼度を向上させるために非常に重要です。

送信ドメイン認証技術は、送信者情報が偽装されているかどうかを確認可能とする技術なので、送信側で送信ドメイン認証技術を導入することにより、迷惑メールの多い ISP のドメイン名が、逆に迷惑メールの送信元として判断されてしまう可能性もあります。ISP から日々大量に送信されるメールの中に、メールの受信者にとって迷惑メールとなるようなメールが含まれていないか、それらが誰から送信されているのかを管理することも重要です。自社のドメイン名に対して迷惑メールを送信するドメインとしての評判が下がらないように、何らかの監視等の管理が必要です。

5.2.2　送信ドメイン認証技術の導入

5.2.2.1　SPF/Sender ID の導入

ネットワーク方式の送信ドメイン認証技術である SPF / Sender ID を送信側で導入するためには、メールに利用しているドメインについて、3.2.4 で解説した SPF レコードの記述が必要です。

SPF レコードには、メールの出口であるホストのグローバル IP アドレスが含まれるような、ネットワークアドレスや IP アドレス、ドメイン名などを記述します。これらの出口には、通常の送信用のホスト以外に、例えば、受信側が一時的に受け取らなかった場合に移される再配送用のホストや、メールサービスで利用しているドメイン名を使った顧客向けの連絡用の送信用メールサーバなども含める必要があります。

5.2.2.1.1　サブドメイン利用時の注意

メールサービスに、複数のドメイン名が利用できるようになっている場合には、それぞれのドメインについて SPF レコードを記述する必要があります。

また、複数のドメイン名を利用している場合で、それぞれがサブドメインの構成となっており、それらの親ドメインをメールサービスに利用していないときは、注意が必要です。SPF レコードが記述されていないドメイン名は、詐称されても受信側で判定できませんので、よく目にするドメイン名の認証結果が fail / softfail などの認証失敗でない場合には、誤解を与えてしまう可能性がありますので、3.2.3 と 4.1.2.2 で解説したとおり、以下のように、メールに利用しない親ドメインの場合は、明示的にすべて認証が失敗するような SPF レコードを宣言した方が良いでしょう。

```
example.jp              TXT "v=spf1 -all"
apple.example.jp    TXT "v=spf1 +ip4:192.168.0.4 -all"
peach.example.jp    TXT "v=spf1 +ip4:192.168.0.4 -all"
mango.example.jp    TXT "v=spf1 +ip4:192.168.0.4 -all"
```

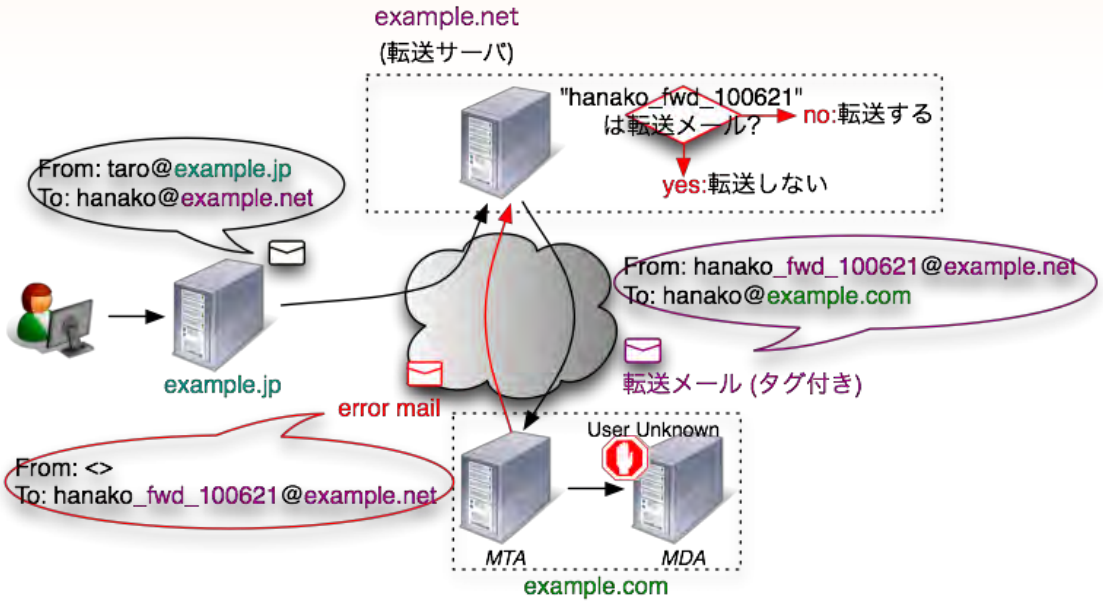
図表５－１　サブドメインがある場合の SPF レコードの例

5.2.2.1.2　転送処理

一度受信したメールを、あらかじめ設定された別のメールアドレスへ送信する転送機能は、古くから提供されてきた機能の一つですが、 4.2.1.2 で解説したとおり、ネットワーク方式の送信ドメイン認証技術との相性は良くありません。すなわち、現在提供されている多くの転送機能は、転送時のリバースパスに元々の送信者のリバースパス情報をそのまま使いますので、転送先での SPF の認証は失敗してしまいます。

転送設定は、メールの利用者がそれぞれ設定しますし、転送先のメール利用者は転送者と同一であることが一般的です。そのため、転送先のメール受信設定で、転送元からのメールが SPF の認証が失敗しても受け取るようなフィルタ等の設定が可能であれば、受け取ることは可能になります。

SPF の場合は、送信者情報としてリバースパス を利用しますので、4.2.1.2 で解説したとおり、転送時に送信元の情報を利用するのではなく、転送者のメールアドレスを設定し直すことによりこの問題は回避できます。ただし、単純にリバースパスを書き換えてしまうと、転送先で受け取れなかった場合やエラーメールなどが、ループしてしまう可能性があります。そのため、転送時に書き換えるメールアドレスは、ローカルパート部分に何らかの印となるような文字列を別途挿入し、通常の受信メールと転送メールの戻りメールとを区別できるような工夫も考えられます。通常の受信メールは転送し、転送したメールが戻ってきた場合には、そのまま転送せずに利用者のメールボックスに格納するなどです。



図表５－２　転送時の処理の例

転送先のメールシステムが Sender ID で認証している場合も、単純に受信したメールを転送したときには、認証が失敗します。転送時には、転送者のメールアドレスを Resent-From ヘッダに記述することで、転送先の Sender ID の認証時に送信者情報として認識されることになります。メール形式を定義する規格である RFC5322 では、転送のような再送信されるメールについては、Resent-From ヘッダなどの Resent- ヘッダを追加すべきと示されています。

5.2.2.2　DKIM の導入

DKIM は、送信するメールそれぞれに電子署名を追加して送信元を明らかにします。3.4.3 で解説したとおり、電子署名は、メール本文（ヘッダとメール本文の内容）のハッシュ値の計算、公開鍵暗号技術による電子署名の作成という処理を、メール送信のたびに行います。そのため、これまでのメール送信時より負荷が高くなることが予想されますので、導入時にある程度設備に余裕があるかどうかを確認する必要があります。設備負荷は、電子署名の作成に利用するアルゴリズムとも関連しますので、それとも合わせて検討が必要です。

次に、どのメールに対して電子署名を行うかの判断については、送信者情報が偽装されていないかを確認するという送信ドメイン認証技術の目的を考えると、基本的にはすべての送信メールを対象に電子署名を付与することが望ましいでしょう。自 ISP 宛に送信するメールなど、送信者が明確に判断できるような場合もありますが、そのメールが転送されて外のメールシステムに届くような場合も考える必要があります。

5.2.3　迷惑メールの管理

多くのユーザが利用する ISP のメールサービスでは、自身のドメイン名の評判を下げないような運用を心がける必要があります。

例えば、迷惑メールが自社のメールサーバを経由して送信されていた場合には、その迷惑メールの受信側からの申告により、ブラックリストに登録され、以降そのブラックリストを利用しているメール受信側に通常のメールも含めた全ての届かなくなってしまうことが考えられます。近年の迷惑メールの増加傾向により、こういった迷惑メール対策を行うメール受信者は増えていますし、送信ドメイン認証技術の普及によりドメイン名による受信制御が行われることが予想されます。

そのための対策としては、以下の事項が考えられます。

5.2.3.1　送信側の迷惑メール対策

迷惑メールの送信元となる ISP と判断されないためには、そもそも迷惑メールが外部に送信されないような仕組みがあれば良いことになります。現在、多くの ISP ではメール受信時に迷惑メールかどうかを判定する迷惑メールフィルタを提供しています。こういったフィルタがメールの内容から判断するタイプのものであれば、それを送信時にも適用し、迷惑メールを送信しようとしている場合に保留することによって、外部への送信を抑制することができます。

しかし、迷惑メール判定には誤判定が発生しますし、送信されなかったことが送信者に通知できない場合に問題となる可能性がありますので、利用者のサポートは十分に行う必要があります。また、送信側にもフィルタを導入することで新たな費用が発生する可能性もありますので、費用対効果なども含めて検討する必要があります。

5.2.3.2　送信者の特定とその対策手順の確立

迷惑メールが ISP のメールサーバから送信される可能性を完全に排除することは困難ですので、問題を大きくしないためにも、仮に迷惑メールが送信されても、受信者からの連絡があった場合などには、その迷惑メールを誰が実際に送信したのかを判断する仕組みが重要になります。

送信者を特定するには、メール送信時に送信者の認証を ID とパスワードによって行う SMTP-AUTH を導入し、メールヘッダやメール送信ログに、その AUTH ID を記録するなどして、誰が実際に送信したかを調べる方法があります。最近では、不正プログラム (マルウェア) に感染して、利用者が知らない間に外部から制御されて迷惑メールを送信することが問題となっており、SMTP-AUTH にも対応したマルウェアが現れているのではないかともいわれています。そのため、AUTH ID を利用して迷惑メール送信者を特定し、利用者への通知及び解決のためのサポートを行うことは、顧客保護の意味でも重要になってきます。また、迷惑メールの大量送信を抑制するために、AUTH ID 単位で、一定時間内に送信できるメール数を制限する方法があります。

5.2.3.3　送信者情報を変更できないような仕組み

送信ドメイン認証技術で送信者情報として使われるのは、リバースパスと From ヘッダアドレスのドメイン部分となります。受信側で送信ドメイン認証が失敗しないためには、これらが正しい情報となっている必要がありますので、顧客からメールが投稿された場合に、これらの情報が認証失敗するものになっていないかどうかを、配送前に確認すると良いでしょう。

メール投稿時に指定されたこれらの情報が、あらかじめ送信ドメイン認証に失敗することが分かった場合に、ISP が取りうる対応方法の例を以下に示します。

(a) メールの投稿そのものを受け付けない (エラー応答する)
(b) リバースパスの場合、ISP のドメイン名のメールアドレスに付け替える
(c) From ヘッダアドレスの場合、Sender ヘッダなどに ISP のドメイン名のメールアドレスを追加する

これまで、多くのメールサービスでは、これら送信者情報の指定方法については比較的緩やかな運用をしていました。そのため、このような対応を急激に行うと、利用者にとって混乱の原因になりかねませんので、事前の周知が重要になります。

また、DKIM の場合も From ヘッダアドレスのドメイン名とは無関係ではありませんので、DKIM-Signature ヘッダに示される送信者情報のドメインと異なるようなことがある場合は、同様に何らかの対策が必要になります。

5.2.3.4　エラーメール処理

受信したメールが宛先不明で配送できなかった場合は、メールの送信者にエラーメールを送信する必要があります。エラーメールは、リバースパスに指定されたメールアドレスに送信されます。迷惑メールの多くは、このリバースパスを詐称する場合が多いので、結果として不要なエラーメールがメールアドレスを詐称された側に大量に送信されることになります。

ISP では、決まったドメインを使ってメールサービスを提供しますので、詐称に使われる可能性が比較的高いドメイン名である一方、不特定多数にサービスを提供していることもあり、宛先不明となる迷惑メールも多く、結果として不要なエラーメールを多数送信している可能性もあります。こうした不要なエラーメールを抑制するためには、次の対策があります。

(a) メールの受信時点で宛先が存在するかを確認して存在しない場合は受け取らない
(b) 受信時に送信ドメイン認証技術で認証が失敗した場合にエラーメールを送信しない

(a) の対策のために、メールの受信時に、宛先が存在するかを確認するには、顧客管理を行っているシステム (データベースなど) とリアルタイムで問合せできることが必要です。メールシステムの構成として、

メールスプールが存在するかどうかで宛先不明かどうかを MTA ではなく、MDA が判断している場合には、システムの変更が必要になります。また、メール受信時に宛先不明かどうかを SMTP 上の応答として返すことになりますので、送信側でその応答を確認することにより、実在するメールアドレスかどうかを簡単に調べることができてしまいます。よく使われるローカルパートの文字列を総当たり的に指定して実在するメールアドレスを取得する攻撃は、辞書攻撃 (DHA: Directory Harvesting Attack) と呼ばれます。これを防ぐためには、一定数以上の宛先不明が発生した場合に、以後の SMTP 処理を継続しない、という方法があります。

宛先不明時にエラーメールを返す送信先は、詐称されていない実際の送信元です。そのため、送信ドメイン認証技術で認証が失敗した送信先、例えば SPF / Sender ID で認証結果が fail / softfail となった送信元や、DKIM で認証が失敗した場合や、ADSP で fail/discard であったような送信元には、エラーメールを送信する必要はありません。このため、(b) の対策を実施することも考えられます。

5.3　メール受信側としての検討

5.3.1　概要

第３章で解説したとおり、送信ドメイン認証技術を用いることにより、メールの受信側が認証を行うことで、そのメールが本当にそのドメインから発信されたかどうかを判定することができます。送信ドメイン認証技術は、送信側の対応も必須ではありますが、受信側が対応を進めることは送信側の導入モチベーションにも繋がるものです。そのため、送信ドメイン認証技術の普及に向けてのよいサイクルを生むためにも、ISP では積極的に受信時の認証およびラベリングを行うべきであり、受信したメールを適切に取り扱う努力を行っていることを、利用者・送信者へアピールしていくことが望まれます。

