第 2 章

応用編

2.1　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メールの送信側と受信側のどちらの立場からも導入することができます．

第 1 章の基礎編において，送信ドメイン認証技術 SPF, DKIM, DMARC それぞれの基本的な仕組みや設定方法については解説しました．応用編では，送信ドメイン認証技術の導入に際し，DMARC 認証が有効に機能する観点から，事前に検討しておくべきことや，送信側と受信側それぞれの側での作業にあたり留意すべき点，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．

また近年では，メール機能の一部あるいは全体を，クラウド等を利用した外部の事業者が提供するサービスを利用したり，メールマガジンなど特定目的のメール配信を送信事業者に外部委託するなど，他の事業者が提供するサービスと連携した利用が進んでいます．外部の事業者との連携する方法や，いわゆるクラウドサービスを利用した場合でも，正しく送信ドメイン認証技術が利用できる設定運用方法についても解説します．

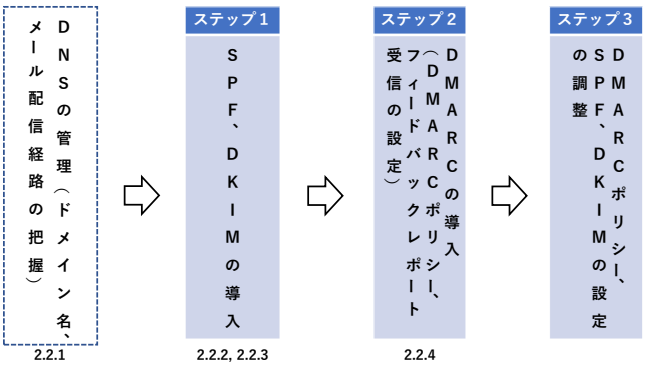

図 2.1　DMARC の導入手順

2.2 メール送信側の設定

本節では，主にメール送信側として設定する内容について解説します．設定する内容としては，SPF の場合は SPF レコードの設定，DKIM の場合は送信メールサーバへの DKIM 署名機能の導入と DKIM レコードの設定，DMARC の場合は DMARC レコードの設定がそれぞれ必要となります．また，DMARC レポートを受け取る場合には，そのための設定も必要となります．

それぞれの送信ドメイン認証技術や関連技術ごとに，設定に関して注意すべき点や有益となる設定方法について解説します．また，SPF, DKIM は，それぞれ独立した送信ドメイン認証技術ですが，ここでは最終的に DMARC で認証できるための設定方法を中心に解説します．

2.2.1 DNS の管理

送信ドメイン認証技術は，DNS に大きく依存した形で実現されています．SPF, DKIM, DMARC を送信側として導入するためには，DNS に対して対象となる送信ドメイン名に関する情報を正しく設定する必要があります．また，組織内でメールの管理運用の担当者と，DNS の管理運用の担当が異なっている場合や，DNS の設定を外部委託している場合など，双方での連携や意思疎通など，適切な情報共有が必要となります．

自組織のドメイン名を DNS に設定し運用する方法として，外部事業者（DNS サービス事業者）に委託する場合が多いと思います．DNS サービス事業者によっては，送信ドメイン認証技術の送信側の設定をする上で，必要となる設定ができるのかを予め確認しておく必要があります．具体的には，以下の項目です．

- ドメイン名のラベルとして “_”（アンダースコア）が先頭に利用できること
- テキスト資源レコード (TXT RR) を自由に設定できること
- テキスト資源レコードが十分な長さで記述できること
- CNAME 資源レコードの設定ができること（DKIM 署名を外部の事業者が行う場合等）

DNS で設定するラベルの先頭にアンダースコアを利用する場合としては，DKIM レコード，DMARC レコードの設定に必要となります．CNAME 資源レコードは，いわゆる別名定義に用いられる資源レコードですが，クラウド型メールサービスでの DKIM 署名に利用する鍵を，利用するサービス側（クラウド側）で管理する場合に利用することがあります．そのため，特にテキスト資源レコードに対する CNAME 資源レコードを設定できることが必要になる場合があります．詳細は，2.2.3 項で解説します．

さらに，こうした DNS に設定される情報の信頼性を高めるためには，DNSSEC(DNS Security Extensions) に対応しておくことも有効です．利用する DNS サービス事業者および管理しているドメイン名が，DNSSEC に対応しているのかを確認することも必要です．

DNS サービス事業者を利用した DNS の設定には，Web 上で各種の操作を行うことが多いと思います．これらの設定の参照や変更を行うには，Web 上で認証用の ID とパスワードを入力するログイン作業が一般に必要となります．このログインのための認証情報が外部に漏れると，送信ドメイン認証関連の設定はもちろん，メールの配送先を示す MX 資源レコード等の設定も変更されてしまうおそれがあります．DNS サービスに限りませんが，Web 上で操作する各種サービスを利用する場合は，認証のための情報（認証 ID やパスワード）が無関係の第三者に漏れないように管理すべきです．また，サービス提供側も，ログイン時に多要素認証を必要とするなど，不正なログインを防ぐ仕組みを導入するべきです．

