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。

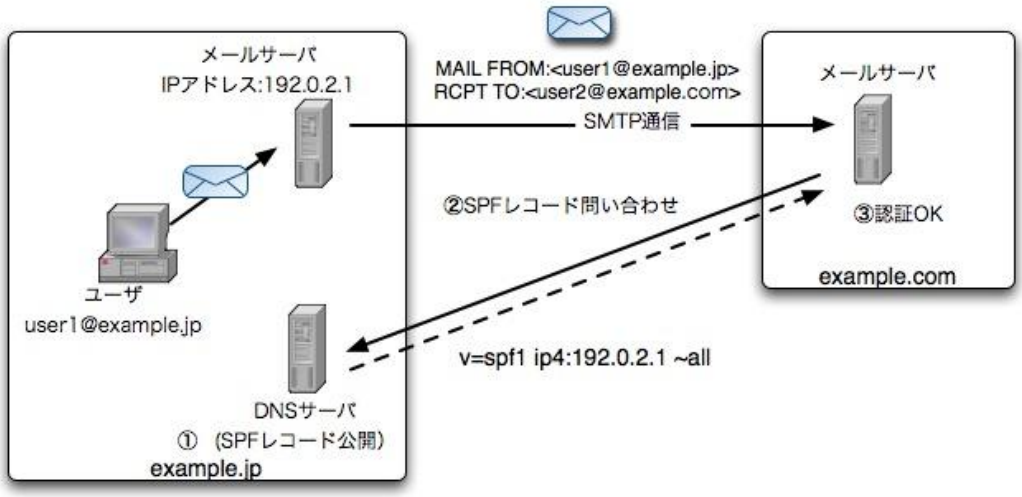
3.2　Sender Policy Framework (SPF)

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。

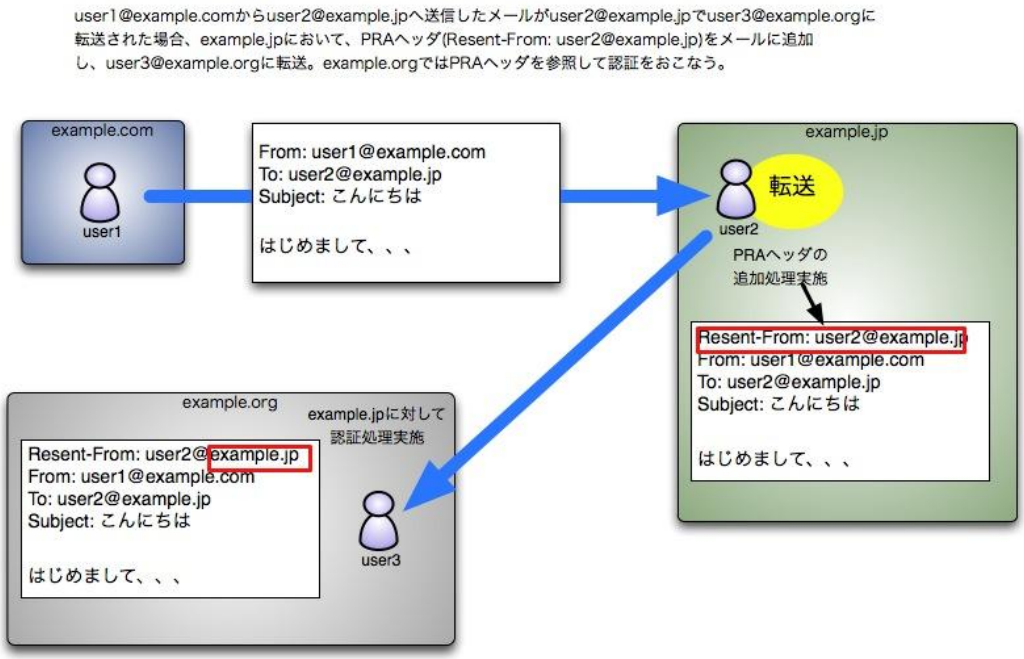
3.3.2　Puported Resposible Adress(PRA)

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)