5.3.2　利用する送信ドメイン認証技術の選定

受信時に利用する送信ドメイン認証技術を選定する場合には､4.1.1 を参考にします。送信ドメイン認証技術を複数導入すれば、ドメインの正当性の判断に利用できる情報は増えますが、認証のために必要な追加コストが増加する場合があります。特に ISP の場合、取り扱うメールの通数が一般的な企業に比べ多くなりますので、機能を追加する設備の規模も大きくなると考えられます。現状のネットワーク構成やハードウェアを考慮しながら、段階的に送信ドメイン認証技術を導入していくことが現実的でしょう。

5.3.3　メールの配送制御

改めての説明になりますが、送信ドメイン認証技術は、あくまでも「特定の送信元から確かに送信されたかどうか」を機械的に判断するための技術であり、認証結果とメールのコンテンツは何の関係もないものです。ISP では多様な利用者にサービスを提供するという性質上、送信ドメイン認証技術での認証結果の取り扱いについては、特に慎重になるべきです。

5.3.3.1　配送前制御に関する注意

送信ドメイン認証技術による認証結果を利用した受信側のアクションで特に注意すべきなのが、認証結果による配送方法の取扱いです。4.1.3 で解説したとおり、送信ドメイン認証技術では、受信者の意図しないメーリングリスト経由での再配送や送信時ポリシーの記述ミスなどによって認証が失敗する場合もあります。特に、ISP ではさまざまな受信者による利用シーンが考えられるため、送信ドメイン認証技術による認証結果だけを利用して、一律にメールの受信を拒否したり破棄したりする取り扱いをしてはなりません。ただし、以下の場合にはこの限りではありません。

(a) 受信設備の高負荷による緊急避難など限定的対応の場合
(b) エンドユーザからの個別の同意がある場合

(b) による場合には､エンドユーザに対してリスクについて十分な説明を行うとともに、簡易に機能を解除させたり、個別に回

避できるような機能を設けるなどの機能的配慮もした上で、個別に同意を取って提供しなければなりません 。

5.3.3.3　ホワイトリストやドメインレピュテーションの活用

4.1.4.3 で示したとおり、送信ドメイン認証の結果と、ISP が事前に用意したホワイトリストやドメインの評判（ドメインレピュテーション）情報と照合することもできます。照合結果によって、メールに特別なマークを付与したり、迷惑メール判定を実施せずにフィルタを通過させたりするなどの活用方法が考えられます。また、サービスの利用者が個別にドメインを設定することにより、Web ブラウザや MUA 上でのフォルダ振分けなどに利用できるようにするサービス形態も考えられます。

ISP が他組織により提供されるホワイトリストやレピュテーション情報を利用する場合は、自組織のポリシーと一致しないことも十分に考えられるので注意が必要です。そのため、これらホワイトリストやレピュテーション情報は、自組織でコントロールができる権利もしくは機能を持つタイプのものでなければなりません。

5.3.3.4　認証結果の可視化による利用者のユーザビリティ向上

利用者が認識できるように認証結果の表示を行うためには、Web ブラウザ経由や MUA 経由など、表示領域を任意に制御できるような環境でメールを閲覧する必要があります。

一部の ISP では Web ブラウザ上でメールを利用できるサービスを提供していますが、このような環境の場合、画面インターフェース中に認証に利用したドメイン名や認証結果、ホワイトリストなどとの照合結果を分かりやすく表示させることが可能です。一方 MUA ではこのような画面表示に標準的に対応しているクライアントはまだほとんど存在していません。

送信ドメイン認証結果を分かりやすく表示するアプリケーション環境が整い、利用者が積極的に利用できるよう、ISP として可能な取り組みを推進することが好ましいといえます。

5.4　ユーザ周知

送信ドメイン認証を導入する場合には、導入した結果として発生する影響について、ユーザに周知する必要があります。周知の方法は、メールや郵便物で行う方法もありますが、最低限ホームページでの周知は実施するべきです。

なお、ユーザへの周知内容は、各社の対応内容によっても異なりますが、ユーザは送信ドメイン認証という技術の理解をすることが困難な場合も多いと想定されるため、表現方法や影響をよりわかりやすくする工夫が必要です。特に、「送信ドメイン認証技術」という表現にこだわらず、ユーザの理解を得られる表現を使うことも重要です。

5.4.1　送信側の対応

ユーザによるメールの利用方法により認証が失敗してしまう場合として、送信側では、ユーザが自社のサーバ（MSA）経由で送信アドレスを該当ドメイン以外で送信した場合と、ユーザが自社のサーバ以外のサーバから該当ドメインのメールを送信したケースの２つがあります。後者については、自社の管理外の問題であるため、ユーザに対して必ずしも説明する必要はないとも思えますが、前者と合わせて説明することが望ましいものです。

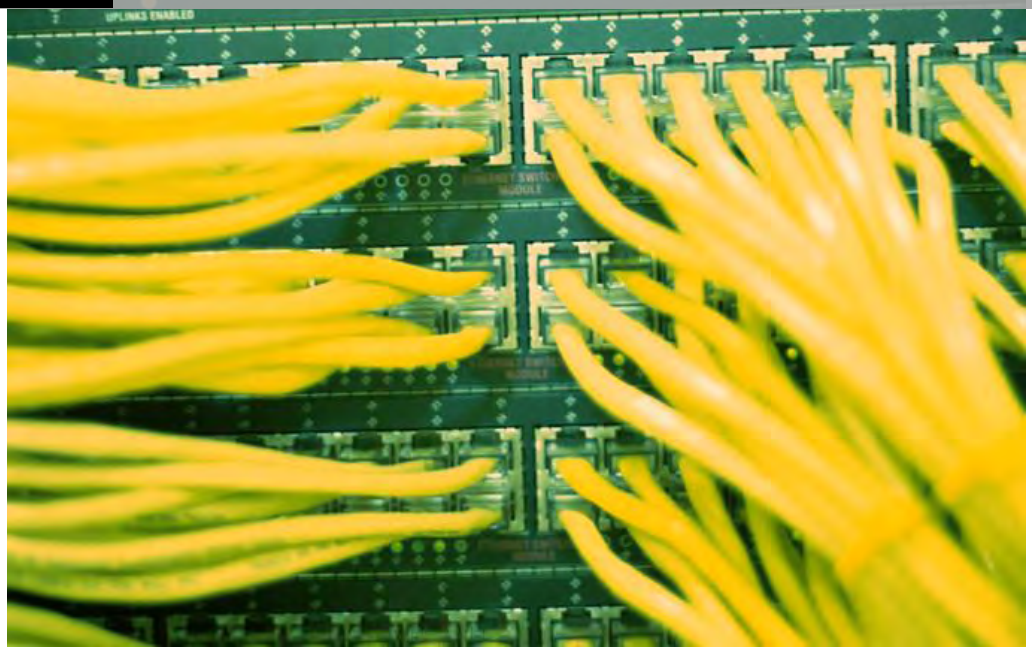
また、送信側の対応について、導入した技術と期待される効果を説明することが推奨されます。

5.4.2　受信側の対応

受信側の対応については、どの技術を採用しているかを説明する必要があります。

認証結果をラベリングとして記述する場合には、ラベリングの確認方法を、代表的なメールクライアントの設定方法について説明することが推奨されます。また、フィルタサービスを提供する場合には、該当のサービスの利用方法に加えて、利用した場合の影響について説明することが必要です。特に、ユーザにはドメイン詐称に対する認識が少ないため、どのような送信方法のメールがフィルタリングされるかを図解なども用いて説明することが推奨されます。

第６章　ホスティングサービスでの対応



第６章　ホスティングサービスでの対応

本章では、送信ドメイン認証技術を適用する際に、メールホスティングサービスを提供する事業者特有の対応方法、課題、解説などを示します。

サービス提供方法の違い、DNS サーバの管理の違いによるホスティングサービスの分類について、メールサービスに関連する DNS サーバについて、送信側・受信側の対応方法などについて、以下で解説します。

6.1　ホスティングサービスの分類

メールホスティングサービスとは、通信事業者や ISP・ASP 事業者（以下「ホスティング事業者」といいます。）が、自社設備を用いて、主に企業などにメール機能を提供するサービスです。このメールホスティングサービスは、メールサーバの割当てや DNS サーバの管理の状況により、それぞれ以下のように分類できます。

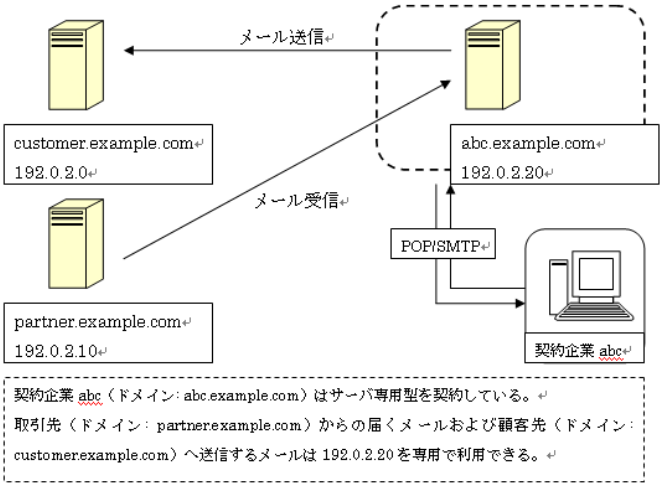
6.1.1　メールサーバによる分類

メールホスティングサービスは、メールサーバの割当てにより、「サーバ専用型」、「サーバ共用型」、「ゲートウェイ型」の 3 つに分類できます。

6.1.1.1　サーバ専用型

サーバ専用型は、１つの契約ドメイン（企業）に対して、１つ又は１つの集合体のメールサーバを「専用」で割り当てる形でメール送受信機能を提供するサービス形態です（図表６－１）。

割り当てられたメールサーバから送信されるメールは、すべて１つの契約ドメイン（企業）からのメールに限られます。

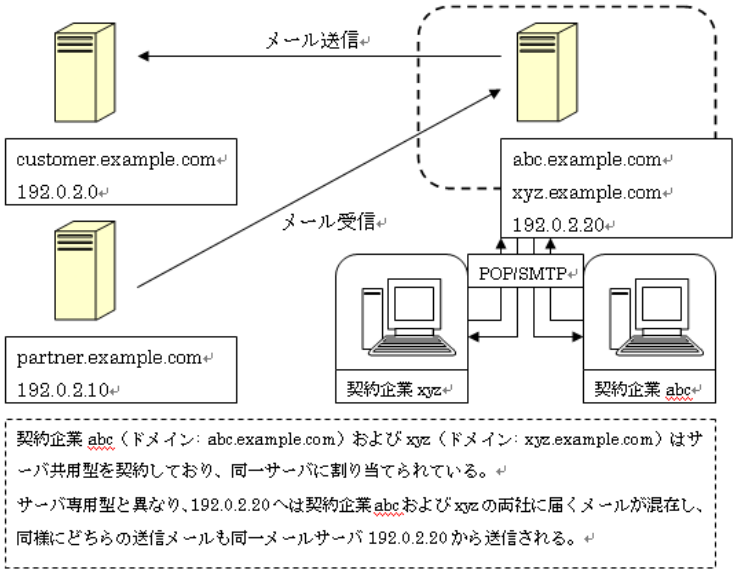


図表６－１　サーバ専用型のホスティング事業者の例

6.1.1.2　サーバ共用型

サーバ共用型は、複数の契約ドメイン（企業）に対して、１つ又は１つの集合体のメールサーバを「共用」で割り当てる形でメール送受信機能を提供するサービス形態です（図表６－２）。

専用型とは異なり、割り当てられたメールサーバから送信されるメールには、共用している他社ドメインからのメールも混在することになります。

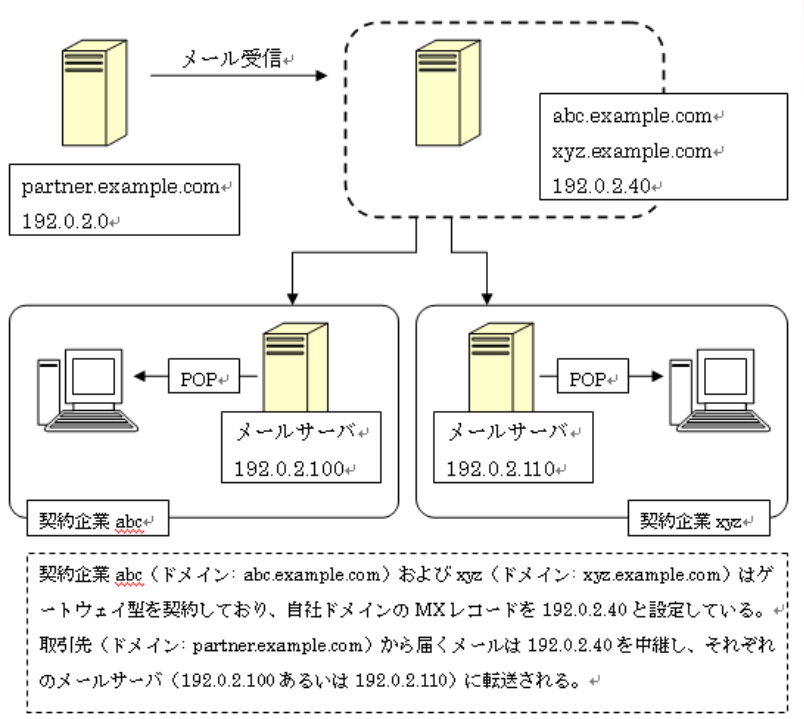


図表６－２　サーバ共用型のホスティング事業者の例

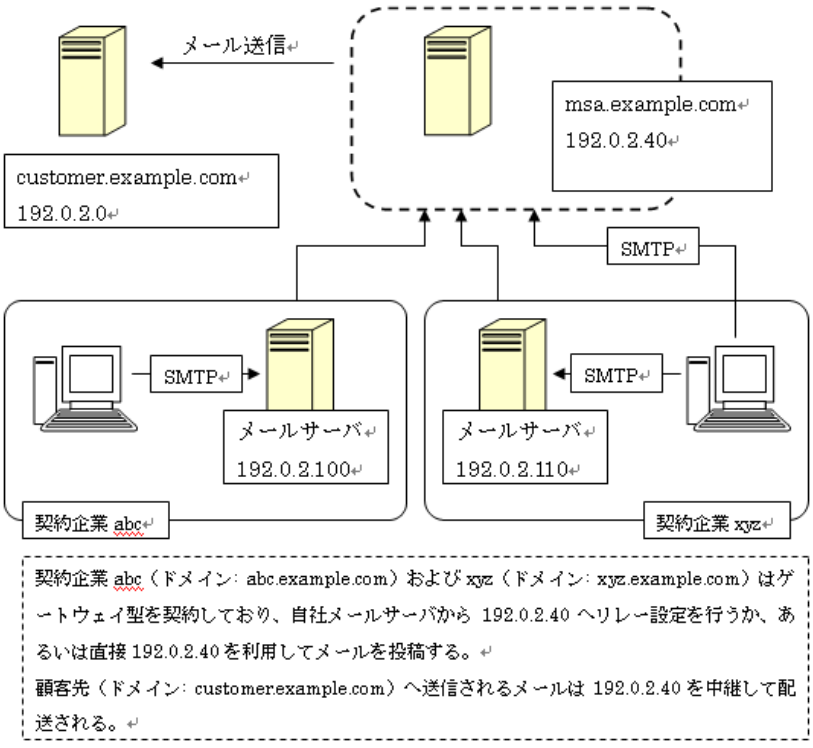
6.1.1.3　ゲートウェイ型

ゲートウェイ型は、契約ドメイン（企業）に対して、MX サーバやフィルタリングサーバ、投稿サーバを割り当てる形で、主に迷惑メール対策機能やウイルス対策機能、監査機能などを提供するサービス形態です（図表６－３、図表６－４）。

ゲートウェイ型のうち受信メールサーバの場合、ホスティング事業者はゲートウェイ用 MX サーバのみ提供し、メールデータを蓄積するメールボックス機能や投稿サーバなどの機能は提供しません。反対に、ゲートウェイ型のうち送信メールサーバの場合、契約企業のメールサーバが設定するリレー先サーバ（あるいは投稿サーバ）を提供し、MX サーバは提供しません。



図表６－３　ゲートウェイ型のホスティング事業者の例（受信）



図表６－４　ゲートウェイ型のホスティング事業者の例（受信）

6.1.2　DNS サーバによる分類

メールホスティングサービスは、DNS サーバの管理により、「DNS 自社管理型」、「DNS ホスティング型」、「DNS 提供型」の 3 つに分類できます。

6.1.2.1　DNS 自社管理型

DNS 自社管理型は、契約企業ドメインの DNS サーバを、契約企業自身で管理する形態です。ホスティング事業者は、契約企業のメールサーバは管理しますが、DNS サーバの管理（MX レコードや TXT レコードの登録・更新・削除）は行いません。

6.1.2.2　DNS ホスティング型

DNS ホスティング型は、契約企業ドメインの DNS サーバを、ホスティング事業者側が代行して管理する形態です。ホスティング事業者は、契約企業のメールサーバとともに DNS サーバの管理も行います。

6.1.2.3　DNS 提供型

DNS 提供型は、契約企業ドメインの DNS サーバのみをホスティング事業者が代行して管理する形態です。ホスティング事業者は、契約企業の DNS サーバは管理しますが、メールサーバの管理は行いません。

この場合には、DNS 自社管理型とも異なり、契約企業、メールサーバのみを管理するホスティング事業者、DNS サーバのみを管理するホスティング事業者の三者が登場します。

6.2　送信側の対応

ホスティング事業者は、契約企業が自社ドメインを差出人としてメールを送信する際に、SPF / Sender ID 及び DKIM に適合したメール送信環境を準備しなければなりません。

以下、 SPF / Sender ID の対応、 DKIM の対応について解説します。

6.2.1　SPF / Sender ID の対応

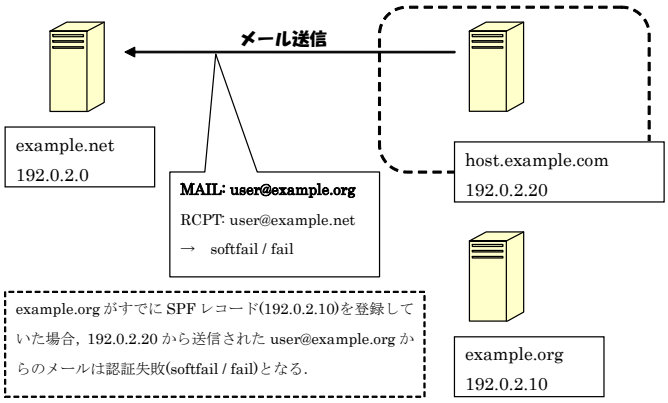
ホスティング事業者が送信側で SPF / Sender ID を導入する場合には、第４章で解説した一般的な対応のほか、以下のような事項についての対応を行わなければなりません。

6.2.1.1　SPF/SenderID 利用の確認

ホスティング事業者は、事前に SPF / Sender ID を利用することのメリットやデメリットを契約企業へ説明し、利用の確認を行わなければなりません。

例えば、4.1.3.4 で解説したとおり、契約企業が、登録したドメイン以外の差出人アドレスを用いてメール送信を利用している場合（図表６－５）には、SPF / Sender ID を利用することで認証結果が fail / softfail になる可能性があります。

説明内容については、第４章を参考にして、契約企業向けの説明資料を事前に準備することが推奨されます。



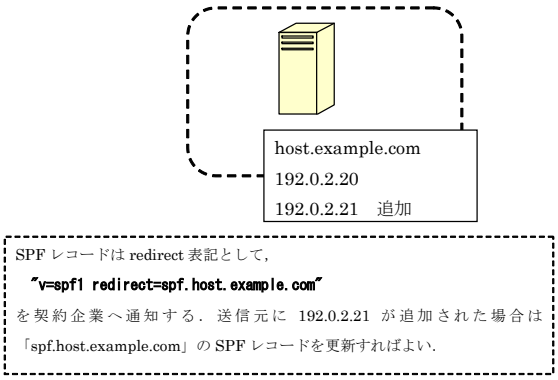
図表６－５　自社ドメイン以外のメール送信の例

6.2.1.2　SPF レコード登録に必要な情報の通知

DNS 自社管理型の場合には、SPF レコードの登録作業を契約企業自身が行わなければなりません。

この場合に、ホスティング事業者は、送信元となるIPアドレスなどの必要な情報を契約企業へ通知することが必要です。また、ホスティング事業者は、契約企業に対して、”redirect” で呼び出せるドメインなどを通知することが推奨されます（図表６－６）。送信元を IP アドレスで通知すると、IP アドレ

スの追加・削除のたびに、それぞれの契約企業に対して通知を行うことになりますが、”redirect” で呼び出せるドメインなどを通知することにより、IP アドレスの追加・削除があっても、通知しなくてもすむことになるためです。



図表６－６　SPF レコード (redirect) の利用例

また、ホスティング事業者は、契約企業に対して、”redirect” ではなく ”include” を用いて送信側のメールサーバを指定させることもできます。この場合には、契約企業側で認証結果の扱いをカスタマイズすることができます。

	特徴
redirect	契約ドメインに同一の SPF レコードを設定することができ、管理しやすい。
include	各契約企業ごとに認証結果のポリシーを変更することができる。

※ redirect, include については、3.2.4.2 を参照

図表６－７　SPF レコード(redirect, include)の特徴

6.2.1.3　SPF レコード登録のサポート

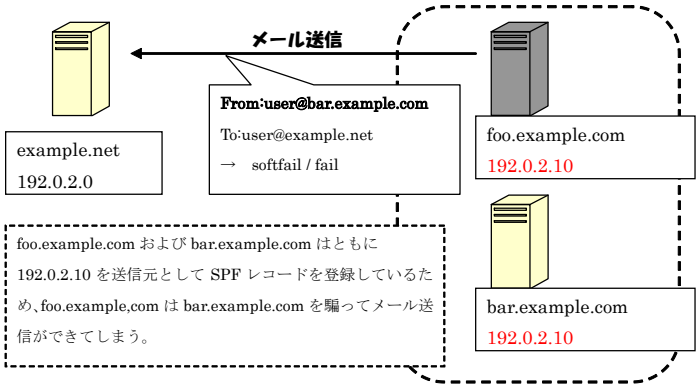
契約企業側の管理者がSPF レコードの記述方法に詳しくないことも考えられますので、DNS 自社管理型の場合には、ホスティング事業者は、SP F レコードの記述方法の説明や契約企業の要求に合った SPF レコードの作成準備を行うことが推奨されます。また、Appendix 1 で紹介している記述例や間違えの例を参考にして、契約企業側の SPF レコード登録をサポートすることが推奨されます。

6.2.1.4　サーバ共用型でのユーザ管理体制

サーバ共用型の場合には、ホスティング事業者は、契約ドメインの送信状況を随時監視しなければなりません。また、ホスティング事業者は、SPF / Sender ID の認証結果が pass とならないメールの送信を禁止したり、発信元 IP アドレスを分けるなどの対策をとる

ことが推奨されます。

これは、同一サーバに収容されているドメインの SPF レコードも同一となりますので、悪意のあるユーザがいた場合に、同一収容された契約ドメインの From ヘッダアドレスやリバースパスを騙って、正当なメールを送信することができてしまうためです（図表６－８）。



図表６－８　サーバ共用型でのなりすましメール例

また、サーバ共用型の場合では、同一サーバ（IP アドレス）に割り当てられた他社ドメインによって、SPF / Sender ID の認証結果が fail / softfail するメールを大量に送信されてしまい、その結果割り当てられたメールサーバが迷惑メールの送信元として認知されてしまう危険性があるためです。すなわち、他社ドメインのメール送信が、無関係である自社ドメインの送信メールに影響を及ぼし、最悪の場合は送信メールの不達が生じるものです（お隣さん問題）。

6.2.2　DKIM の対応

ホスティング事業者が送信側で DKIM を導入する場合には、第４章で紹介した一般的な対応のほか、以下のような事項についての対応を行わなければなりません。

6.2.2.1　DKIM 利用の確認

ホスティング事業者は、SPF / Sender ID の場合と同様に、事前に DKIM を利用することのメリットやデメリットを契約企業へ説明し、利用の確認を行わなければなりません。

例えば、契約企業が自社ドメイン以外の差出人アドレスを用いてメール送信に利用している場合には、電子署名を作成する際に利用したドメインと From ヘッダアドレスのドメインが一致しない可能性があります。

具体的な説明内容については、第４章を参考にして、契約企業向けの説明資料を事前に準備することが推奨されます。

また、電子署名を作成する際に利用したドメインと From ヘッダアドレスのドメインの違いによって、いくつかのサービス仕様が考えられますので（図表６－９）、ホスティング事業者は、契約企業の送信ポリシーと照らし合わせて実装を行うことが推奨されます。

	DKIM 利用方法	サービス仕様の例
1	すべての送信メールに電子署名を作成する方式	・From ヘッダアドレスが自社ドメインの場合は送信者署名となり、From ヘッダアドレスが自社ドメイン以外の場合は第三者署名となる
2	自社ドメインのメールだけに電子書名を作成する方式	・From ヘッダアドレスが自社ドメインの場合は送信者署名となりますが、From ヘッダアドレスが自社ドメイン以外の場合は、電子署名を作成しない ・どちらの場合もメール送信は許可する
3	自社ドメインのメールだけ送信を許可する方式	・From ヘッダアドレスが自社ドメインの場合は送信者署名となるが、From ヘッダアドレスが自社ドメイン以外の場合は、メール送信を許可しない

図表６－９　DKIM 利用方法とそのサービス仕様の例

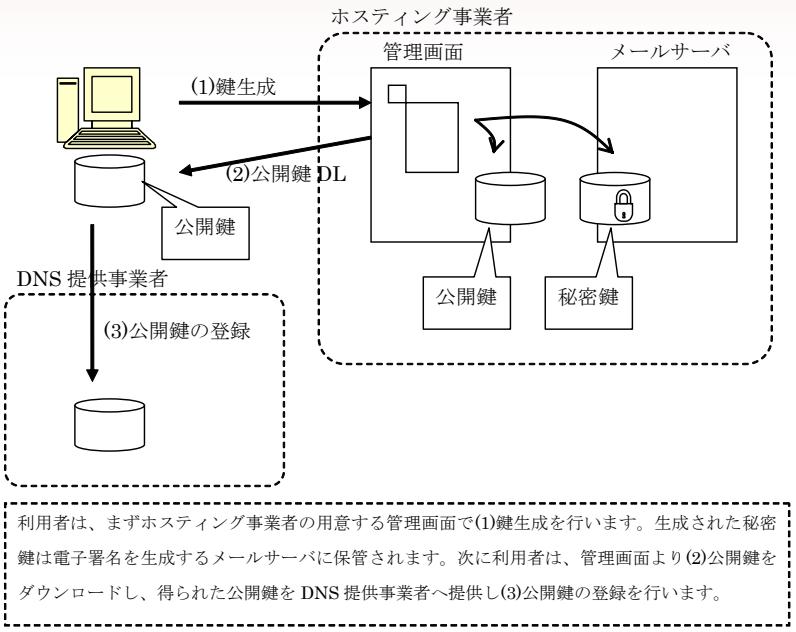
6.2.2.2　公開鍵の通知

DNS 自社管理型の場合には、公開鍵の登録作業は契約企業が行うことが必要です。ホスティング事業者は、公開鍵・セレクタなどの必要な情報を契約企業へ通知することが必要です。電子署名の解読行為を防止するために、定期的な公開鍵と秘密鍵の更新を行うことが推奨されますので、ホスティング事業者は、公開鍵と秘密鍵の更新のたびに、この手続を行うことが必要です。