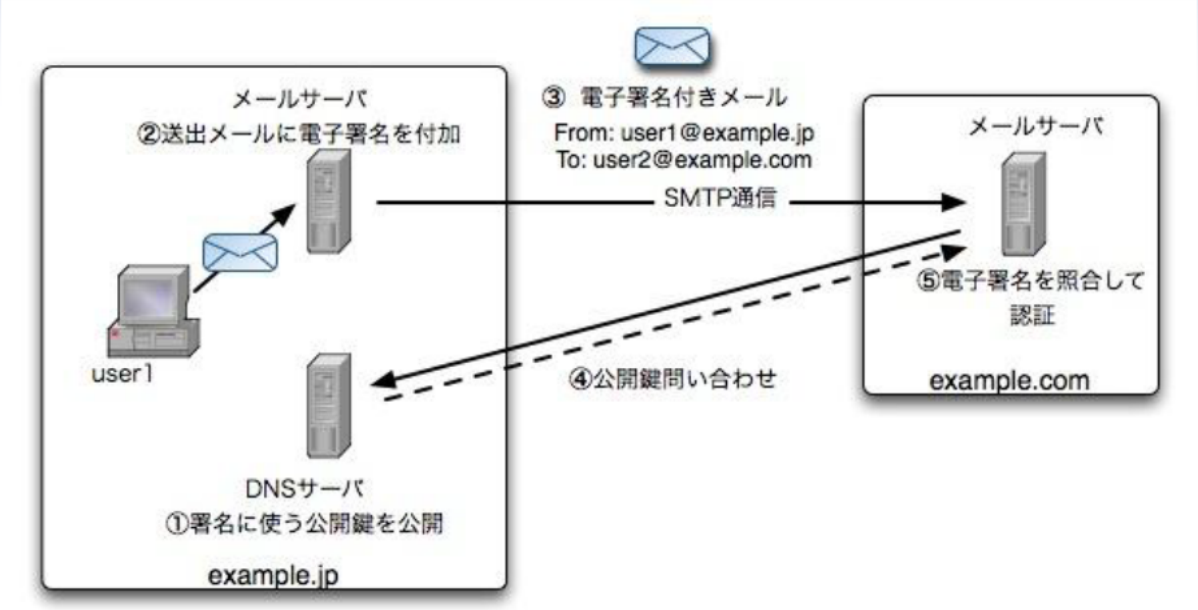
3.4.1　概要

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。

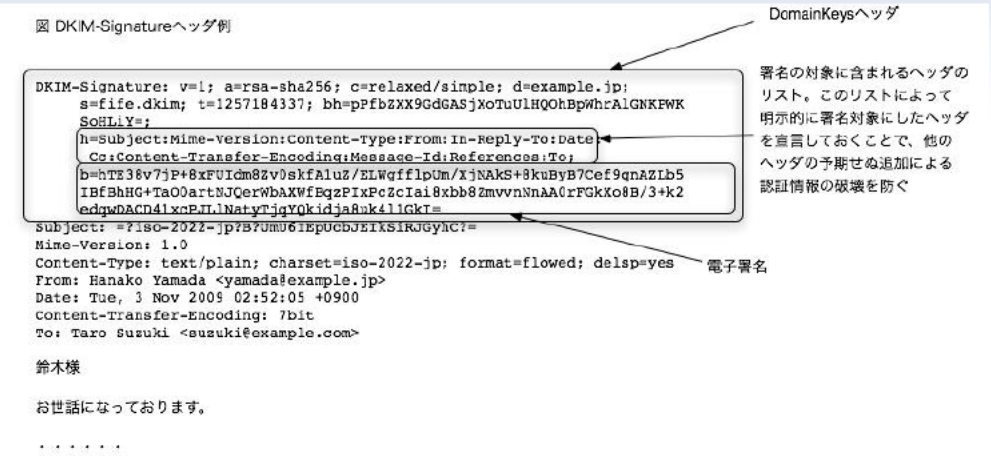
公開鍵のレコードは、「タグ＝値」を ; で列挙することになります。利用できるタグを、図表３－13 に示します。

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