6.2.2.3　公開鍵登録のサポート

DNS 自社管理型の場合には、契約企業側の管理者が公開鍵レコードに詳しくないことが考えられますので、ホスティング事業者は、公開鍵レコードの記述方法の説明や公開鍵レコードの作成準備を行うことが必要です。

また、DNS 提供型のように、メールサーバをホスティングする事業者と DNS をホスティングする事業者が異なる場合には、公開鍵と秘密鍵の管理方法が課題となります。ホスティング事業者は、ブラウザなどから操作できる管理画面などを用意し、公開鍵と秘密鍵の生成と、公開鍵のダウンロード機能を提供することが推奨されます（図表６－１０）。この機能を利用して、契約企業側の管理者は DNS 提供事業者への公開鍵提供と公開鍵の登録をすることができます。



図表６－１０　ホスティング事業者の提供する公開鍵と秘密鍵の管理システムの例

6.3　受信側の対応

ホスティングサービスでは、ホスティング事業者の設備で受信側の対応を行うことが必要です。第３章で紹介した一般的な対応のほか、以下のような事項についての対応を行うことが必要です。

6.3.1　認証結果の解説と利用方法の提示

送信ドメイン認証技術による認証結果を Authentication-Results ヘッダに記録する場合には、契約企業に対して Authentication-Results ヘッダに関する説明を行い、必要であればメールクライアント側での適切なフィルタリングの指導を行うことが必要です。

ホスティング事業者は、第３章を参考にした説明資料を準備することが推奨されます。

6.3.1.1　判定結果の確認

契約企業にフィルタリングの指導をする準備として、該当ドメイン宛の受信メールのうち、適切に送信ドメイン認証が実施された割合を調査します。受信メールの多くが fail / softfail と判定されているドメインのうち、契約企業とやり取りをされている顧客が含まれる場合は、フィルタリングのホワイトリスト対象を講じることが考えられます。この場合には、該当するドメインをリスト化して、契約企業に確認してもらうことが推奨されます。

受信メールの多くが neutral / none と判定されている契約企業の場合は、フィルタリングによる効果が低いため、この指導は見送ることが推奨されます。

6.3.1.2　契約企業への説明とメールクライアント側へのフィルタリング指導

契約企業に対して、契約ドメイン宛の受信メールの判定結果及びフィルタリングによって得られる効果を報告します。ホスティング事業者は、メールクライアント側で設定すべきフィルタリング条件の設定をサポートするとよいでしょう。

6.3.2　認証結果によるフィルタリング実施

メールクライアント側のフィルタリングでは、ホスティング事業者の設備コストは直ちに効果がでるとはいえませんが、今後送信側の対応が進むとエンドユーザ側での様々な活用が進むと予想されております。

ホスティング事業者は、メールの隔離、拒否、破棄などのサーバ側でのフィルタリング機能を準備することが推奨されます。サーバ側のフィルタリング機能を実装するにあたっては、以下の点について考慮することが必要です。

6.3.2.1　フィルタリング利用を選択できる機能の提供

特にサーバ共用型の場合には、フィルタリング機能を利用する契約企業と利用しない契約企業が共存する場合が想定されますので、ホスティング事業者は、契約ドメインごとにフィルタリング設定の有効・無効を管理する

ことが必要です。

6.3.2.2　ドメイン単位のホワイトリスト機能の提供

6.3.2.1 で解説したとおり、送信元ドメインによってはすべてのメールの送信元に対して送信ドメイン認証技術に対応していない場合があります。言い換えれば、認証結果が fail / softfail であっても受信すべき送信元ドメインが存在することになります。このため、ホスティング事業者は、各契約ドメインごとに、ホワイトリスト機能を提供し、必要なメールの不達を防ぐことが必要です。

6.3.2.3　なりすましメールの措置を選択できる機能の提供

フィルタリング結果で送信者情報が偽装されているメール（なりすましメール）であると判定された場合には、それらのメールは何らかの措置（隔離、ラベリング、拒否等）がとられることが推奨されます。ホスティング事業者は、このような措置として複数の選択肢を用意し、契約企業にリスクと効果をかんがみて、設定してもらうことが推奨されます。ホスティング事業者の用意する措置としては、以下のようなアクションが考えられます。

	仕様	特徴
ヘッダに目印を記録	X ヘッダ又は Subject ヘッダなどになりすましと認識できる目印を記録する	・受信すべきメールの不達を防止することができるが、契約企業のユーザがメールクライアントでフィルタリング設定をする手間が生じる
隔離して受信	ごみ箱や迷惑メールボックスなど、受信箱とは別の場所に受信する	・受信すべきメールの不達を防止することができるが、隔離されていることで False Positive が発生した場合にユーザが受信を見落とす可能性がある ・ゲートウェイ型では提供できない
SMTP で拒否する	なりすましメールと判定された時点で、SMTP 応答で該当メールを拒否する	・なりすましメールが契約企業のユーザに着信しなくなるが、ホワイトリストが適切に設定されていない場合には、メール不達が生じる
NDR をメールサーバで破棄	なりすましメールと判定されたメールのうち、NDR については SMTP レスポンスを正常応答したのち、メールサーバ内で破棄する	・不要な NDR によるコストが軽減されるが、通常のメールについては他の施策と組み合わせて実装する必要がある

図表６－１１　なりすましメールの措置の例

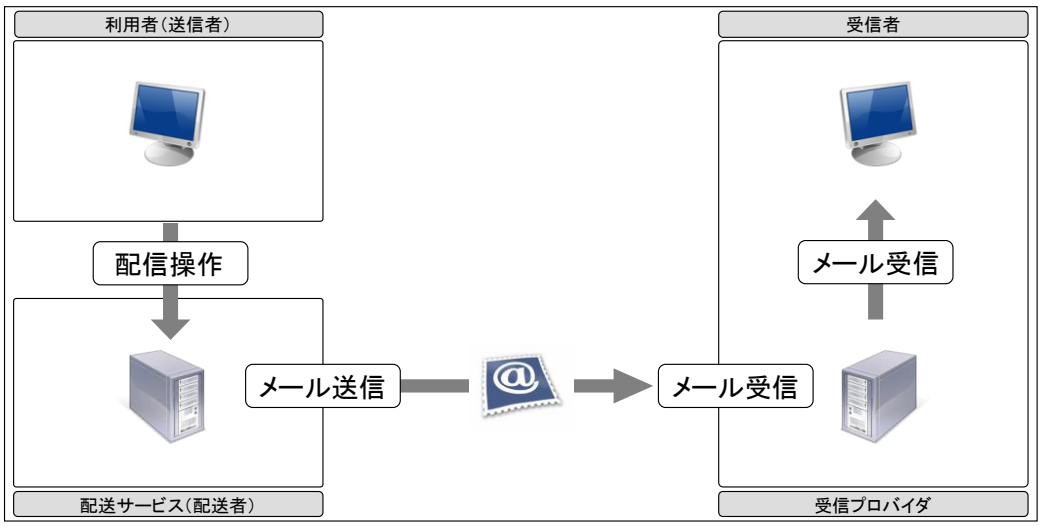
第1章　配信サービスでの対応

第７章　配信サービスでの対応

本章では、配信サービスを利用してメールを送信する送信者（配信サービス利用者。以下この章で「利用者」といいます。）と、クライアント組織に代わってメール送信する実際の配送者（配信サービス提供者。以下この章で「配信サービス」といいます。）が、送信ドメイン認証を導入する上で、対応すべき事項を説明します。

7.1　配信サービスとは

配信サービスとは、電子メール配信のための設備を備えた業者が当該設備を利用して、クライアント組織に代わってメールを配信するサービスを指します。



図表７－１　配信サービス　概要

7.1.1　配信サービスと送信ドメイン認証技術

メールの配信設備を保有していない組織が、配信サービスを利用して一般消費者や顧客にメール配信する場合には、From ヘッダアドレスにその組織のドメイン（利用者ドメイン）のメールアドレスを指定しながら、配信サービス環境から送信することになるため、受信者から送信者情報を偽装したメール（なりすましメール）であると勘違いされかねません。

配信サービスは、配信するメールに送信ドメイン認証技術を導入することにより、受信者に対して自ら配信したメールであることを証明することができます。

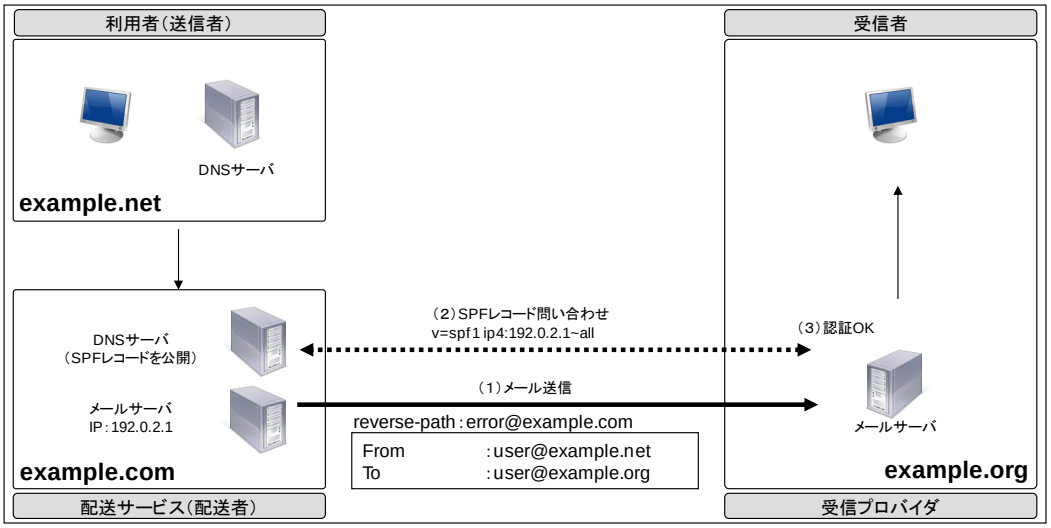
今後、送信ドメイン認証技術が普及するとともに、ホワイトリストの普及が本格化する可能性があります。この場合、配信サービスは、送信ドメイン認証技術を施した

送信メールから迷惑メールを削減する努力を継続することで、結果として、自らのドメインの評判を上げることができます。

配信サービスは、専門的な知識や技術を持たない利用者が送信ドメイン認証技術を導入するための道を拓き、社会全体のなりすましメールや迷惑メールの削減に貢献できる立場にありますので、積極的に送信ドメイン認証に対応することが望まれます。

7.1.2　From ヘッダアドレスの管理主体

配信サービスを利用する際は、主に利用者の管理するドメインの From ヘッダアドレスで送信する場合と、配信サービスが管理するドメインの From ヘッダアドレスで送信する場合があります。それぞれの場合によって、送信ドメイン認証技術の利用時の対応が異なりますので、導入する際には、あらかじめ From ヘッダアドレスの管理主体を確認しておくことが必要です。



図表７－２　SPF（From ヘッダアドレスのドメインが利用者管理の場合）

7.2　送信ドメイン認証技術の導入

配信サービスから送信ドメイン認証技術に対応したメールを送信する際に、配信サービスと利用者が対応すべき事項は、以下のとおりです。

7.2.1　SPF

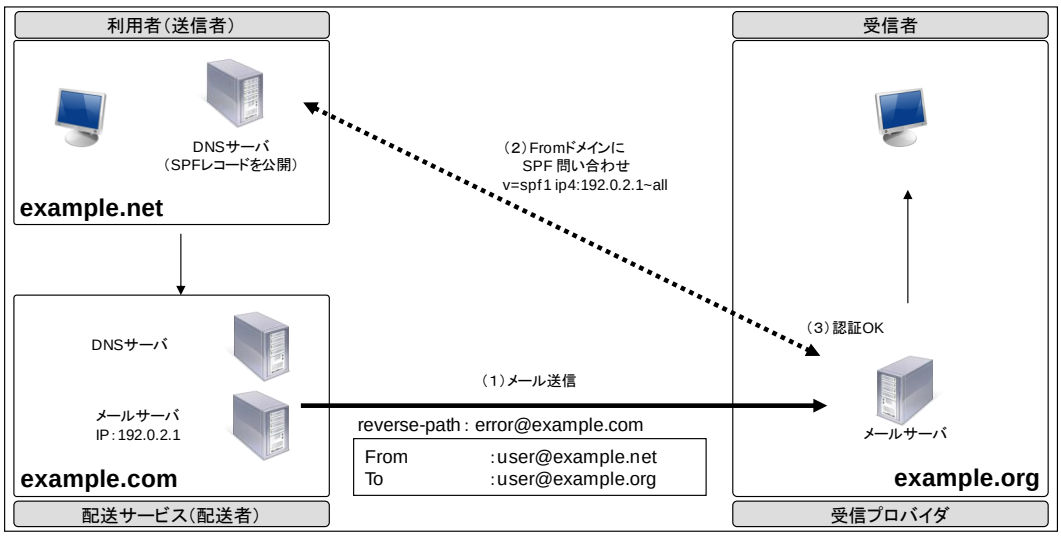
SPF は、送信するメールのリバースパスのドメインで認証します。配信サービスでは、一般にエラーメール解析等のバウンスメール処理のために、リバースパスには配信サービスのドメインのメールアドレスが指定されます。この場合に、配信サービスは、リバースパスで使用するドメインの DNS に SPF レコードを公開することになります。このとき、利用者が対応する事項はありません。

7.2.2　SenderID

Sender ID 認証は、PRA を用いて認証を行います。このため、メールヘッダに Sender を使用しているかいないかで対応内容が異なります。Sender は省略されることが多いヘッダですが、メール作成者が複数存在する場合や、From ヘッダアドレスと実際の配送者が異なる場合に用いられます。From ヘッダアドレスに利用者ドメインのメールアドレスを指定してメールを配信する場合は、実際の配送者である配信サービスの情報を Sender に記載することができます。

7.2.2.1　メールヘッダに Sender を使用しない場合

メールヘッダに Sender を使用しない場合には、Sender ID での認証の対象は、PRA に基づき、From ヘッダアドレスとなります。



図表７－３　SenderID/Sender 使用せず
（From ヘッダアドレスのドメインが利用者管理の場合）

7.2.2.1.1　From ヘッダアドレスのドメインが利用者管理の場合

From ヘッダアドレスのドメインが利用者管理の場合には、利用者、配信サービスは、それぞれ、次の対応が必要です。

(1)　利用者の対応

利用者は、利用者が管理するドメインの DNS の SPF レコードに配信サービスの送信ドメイン情報を記載します。

(2)　配信サービスの対応

配信サービスは、送信時に利用者が指定する From ヘッダアドレスのドメインの SPF レコードに問い合わせ、正しい送信元情報が記載されていることを確認し、正しくない場合は警告を出す、送信しない等の対応を行うことが推奨されます。

利用者が SPF レコードに配信サービスの送信ドメイン情報を誤って記載したことにより、受信側の検証結果が fail になった場合には、その検証結果が受信ブロックの原因となる可能性があり、この状況が継続することによって、同じ IP アドレスから送信される他の利用者のメールが届きにくくなる可能性がありますので、注意が必要となるものです。

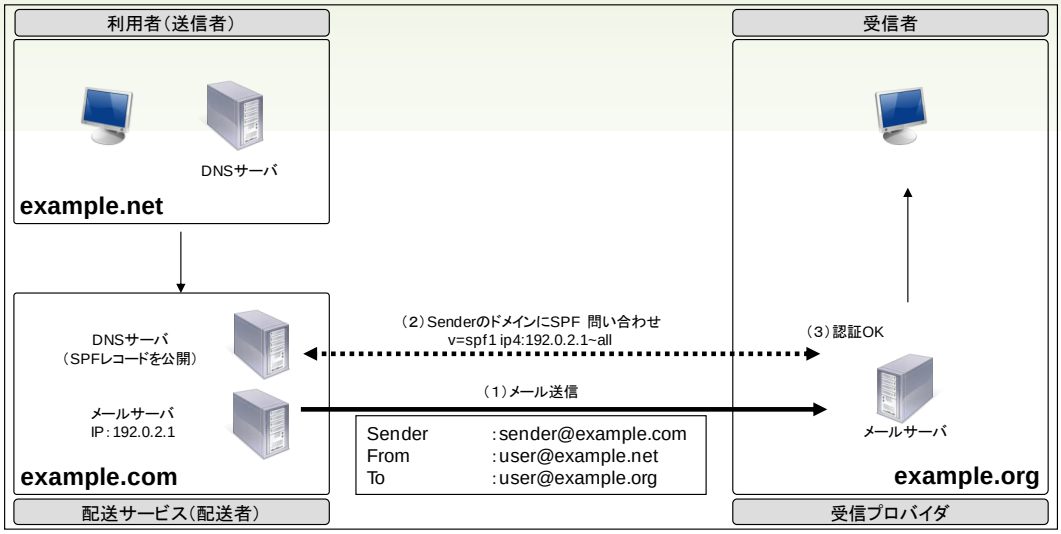
7.2.2.1.2　From ヘッダアドレスのドメインが配信サービス管理の場合

From ヘッダアドレスのドメインが配信サービス管理の場合には、配信サービスで、配信サービスが管理するドメインの DNS の SPF レコードに配信サービスの送信ドメイン情報を記載します。

7.2.2.2　メールヘッダに Sender を使用する場合

メールヘッダに Sender を使用する場合には、PRA に基づき、Sender ID の認証対象は Sender となります。Sender には、実際の配送者である配信サービスのドメインを記載します。したがって、配信サービスは、Sender で使用するドメインの DNS の SPF レコードに、配信サービスの送信ドメイン情報を公開します。

利用者が対応する事項はありません。



図表７－４　SenderID/Sender 使用
（From ヘッダアドレスのドメインが利用者管理の場合）

7.2.3　DKIM

DKIM は、DKIM-signature ヘッダに記載されたドメインで認証します。

DKIM は送信者署名を基本とし、From ヘッダアドレスのドメインが利用者管理であるか配信サービス管理であるかによって異なる対応が求められるため、配信サービスは、あらかじめ From ヘッダアドレスの管理主体を確認しておく必要があります。

7.2.3.1　From ヘッダアドレスのドメインが配信サービス管理の場合

From ヘッダアドレスのドメインが配信サービス管理の場合には、配信サービスのドメインで電子署名を作成します。

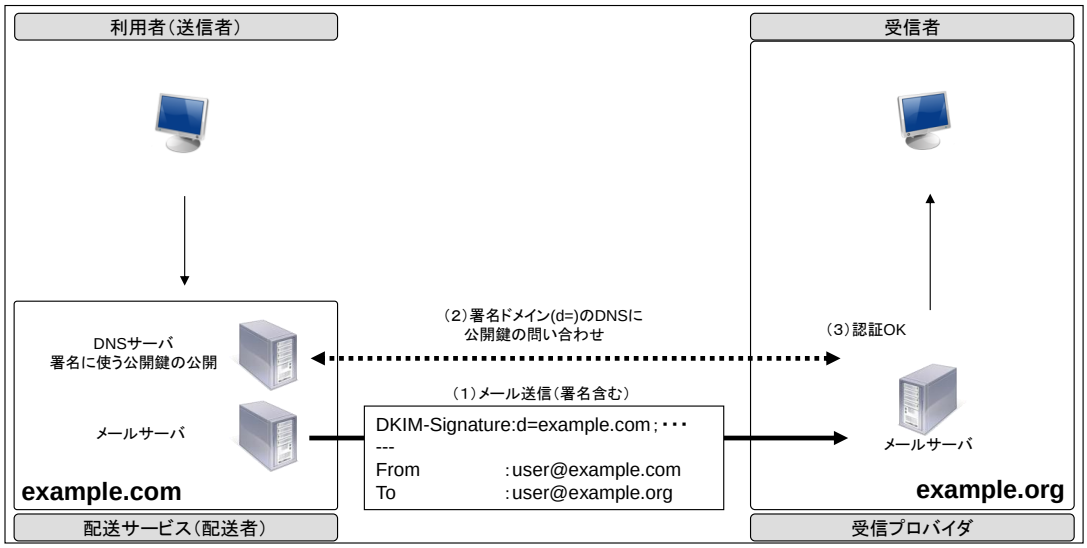


図７－５　DKIM／配信サービスドメインによる署名

(1)　配信サービスの対応

　配信サービスは、From ヘッダアドレスに使用するドメインの DNS に公開鍵を設置し、これに対応する秘密鍵で DKIM の電子署名を作成するソフトウェアを用意する必要があります。

(2)　利用者の対応

　利用者が対応する事項はありません。

7.2.3.2　From ヘッダアドレスのドメインが利用者管理の場合

　利用者が管理するドメインの From ヘッダアドレスで配信する場合は、利用者自らが管理する DNS へ公開鍵を設置して、電子署名を作成することが望まれます。

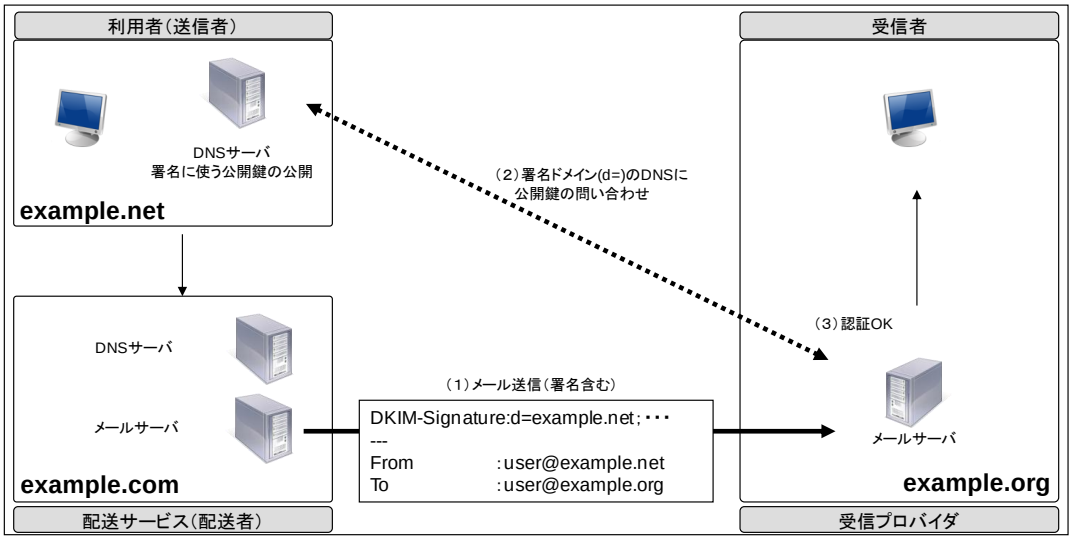


図７－６　DKIM／利用者ドメインによる署名

(1)　配信サービスの対応

　配信サービスは、送信メールに DKIM 署名したい利用者の鍵の管理やドメインの管理を軽減するために、以下のような環境を提供することが推奨されます。

(a)　鍵管理の支援

　DKIM を利用したい利用者の中には、DNS の管理や鍵の設置が可能な担当者もいれば、困難な担当者もいます。こういった様々な利用者が幅広く DKIM を利用してメールを配信するために、配信サービスは、配信サービス側で秘密鍵と公開鍵を生成して利用者に公開鍵を提供する等、以下の機能を用意することが推奨されます。

・　公開鍵ダウンロード機能

　利用者がメールを送信する場合には、利用者の鍵管理の負担を軽減する為に、あらかじめ From ヘッダアドレスに使用するドメインを申請してもらい、当該ドメインに対して電子署名の作成に使用する鍵を生成

し、利用者のドメインの DNS に設置するための公開鍵をダウンロードする画面を用意します。

(b)　鍵管理と DNS 管理の支援

利用者の鍵管理の負担の軽減に加えて、DNS の管理の負担を軽減するために、配信サービスが送信者のドメイン又はサブドメインの DNS 管理を代行し、鍵とドメインの管理を併せて代行するといったサービスを提供することも有効です。

(2)　利用者の対応

電子署名の作成用の公開鍵を DNS に設置することが可能な場合は、配信サービスから提供されるなどして用意した公開鍵を DNS に設置します。

※　From ヘッダアドレスのドメインの DNS サーバの管理をホスティング事業者に委託していて、当該事業者が公開鍵の設置に対応していない場合には、送信者署名は利用できません（受信者は電子署名を正しく検証できません）。

7.3　配信サービスによる利用者への周知

配信サービス提供者は、導入している送信ドメイン認証技術、及び利用者が対応すべき事項等の情報を Web サイト等に公開することが推奨されます

第８章　利用者への周知

第８章　利用者への周知

メールを利用する際に、多くのエンドユーザはメールのなりすましを意識することは少ないと想定されます。しかし、エンドユーザが意識しないところで、送信ドメイン認証技術による影響を受ける可能性があります。

本章では、エンドユーザに、最低限意識して欲しいことについて解説します。

8.1　送信ドメイン認証技術とは

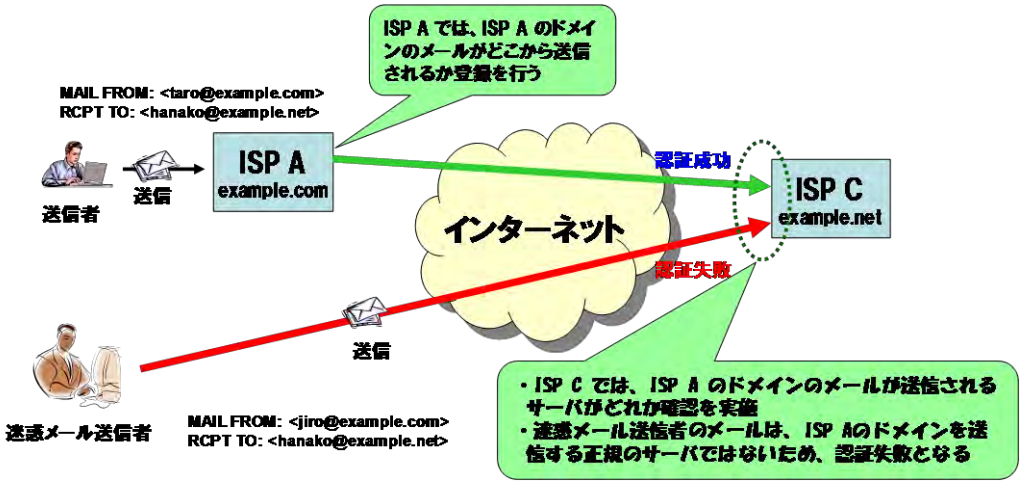
送信ドメイン認証技術とは、受信者が受け取ったメールについて、送信者情報が詐称されているかどうかをドメイン単位で確認可能とする技術です。

メールを普通郵便に例えるならば、送信ドメイン認証技術を用いたメールは、書留郵便のようなものと考えることができます。ただし、決定的な違いは、郵便では、送信者が書留を意識して送信するのに対して、送信ドメイン認証技術では、送信側の該当ドメインのドメイン管理元で送信ドメイン認証技術を導入すれば、送信者が意識しなくても、送信ドメイン認証技術に対応したメールとなることです。

しかし、書留郵便と異なり、送信ドメイン認証技術では、たとえ送信側で送信ドメイン認証技術を導入しても、受信側が対応していなければ、そのメールは、送信ドメイン認証技術に対応したメールとして受信されません。

エンドユーザは、各 ISP / ASP が提示する設定方法にしたがって利用していれば、意識しなくても、基本的には問題が発生することはありません。しかし、自分が利用しているメールについて、送信ドメイン認証技術を意識しないと問題が発生する場合もあるため、これらについて、以下で説明いたします。

なお、各 ISP / ASP が提供する迷惑メール対策のサービスには、本技術を用いたものも存在するため、迷惑メールに困っている場合は、サービスの内容を確認することも重要です。



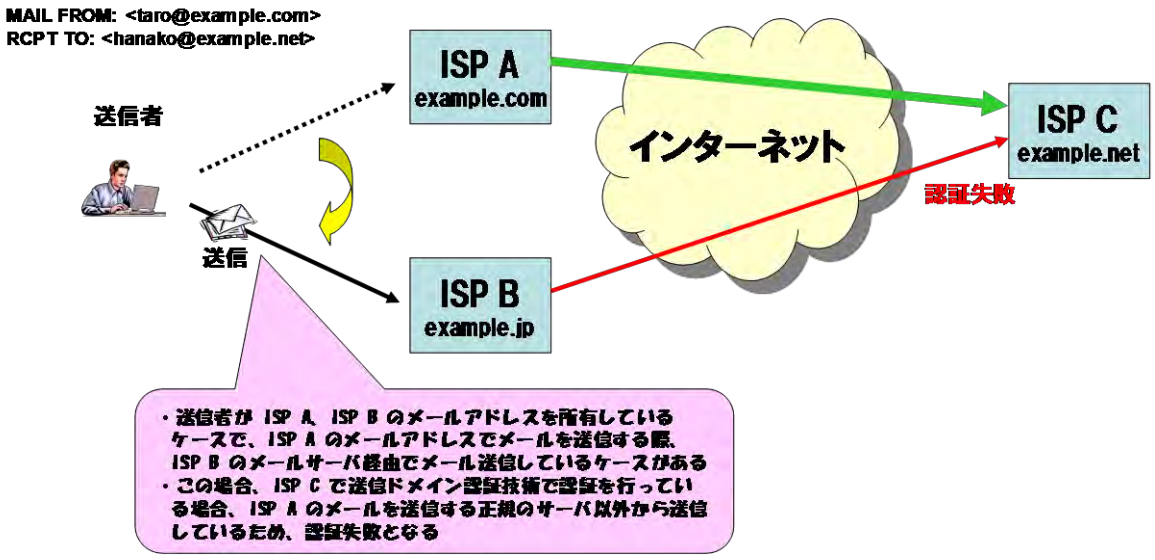
図表８－１　送信ドメイン認証技術の概要

8.2　送信時の注意事項

多くのエンドユーザは、メールの送信時に、送信に用いるメールアドレスを偽装する（なりすます）ことはないと想定されます。しかし、会社などのアドレスを用いて、自宅から自分が契約している ISP 経由で送信すること等も想定されます。そのような送信方法は、厳格な管理を行う企業などでは禁止している場合が多いと想定されますが、実際にはメールクライアントソフトの設定を変更するだけで送信可能な場合もほとんどであり、事実としてこの利用方法は多数利用されているのが現実です。

このような場合に、送信に用いたメールアドレスのドメインが送信ドメイン認証技術に対応している場合、そのメールはそのドメインのメールを許可されているサーバ以外からの送信となり、受信側でも送信ドメイン認証技術に対応していると、そのメールは送信者情報を偽装した（なりすました）したメールと判定されます。仮にそう判定されると、受信側の機能によっては、該当のメールがフィルタリングされ、受信者に到達しない場合もあります。

したがって、このような方法でのメール送信は行わないことが賢明です。なお、このような事態を回避するために、一部のメールクライアントでは、”Sender アドレス” というものが設定できます。



図表８－２　外部メールサーバ利用時の注意事項

8.3　受信時の注意事項

送信ドメイン認証技術で認証されたメールは、あくまでも、送信されたメールアドレスのドメインのメールを許可された送信されたことが確認されているだけですので、その内容まで信頼できる訳ではありません。したがって、送信されたメールの内容や送信者のアドレスを見て、問題ないメールか判断することが重要です。そのため、迷惑メール対策として利用する場合には、内容に基づくフィルタリングサービスなど、他のサービスと組み合わせて活用することが重要です。

迷惑メールの対策として、一部の ISP では、送信ドメイン認証技術を用いたフィルタサービスを提供しています（サービスの名称としては、「なりすましフィルタ」など、別の名称が用いられていることもあります。）。迷惑メールの多くは、送信者情報を偽装している（なりすましている）ため、このフィルタが提供されている場合には、利用者側でも、積極的に導入することが推奨されます。

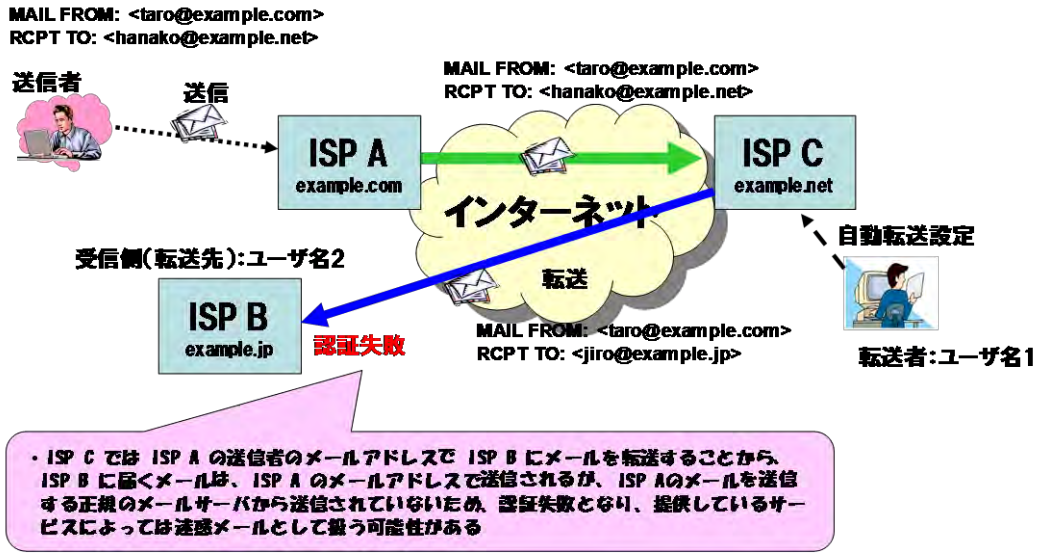
しかし、特別の使い方をする場合には、 8.2 で解説した問題のほか、 8.4 で解説するメール転送の課題などもあるため、場合によっては、その利用方法について注意が必要です。多くの ISP では、回避策を準備していることが多いため、利用の際は、利用している ISP の説明を確認することが推奨されます。

ただし、多くのエンドユーザは、特別な使い方をすることはないと考えられますので、基本的には、そのようなことを意識する必要はないと思われます。

8.4　メール転送時の注意事項

メールを転送する場合には、転送元のアドレスは、最初のメールの送信者のアドレスになるのが一般的です。このため使っているドメイン認証技術によっては、メールの転送が行われる場合に、受信側で送信ドメイン認証技術による確認をする場合に、送信者情報（転送元のアドレス）と送信に用いられたメールサーバ（転送者のサーバ）が異なることになるので、結果として、送信者情報を偽装した（メールアドレスをなりすました）メールを送信したことと同じことになってしまい、転送先の送信ドメイン認証のフィルタを利用している場合などには、転送したメールが届かなくなってしまいます。

したがって、メール転送を行う場合には、転送先のサービスが送信ドメイン認証技術を採用しているか、メール転送時にどのようなアドレスを使っているか等を確認する必要があります。送信ドメイン認証技術を用いたフィルタを提供している多くのサービスでは、ホワイトリストのように、無条件で受信を許可する設定を可能にしており、事前に確認したアドレスをホワイトリストに登録すること等により、フィルタで拒否されなくすることも可能です。利用の際は、具体的な設定の方法等について、利用している ISP の説明を確認することが推奨されます。



図表８－３　メール転送時の注意事項

Appendix 1. SPF レコードの記述例

Appendix 1. SPF レコードの記述例

本節では、SPF レコードの記述例について説明します。

Appendix 1.1 SPF レコードの例

SPF レコードは、記述ミスを防ぐため、なるべく簡潔に記述するよう心がけましょう。また、簡潔に記述することが、受信側での認証処理の負荷を軽減することにもつながります。

include や redirect、またマクロの機能等は、間違えを起こしやすいので、本当に必要な場合にのみ利用し、ip4 や ip6 の記法で簡潔に記述することを推奨します。

Sample 1: ホストの IP アドレスで記述

メールを外部に送出するメールサーバの IP アドレスを直接指定します。送信メールサーバの数があまり多くない場合には、記述ミスを防ぐためや、受信側での DNS クエリを抑制するために、この記述方法を強く推奨します。

```
example.org.    IN      TXT     "v=spf1 ip4:10.0.3.1 ip4:10.0.3.2 ip4:10.0.3.3 -all"
```

Sample 2: ホスト名で記述

メールを外部に送出するメールサーバのホスト名を指定します。Sample 1 の IP アドレスを直接指定する方法に比べて、メンテナンスが簡単ですが、受信側の認証処理で DNS への負荷が少し増える可能性があります。ホスト名は、必ず FQDN で指定します。

```
example.org.    IN      TXT     "v=spf1 a:mx01.example.org a:mx02.exmaple.org a:ns.example.org -all"
```

Sample 3: ネットワークでの指定

メールを送出する可能性のあるホストが存在するネットワークを、CIDR 方式で指定します。CIDR にあまり小さい値を指定すると（つまりネットワークの領域をあまり広く指定すると）、SPF レコード自体の意味がなくなるため、最小限のネットワーク範囲で利用します。

```
example.org.    IN      TXT     "v=spf1 ip4:10.0.4.0/28 -all"
```

Sample 4: ホストの IP アドレスとネットワークアドレスの混在

Sample 2 のホストの IP アドレスの指定と Sample 3 のネットワークの指定とを混在させることも可能です。

```
example.org.    IN      TXT     "v=spf1 ip4:10.0.3.0 ip4:10.0.3.1 ip4:10.0.3.2 ip4:10.0.4.0/28 -all"
```

Sample 5: MX に指定したホストを利用

MX に指定したホストからしかメールを外部に送出しない場合は、mx を利用します。メンテナンスが楽であり、記述ミスの発生を防ぐことができます。ただし、受信側での認証処理でやや DNS への負荷が大きくなる可能性があります。

```
example.org.    IN      TXT     "v=spf1 mx -all"
```

Sample 6: メールを送信しないドメイン

管理しているドメインがまったくメール送信しない場合は、"-all" を利用して、その旨を公開できます。

```
example.org.    IN      TXT     "v=spf1 -all"
```

Sample 7: サブドメインに個別の SPF レコードを定義する

顧客へのアナウンスメールやキャンペーンメールを外部業者に委託しているような組織の場合では、それらの配信メールの送信元サーバの IP アドレスを SPF レコードに追加する必要があります。しかし、外部業者が多数に上る場合など、レコードの管理が複雑になることが考えられるので、可能であれば、それらの業者ごとに専用のサブドメインを払い出して、本来の業務用のドメインと切り離して管理するという方法もあります。業者が既に SPF レコードを公開していれば、include を利用してそのレコードを利用できます。ただし、 include する場合、参照先の SPF レコードに記述ミスがあったり、include や、 redirect で、参照元を相互参照していたりしないか十分に確認した上で行います。

```
example.org.                IN      TXT     "v=spf1 ip4:10.0.3.0 ip4:10.0.3.1 ip4:10.0.3.2 -all"
announce.example.org.       IN      TXT     "v=spf1 ip4:10.1.4.0 ip4:10.1.4.1 -all"
campaign.example.org.       IN      TXT     "v=spf1 include:example.net -all"
```

Sample 8: redirect を利用してマルチドメイン環境での記述を簡略化する

１つの企業でも複数のドメインを利用している場合や、複数のドメインのメールで１つのメールシステムを共有する場合には、redirect を利用して共有化を図ることで、メンテナンスの負荷を軽減し記述ミスを防ぐことが考えられます。ただし、参照先が必ず存在するように注意し、また、相互に参照して参照のループを起こすことのないように、参照先のレコードでは include や redirect を利用しないようにします。

```
example.org.    IN      TXT     "v=spf1 ip4:10.0.3.0 ip4:10.0.3.1 ip4:10.0.3.2 -all"
example.net.    IN      TXT     "v=spf1 redirect=example.org"
example.com.    IN      TXT     "v=spf1 redirect=example.org"
```

Sample 9: 大きなレコードを複数の文字列で記述する

通信事業者や大きな組織ではメールサーバの数が多く、SPF のレコードのサイズが大きくなる可能性があります。SPF の RFC において、1 つの TXT レコードでは複数の文字列を含むことが可能であり、１つの文字列の最大長は 255 バイトであると説明されています。１つの TXT が複数の文字列で構成されている場合には、認証を実施する受信側では、その文字列はすべてつなぎ合わせして１つの文字列として評価します。ただ、複数の文字列を１つの文字列に連結するときに、つなぎ目に空白文字は挿入されないので注意が必要です。

```
example.org.    IN      TXT     "v=spf1 ip4:10.0.3.0 ip4:10.0.3.1 ip4:10.0.3.2" " ip4:10.0.3.3 ip4:10.0.3.4
ip4:10.0.3.5" " include:example.net -all"
```

Sample 10: 大きなレコードをサブドメインを利用して記述する

RFC では、連結した後の１つのレコードが 450 バイト以下であることが目安とされています。DNS のクエリに対するレスポンスが全体で 512 バイト以下でないと DNS のクライアントが無視する可能性があるからです。450 バイトを超えるような長いレコードを記述するのはあまり勧められませんが、どうしても必要な場合は、サブドメインを定義してそれらにレコードを分割して記述した上で、それらを include するような対応が必要です。繰り返しますが、相互参照やループの発生を防ぐため、include 文を利用する場合、参照先ではなるべく include 文や redirect 文を利用しないようにします。

```
example.org.    IN      TXT     "v=spf1 include:_spf-a.example.com include:_spf-b.example.com
include:_spf-c.example.com -all"
   _spf-a.example.org.   IN TXT "v=spf1 ip4:10.0.3.0 ip4:10.0.3.1 ip4:10.0.3.2 ip4:10.0.3.3 -all"
   _spf-b.example.org.   IN TXT "v=spf1 ip4:10.0.5.0 ip4:10.0.5.1 ip4: 10.0.5.2 ip4: 10.0.5.3 -all"
   _spf-c.example.org.   IN TXT "v=spf1 ip4:10.0.7.0 ip4: 10.0.7.1 ip4: 10.0.7.2 ip4: 10.0.7.3 -all"
```

Appendix 1.2 SPF レコードの間違い例

文法的に間違った SPF レコードを公開すると、受信側では permerror と扱われ、せっかく公開しても正しく扱われないことになってしまうばかりでなく、受信側で認証を pass したメール以外受信しないようなサービスを提供していた場合、メールが届かなくなる可能性があります。

ここでは以下に間違えやすい例を示しますので、これらを参考に誤った記述が少なくなることを期待します。

Sample 1: バージョンの間違い(その1)

"v=spf1.0" は間違っており、"v=spf1" でなければなりません。

(誤)
example.org. IN TXT "**v=spf1.0** include:example-example.org -all"
(正)
example.org. IN TXT "**v=spf1** include:example-example.org -all"

Sample 2: バージョンの間違い(その2)

SPFv2 のレコードを公開する場合、SPFv1 での記述方法や、"v=spf2.0/pra" という記述方法は間違っており、"spf2.0/pra" でなければなりません。

(誤)
example.org. IN TXT "**v=spf2.0**/pra include:example-example.org -all"
(正)
example.org. IN TXT "**spf2.0**/pra include:example-example.org -all"

Sample 3: 機構が省略されている

誤り例では、機構が省略されている上に、ドメイン名が FQDN ではないため、エラーとなってしまいます。+a:ホスト名(FQDN)と記述することが必要です。

(誤)
example.org. IN TXT "v=spf1 mx **nm nm1** ~all"
(正)
example.org. IN TXT "v=spf1 mx **a:nm.example.org a:nm1.example**.org ~all"

Sample 4: 1つのドメインに対して複数の SPF1 レコードを公開している

1 つのドメインに対しては 1 つの SPF1 レコードだけ公開可能です。複数公開するとエラーになります。ただし、SPF2 のレコードと SPF1 のレコードを 1 つずつ同時に公開することはできます。

```
(誤)
   example.org. IN TXT "v=spf1 ip4: 10.0.3.0 ip4: 10.0.3.1 ~all"
        example.org. IN TXT "v=spf1 a:mx01.example.org ~all"
        example.org. IN TXT "v=spf1 a:web.example.org ~all"
(正 1)
   example.org. IN TXT "v=spf1 ip4: 10.0.3.0 ip4: 10.0.3.1 a:mx01.example.com a:web.example.org ~all"
(正 2)
   example.org. IN TXT "v=spf1 ip4: 10.0.3.0 ip410.0.3.1 a:mx01.example.com a:web.example.org ~all"
   example.org. IN TXT "spf2.0 ip4: 10.0.3.0 ip4: 10.0.3.1 a:mx01.example.com a:web.example.org ~all"
```

Sample 5: タイプミス

"ip4:" を"ipv4:" や "ip:" などと間違えるケースが非常に多く見受けられます。また、誤 7 の例のように、SPF レコードを作成するために使ったツールなどが、"~" の文字を間違って変換してしまう場合などもあるので、注意が必要です。

```
(誤 1)
   example.org. IN TXT "v=spf1 ipv4: 10.0.3.0 mx ~all"
```

“ipv4:“ は間違い

```
(誤 2)
   example.org. IN TXT "v=spf1 ip: 10.0.3.0 mx ~all"
```

“ip:“ は間違い

```
(誤 3)
   example.org. IN TXT "v=spf1 ip10.0.3.0 mx ~all"
```

“:“ が抜けている

```
(誤 4)
   example.org. IN TXT "v=spf1 ip4=10.0.3.0 mx ~all"
```

“:“ の代わりに “=“ を使っている

```
(誤 5)
   example.org. IN TXT "v=v=spf1 ip4: 10.0.3.0 mx ~all"
```

“v=v=“ とバージョン記述を間違えている

```
(誤 6)
   example.org. IN TXT "v=spf1 ip4"
```

書きかけで終わっている

```
(誤 7)
   example.org. IN TXT "v=spf1 ip4: 10.0.3.0 mx ¥150all"
```

“~“ が文字化けしている

```
(正)
   example.org. IN TXT "v=spf1 ip4: 10.0.3.0 mx ~all"
```

Sample 6: 空白文字(SP)が抜ける

SPF レコードを二重引用符で複数にわけて記述することは可能ですが、その場合には、"ip4:10.0.3.0/26" "ip4:10.5.0.0 ~all" は "v=spf1 ip4:10.0.3.0/26 ip4:10.5.0.0 ~all" と

いう大きな１つのレコードとして扱われることに注意が必要です。"" でくくられた２つの部分を接続するとき空白文字は補われないため、区切り文字として空白文字が入りません。

```
(誤)
   example.org. IN TXT "v=spf1 ip4: 10.0.3.0/26""ip4: 10.0.4.0 ~all"
(正)
   example.org. IN TXT "v=spf1 ip4: 10.0.3.0/26 ip4: 10.0.4.0 ~all"
```

Sample 7: redirect や include の先がない

include している先のドメインの SPF レコードが存在しないとエラーになります。誤り例では、_spf.example.org のレコードが存在していないためエラーになります。公開当初は存在していたものの、その後の DNS レコードの整理などでの変更を反映していないことなどが原因として考えられます。

```
(誤)
   example.org. IN TXT "v=spf1 include:_spf.example.org ~all"

* Can't find _spf.exmaple.org: Non-exisitent domain
```

Sample 8: redirect や include のループ(相互参照)

include している先のドメインの SPF レコードで、元となるドメインを include してしまい、相互参照が起こるとエラーになります。誤り例では、example.org と _spf.example.org がお互いに相手を参照しあっておりエラーになります。

```
(誤)
   example.org. IN TXT "v=spf1 include:_spf.example.org ~all"
   _spf.example.org. IN TXT "v=spf1 include:example.org ~all"
```

Appendix 1.3 SPF レコードの確認方法の例

現行の送信ドメイン認証技術は、認証情報及びポリシーの公開のために DNS 上に TXT レコードを公開する手法が一般的であるため、これを調査することにより、任意のドメインが送信ドメイン認証技術に対応しているか、ある程度調べることもできます。

以下では、例として、UNIX host コマンドの TXT レコードオプションを利用していますが、同様のクエリが発行できれば問題ありません。このような操作を行うことにより、有効なレスポンスがあるかどうかでレコードの有無を判断できます。

SPF レコード

```
$ host -t txt example.com
example.com descriptive text "v=spf1 include:spf.example.com -all"
```

SenderID レコード

```
$ host -t txt example.com
example.com descriptive text "spf2.0/mfrom,pra +mx +ip4:192.168.0.100 -all"
```

Appendix 2. DKIM レコードの記述例

Appendix 2. DKIM レコードの記述例

本節では、DKIM レコードの記述例について説明します。

Appendix 2.1　DKIM レコードの例

DKIM レコードは SPF レコードに比べる指定する内容は簡単ですが、バージョンの記述など間違えないように気をつけて記述するようにこころがけましょう。DKIM レコード公開後に必ず、試験的にメールを送信して認証成功するかどうかを確認することが必要です。

Sample 1: 一般的な DKIM レコード

```
k100430._domainkey.example.co.jp IN TXT "v=DKIM1;k=rsa;p=MIGfMA0GCSqGSIb3DQEB
AQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOooW7HmqsPFzZUUb1nNqMj7ozyv/Q0WwwGJ+bdS
4a9tO9roiT+VyyyMfIBoTdMNEWoXUMHafPgkOFPl5YO52pZM40bdXY/qtfT2nglJqS53zFFqB36qHoN9lg
PRwP/e+ScCPlwHkcfIwD58ISU/lC5Bx+wIDAQAB"
```

Sample2：t=y の指定により試験的運用であることを示す

```
k100429._domainkey.example.com. IN TXT "v=DKIM1; k=rsa; t=y; p=MIGfMA0GCSqGSIb
3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOooW7HmqsPFzZUUb1nNqMj7ozyv/Q0Www
GJ+bdS4a9tO9roiT+VyyyMfIBoTdMNEWoXUMHafPgkOFPl5YO52pZM40bdXY/qtfT2nglJqS53zFFqB36q
HoN9lgPRwP/e+ScCPlwHkcfIwD58ISU/lC5Bx+wIDAQAB"
```

Appendix 2.2 DKIM レコードの間違い例

文法的に間違った DKIM レコードを公開すると、受信側では permerror と扱われ、せっかく公開しても正しく扱われないことになってしまうばかりでなく、受信側で認証を pass したメール以外受信しないようなサービスを提供していた場合、メールが届かなくなる可能性があります。

ここでは以下に間違えやすい例を示しますので、これらを参考に誤った記述が少なくなることを期待します。

Sample 1：誤ったＦＱＤＮ上にＤＫＩＭレコードを公開している （その１）

直接該当ドメインの TXT レコードとして公開しています。DKIM の場合、 SPF とは異なり、"セレクタ._domainkey" サブドメインに公開する必要があります。

```
（誤）
 example.co.jp IN TXT
 "v=DKIM1;k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOoo
 W7HmqsPFzZUUb1nNqMj7ozyv/Q0WwwGJ+bdS4a9tO9roiT+VyyyMfIBoTdMNEWoXUMHafPgkOFPl5
 YO52pZM40bdXY/qtfT2nglJ”
（正）
 k100429. _domainkey.example.co.jp IN TXT
 "v=DKIM1;k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOoo
 W7HmqsPFzZUUb1nNqMj7ozyv/Q0WwwGJ+bdS4a9tO9roiT+VyyyMfIBoTdMNEWoXUMHafPgkOFPl5
 YO52pZM40bdXY/qtfT2nglJ”
```

Sample 2: 誤った FQDN 上に DKIM レコードを公開している（その２）

セレクタを使わないで、サブドメインの _domainkey 以下に直接キーのレコードを記述しています。正しくは、"セレクタ._domainkey" サブドメインに公開する必要があります。

```
（誤）
 _domainkey.example.co.jp IN TXT
 "v=DKIM1;k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOoo
 W7HmqsPFzZUUb1nNqMj7ozyv/Q0WwwGJ+bdS4a9tO9roiT+VyyyMfIBoTdMNEWoXUMHafPgkOFPl5
 YO52pZM40bdXY/qtfT2nglJqS53zFFqB36qHoN9lgPRwP/e+ScCPlwHkcfIwD58ISU/lC5Bx+wIDAQAB"
（正）
 K100429._domainkey.example.co.jp IN TXT
 "v=DKIM1;k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOoo
 W7HmqsPFzZUUb1nNqMj7ozyv/Q0WwwGJ+bdS4a9tO9roiT+VyyyMfIBoTdMNEWoXUMHafPgkOFPl5
 YO52pZM40bdXY/qtfT2nglJqS53zFFqB36qHoN9lgPRwP/e+ScCPlwHkcfIwD58ISU/lC5Bx+wIDAQAB"
```

Sample 3: 公開鍵方式指定の誤り

公開鍵方式の指定をハッシュの方式と間違　　えています (k=sha1 ではなく k=rsa)。

```
（誤）
 k100429._domainkey.example.com. IN TXT"v=DKIM1; k=sha1; t=y;
 p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOooW7HmqsPFzZUU
 b1nNqMj7ozyv/Q0WwwGJ+bdS4a9tO9roiT+VyyyMfIBoTdMNEWoXUMHafPgkOFPl5YO52pZM40bdX
 Y/qtfT2nglJqS53zFFqB36qHoN9lgPRwP/e+ScCPlwHkcfIwD58ISU/lC5Bx+wIDAQAB"
（正）
 K100429._domainkey.example.co.jp IN TXT
 "v=DKIM1;k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOoo
 W7HmqsPFzZUUb1nNqMj7ozyv/Q0WwwGJ+bdS4a9tO9roiT+VyyyMfIBoTdMNEWoXUMHafPgkOFPl5
 YO52pZM40bdXY/qtfT2nglJqS53zFFqB36qHoN9lgPRwP/e+ScCPlwHkcfIwD58ISU/lC5Bx+wIDAQAB"
```

Sample 4: バージョン記述の誤り

DKIM のバージョンを間違えています　　（v=DKIM1.0 ではなく、v=DKIM1)。

```
（誤）
 k100429._domainkey.example.com. IN TXT"v=DKIM1.0; k=rsa; t=y;
 p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOooW7HmqsPFzZUU
 b1nNqMj7ozyv/Q0WwwGJ+bdS4a9tO9roiT+VyyyMfIBoTdMNEWoXUMHafPgkOFPl5YO52pZM40bdX
 Y/qtfT2nglJqS53zFFqB36qHoN9lgPRwP/e+ScCPlwHkcfIwD58ISU/lC5Bx+wIDAQAB"
（正）
 K100429._domainkey.example.co.jp IN TXT
 "v=DKIM1;k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOoo
 W7HmqsPFzZUUb1nNqMj7ozyv/Q0WwwGJ+bdS4a9tO9roiT+VyyyMfIBoTdMNEWoXUMHafPgkOFPl5
 YO52pZM40bdXY/qtfT2nglJqS53zFFqB36qHoN9lgPRwP/e+ScCPlwHkcfIwD58ISU/lC5Bx+wIDAQAB"
```

Sample 5: バージョン記述の位置の間違え

タグの順番を間違えています。v= タグがレ　　コードの先頭に必要です。

```
（誤）
 k100429._domainkey.example.com. IN TXT"k=rsa; v=DKIM1; t=y;
 p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOooW7HmqsPFzZUU
 b1nNqMj7ozyv/Q0WwwGJ+bdS4a9tO9roiT+VyyyMfIBoTdMNEWoXUMHafPgkOFPl5YO52pZM40bdX
 Y/qtfT2nglJqS53zFFqB36qHoN9lgPRwP/e+ScCPlwHkcfIwD58ISU/lC5Bx+wIDAQAB"
（正）
 K100429._domainkey.example.co.jp IN TXT
 "v=DKIM1;k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOoo
 W7HmqsPFzZUUb1nNqMj7ozyv/Q0WwwGJ+bdS4a9tO9roiT+VyyyMfIBoTdMNEWoXUMHafPgkOFPl5
 YO52pZM40bdXY/qtfT2nglJqS53zFFqB36qHoN9lgPRwP/e+ScCPlwHkcfIwD58ISU/lC5Bx+wIDAQAB"
```

Appendix 2.3 DKIM のレコードの確認方法の例

現行の送信ドメイン認証技術は、認証情報及びポリシーの公開のために DNS 上に TXT レコードを公開する手法が一般的であるため、これを調査することにより、任意のドメインが送信ドメイン認証技術に対応しているか、ある程度調べることもできます。

Appendix1.3 と同様に、以下では、例として、UNIX host コマンドの TXT レコードオプションを利用していますが、同様のクエリが発行できれば問題ありません。このような操作を行うことにより、有効なレスポンスがあるかどうかでレコードの有無を判断できます。

DKIM / DomainKeys レコード

```
$ host -t txt selector._domainkey.example.com
selector._domainkey.example.com descriptive text "k=rsa¥; t=y¥; p=(中略)¥; n=A 768 bit key¥;"
```

DKIM ADSP レコード

```
$ host -t txt _adsp._domainkey.example.com
_adsp._domainkey.example.com descriptive text "dkim=all"
```

ただし、DKIM の場合は、ドメインに加えて前述のセレクタが分からなければ確認することは困難です。

また、そもそも、これらの DNS レコードは、送信者が試験として一時的に設置している可能性もあり、DNS レコードが存在しているからといって送信ドメイン認証技術に対応しているかは断定できません。したがって、以上のような確認方法は、あくまで補助的な確認方法となることに注意して下さい。

Appendix 3. 関連 RFC

Appendix 3. 関連 RFC

no	title	概要
RFC2554	SMTP Service Extension for Authentication	SMTP での送信者の認証方式である SMTP-AUTH の標準規格
RFC4406	Sender ID: Authenticating E-Mail	送信ドメイン認証技術の一方式である Sender ID の標準規格
RFC4407	Purported Responsible Address in E-Mail Messages	Sender ID で利用する PRA の標準規格
RFC4408	Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, version 1	送信ドメイン認証技術の一方式である SPF の標準規格
RFC4871	DomainKeys Identified Mail (DKIM) Signatures	送信ドメイン認証技術の一方式である DKIM の標準規格
RFC5321	Simple Mail Transfer Protocol	電子メールのプロトコルである SMTP の標準規格
RFC5322	Internet Message Format	電子メールの形式に関する標準規格
RFC5451	Message Header Field for Indicating Message Authentication Status	認証結果のヘッダーへの記録形式の標準規格
RFC5617	DomainKeys Identified Mail(DKIM) Authoer Domain Signing Practices (ADSP)	DKIM の署名方針に関する補助規格
RFC5672	RFC 4871 DomainKeys Identified Mail (DKIM) Signatures – Update	DKIM の標準規格（RFC4871）の更新

Appendix 4. 用語集

Appendix 4. 用語集

インターネット標準	インターネットにおける技術等について、オープン標準として承認されたもの。
エラーメール	宛先不明や、メールサイズが大きすぎるなどメールを宛先に配送できない場合に、送信元へエラーが発生したことを通知するメール。エラーメールの送信先には、送信者情報を用いる。
公開鍵暗号技術	公開鍵と秘密鍵という鍵ペアを用いて、データの暗号化・復号化を行う暗号方式。迷惑メール対策技術の中では、送信ドメイン認証技術の一つである DKIM において利用される。
サーバ	クライアントからの要求に対してサービスを提供するシステムのこと。電子メールの配送をするためのシステムはメールサーバと呼ばれる。
サーバ・アプリケーション・プログラム	サーバのサービスを処理するためのプログラム。メールサーバの場合には、メールの相手先を振り分けるメール転送エージェント (MTA) や、振り分けられたメールをサーバ内のユーザや別のサーバへ配送するメール配送エージェント (MDA) などといったサービスを処理するプログラムがある。
送信者情報	電子メールの送信者の情報。
リバースパス	電子メールの送信元。エンベロープ from とも呼ばれる。メールヘッダには ”<Return-Path: メールアドレス>“ として記録される。
From ヘッダアドレス	ヘッダ form 参照。
PRA	Purported Responsible Address の略で From 、 Sender 、 Resent-From 、 Resent-Sender で記述するアドレスを指す。
エンベロープ from	リバースパス参照。
ヘッダ from	一般的に、メールを作成した者のアドレス。メールのヘッダーフィールドに記載された送信者のメールアドレス。メールヘッダには 、“From: メールアドレス” で記録される。
Sender アドレス	メールの作成者と送信者が異なる場合に、送信者の名前やアドレスを記載するもの。メール配信業者がメールを送信する場合に使うことが多い。
Resent From アドレス	メールを転送時等に付与する転送者のアドレス。メールヘッダには、”Resent-From: アドレス” で記録される。
Resent Sender アドレ	メールを再送時等に付与するアドレス。Sender アドレスが記載さ

	ス	れている場合は、“Resent-Sender” を使うのが一般的である。
送信ドメイン認証技術		
	ネットワーク方式	ネットワークを用いた認証方式
	電子署名方式	公開鍵暗号方式を用いた認証方式。
セレクタ		公開鍵を取得する際に、クエリを発行する対象のドメイン名の一部に利用する。複数のセレクタを持つことで１つのドメインで複数 の公開鍵を利用できる。
電子署名		本人確認や、偽造・改ざんの防止に用いる電子的な署名。
ドメイン		インターネット上に存在するコンピュータやネットワークを識別する名前。重複しないように ICANN という国際組織により一元管理されている。
ドメインレピュテーション		電子メールの送信に利用されているドメインの評判情報（レピュテーション情報）、または、この情報を用いて、通信を制限する技術。
バウンスメール		エラーにより、送信元に送り返されてくるメールのこと。
ハッシュ		ハッシュ関数から得られた数値のこと。検索やデータ比較処理の高速化、改竄の検出などに用いられる。
ハッシュ関数		元となる情報から、不可逆な一定長の情報を算出する関数。SHA1、SHA256 などがある。
配信サービス		メールの配信を作成者に変わって行うサービスのこと。
標準規格		RFC で規定される標準化規格のうち、Standard の標準状態のもの。
フィルタ		
	アンチウィルスフィルタ	メールに添付されたウィルスファイルを検知し、削除したりする機能。
	迷惑メールフィルタ	迷惑メールの特徴や送信元情報などをあらかじめデータ化して、受信メールと照らし合わせて機械的に判断し、迷惑メールと判断したメールを専用フォルダに格納したり削除したりする機能。
ブラウザ		データを表示、閲覧するためのソフトウェア。Web ブラウザ、画像ブラウザなど。一般的にブラウザと言った場合、ホームページ（html 言語）を表示するための Web ブラウザを示す。
ブラックリスト		アクセスを許可しないリスト。メールで用いる場合は、メール受信を拒否するアドレスリストを指すのが一般的である。
ホスティングサービス		記憶領域や演算能力等のサーバの機能を提供するサービス。
ホスト		ネットワークに接続された機器につけられた名前のこと。
ホワイトリスト		アクセスを許可するリスト。ブラックリストの逆。メールで用いる場合は、メール受信を許可するアドレスリストを指すのが一般的。

メールサービス	電子メールの使用権利を提供するサービス。
メールシステム	電子メールの送受信のために用いられるシステム。
メールスプール	第２章参照。
メールヘッダ	電子メールの先頭に記載されたデータ領域で、送受信に用いられる情報を記載する部分。
ラベリング	メールの題名などに、特定の情報を追加する機能。例えば迷惑メールフィルタによって迷惑メールと判定されたメールの題名に、[meiwaku] などの文字列を追加し、見分けやすくするものなどがある。また、ドメイン認証の結果をヘッダに付与するように、ヘッダ情報に付与する付加情報もラベリングと呼ぶ場合が多い。
リゾルバ	DNS のネームサーバに対して IP アドレスからホスト名を取得したり、その逆を行ったりするためのプログラム
Authentication Results ヘッダ	送信ドメイン認証における認証結果などを記述するためのヘッダーフィールド
CRAM-MD5	SMTP AUTH で使われる SASL の認証方式の一つ
DKIM	送信ドメイン認証技術の一方式。送信元が付した電子署名により送信元情報の真偽及び電子メールの本文の改変を検知することができる。DomainKeys と IIM を合わせて策定されたもの。RFC4871
DKIM-ADSP	DKIM Author Domain Signing Practice の略。DKIM の拡張技術
DKIM-Signature ヘッダ	DKIM において、作成した電子署名を付与するためのヘッダーフィールド
DNS	Domain Name System の略。ドメイン名と IP アドレスを対応付けるデータベースシステム。インターネット上のコンピュータにアクセスするためには IP アドレスを知らなければならないが、直接数字入力するのは実用的ではないので、名前を用いてアクセスする方法が考案された。
再帰検索	DNS サーバに対して DNS 解決が完結するまでドメイン・ツリーをたどって検索を行うもの
資源レコード	DNS サーバに登録する情報のこと。A レコード、MX レコード、NS レコードなどがある。
MX レコード	Mail eXchange レコードの略。DNS サーバに定義された受信メールサーバーのホスト情報など
TXT レコード	ホスト名に関連付けるテキスト情報（文字列）を定義する DNS レコードの一つ
SPF レコード	SPF / Sender ID において、そのドメインが使用する送信サーバを

		インターネット上で宣言するための DNS レコードの一つ
	A レコード	ホスト名から IPv4 アドレスを取得するための情報を記録した DNS レコードの 1 つ
ESMTP		SMTP の拡張を定義したもの。
FQDN		Fully Qualified Domain Name の略。TCP / IP ネットワーク上で、ドメイン名・サブドメイン名・ホスト名をすべて省略せずに指定した記述形式のこと
GlobalIP		インターネットに接続された機器に一意に割り当てられた IP アドレス。
IETF		The Internet Engineering Task Force の略。インターネット上で利用される技術の標準化を行う組織。策定された標準仕様を、RFC（Request For Comment）として発行している。
IMAP4		Internet Message Access Protocol version 4 の略。メールサーバ上に保存されている電子メールに直接アクセスすることができる通信プロトコル。
IP アドレス		インターネット上で個別の端末を判別するための番号。
IPv6		Internet Protocol version 6 の略。現在主流のインターネットプロトコルである IPv4 に変わる次世代版プロトコル。
ISP		Internet Service Provider の略。インターネットに接続するサービスの提供を行う企業や団体をいう。
MARID WG		Mta Authorization Records In Dns Working Group の略。
MDA		メール配送エージェント。Mail Delivery Agent の略。第２章参照。
milter		mail filter の略で、Sendmail が開発したメールフィルタプラグインの仕組み
MTA		Mail Transfer Agent の略。電子メールをクライアントーサーバ間・サーバーサーバ間で転送するサーバ。第２章参照。
MUA		Mail User Agent の略。いわゆるメールクライアントであり、電子メールを使用するもののユーザーインターフェイスとなる。例えば Microsoft Outlook や Mozilla Thunderbird などである。第２章参照。
MSA		Message Submission Agent の略。MUA から発信されたメールを受け取るサーバ。MTA と同義で使用することもあるが MSA は、SMTP AUTH や POP before SMTP などの認証機能や不完全なメールヘッダの修正を行う機能を提供する。第２章参照。
POP3		Post Office Protocol Version 3 の略。メールサーバから電子メールを取り出すときに使用される通信プロトコル。RFC1939。

RFC	IETF が正式に発行する技術の標準を定めた文書。
実験的 RFC	RFC の位置づけで、インターネットに関して有用と考えられる研究成果や実験結果を広く公開するためのもの
SenderID	送信ドメイン認証技術の一つ。SPF と同様のチェックに加え、Resent-sender: → Resent-from: → Sender: → From: 順序でヘッダ情報の送信ドメインをチェックし、当該 DNS に確認を行い送信元情報の真偽を確認する。RFC4406。
SMTP	Simple Mail Transfer Protocol の略。インターネットで電子メールを転送するプロトコル
HELO コマンド	SMTP コマンドの一つ。SMTP セッションを開始するコマンド。
MAIL コマンド	SMTP コマンドの一つ。メールを送るコマンド
DATA コマンド	SMTP コマンドの一つ。メールを転送するコマンド
エラーメール	メールの配送になんらかの問題が発生した場合に送信者に対して送られるメール。エラーの内容が書かれている場合が多い
SMTP AUTH	RFC 2554 によって規定された、SMTP にユーザ認証機能を追加するもの。
SPF	Sender Policy Framework の略。送信ドメイン認証技術の一つ。エンベロープ情報の From メールアドレスのドメイン名をチェックし、当該 DNS に確認を行い送信元情報の真偽を確認する。RFC4408。
SPF レコード	SPF で、DNS サーバ上にメールを送信するサーバの情報を公開するためのヘッダーフィールド。
限定子	限定子は、それに続く機構にマッチした場合の認証結果を指定する。
機構	機構には、認証対象の送信元ホストの IP アドレスと照合する条件を記述する。
修飾子	引数であるドメイン名に指定されたドメインの SPF レコードにより認証処理を実行する「redirect」と、認証が失敗した場合、引数であるドメイン名に指定されたドメインの TXT RR に設定されている文字列を、認証失敗した理由や説明等として利用する「exp」がある。
TCP	Transmission Control Protocol の略。インターネットでデータ転送に用いられるプロトコル。複数のエラー制御によって信頼性を確保することができる。
TTL	Time To Live の略。パケットの無限ループを防止するためにあらかじめ設定されるパケットの生存時間の値。
UDP	User Datagram Protocol の略。インターネットでデータ転送に用い

	られるプロトコル。TCP とは違いエラー制御のための仕組みをもたない。

送信ドメイン認証技術導入マニュアル第2版

2011 年 8 月発行

企画・著作・制作　　迷惑メール対策推進協議会

（事務局）

（財）日本データ通信協会迷惑メール相談センター

〒170-8585　東京都豊島区巣鴨2－11－1

URL　　http://www.dekyo.or.jp/soudan/

TEL：03-5907-5371

迷惑メール対策推進協議会