2.2.2 SPF レコードの設定

SPF レコードには，メール受信側からみてメールを送信するホスト情報（IP アドレス）を記述します．メール送信ホストに変更がなければ，基本的には SPF レコードを変更する必要は無いので，定期的な作業は必要ありません．

■外部サービスの利用 メールサービスの提供元は，提供先で SPF レコードの設定を容易にするため，メールサービスで利用する送信元のメールサーバの IP アドレスを示した SPF レコードを提供すべきです．メールサービス利用元は，この提供された SPF レコードを include 機構を利用して IP アドレスを取り込みます．このような取り込み (include) 用の SPF レコードを用意し利用してもらうことで，メールサービス提供元がメールサーバの構成を変更する場合や，IP アドレスを書き換えた場合でも，利用元にその都度連絡することなく変更を反映させることができます．また利用元でも，自ドメイン名の SPF レコードを書き換えることなく構成変更に対応できます．

以下に include の利用例を示します．メールサービスの提供元の SPF レコードが mail.example.net であり，メールサービスの利用元のドメイン名を example.jp とした場合の例を以下に示します．

include の利用例

```
mail.example.net.   IN   TXT   "v=spf1 ip4:203.0.113.1/26 -all"
example.jp.         IN   TXT   "v=spf1 include:mail.example.net -all"
```

■複数ドメインの管理 様々な経緯や目的により，メールに利用するドメイン名を複数管理する場合があります．例えば，部門毎に異なったドメイン名を利用したいと考えたり，何らかのキャンペーン等で配信するメール用にドメイン名を変えたい場合などです．これら複数のドメイン名が実際には同じメールシステムで利用する場合には，SPF レコードの redirect 修飾子が利用できます．

redirect の利用例

```
tokyo.example.jp.   IN   TXT   "v=spf1 redirect=spf.example.jp"
osaka.example.jp.   IN   TXT   "v=spf1 redirect=spf.example.jp"
spf.example.jp.     IN   TXT   "v=spf1 ip4:203.0.113.1/26 -all"
```

上記の例では，tokyo.example.jp や osaka.example.jp の SPF レコードは，redirect 修飾子により spf.example.jp の SPF レコードに向け直されます．これにより，メールシステムに変更があった場合でも，spf.example.jp ドメイン名の SPF レコードを修正するだけで，他の 2 つのドメイン名の SPF レコードを修正することなく反映させることができます．

include 機構との違いについても触れておきます．include 先の SPF レコードで pass の結果にならなかった場合，SPF 認証の失敗の強度は include 先の失敗の強度にはならず，あくまで include 機構部分が適合しないだけであり，その後に記述された all の限定子によって決まります．redirect 修飾子の場合は，

redirect 先の認証の結果が元のドメイン名の認証結果になります．そのため，redirect 修飾子は SPF レコードの末尾に記述するべきであるとされ，all 機構がある場合は，redirect 修飾子は無視しなければならないとなっています．

■DNS 参照回数の上限　SPF レコードを設定する上で注意すべき点は，SPF 認証するメール受信側で，認証処理中に DNS の参照回数が 10 回を超えないように SPF レコードを記述することです．参照回数が 10 回を超えた場合，認証結果としては permerror となり pass しない（認証できない）ことになります．この仕組みは，DNS への問い合わせを多く行うことで，DNS に過度な負荷を与えてしまうことを防止する目的で制限が設けられています．

こうした制約のために SPF レコードには，メールの出口を示す機構として ip4 や ip6 など IP アドレスを直接記述することが望ましいと言えます．SPF レコードで利用可能な機構で，ドメイン名を指定する a や MX レコードを示す mx は，DNS の参照回数が増える記述方法です．機構 a では，指定されたドメイン名から IP アドレスを取得するため，DNS 参照回数が 1 回増えます．機構 mx では，MX レコードに指定されたドメイン名の取得と，そのドメイン名から IP アドレスを取得するための DNS 参照で 2 回増えることになります．

DNS 参照が増える SPF レコード例

```
mx.example.jp.     IN  A     192.0.2.1
mail.example.jp.   IN  MX    mx.example.jp
mail.example.jp.   IN  TXT   "v=spf1 mx -all"
...
msg.example.jp.    IN  TXT   "v=spf1 a:mailhost.example.jp -all"
```

外部のメールサービスや配信サービスを利用する場合に利用する include 機構を利用すると，include 先の SPF レコードを取得するための DNS 参照が 1 回行われます．include 先の SPF レコードがさらに include 機構を利用していたり，ホスト名などを設定している場合には DNS の参照回数が増えます．そのため，あらかじめメールサービス提供側の SPF レコードでも，なるべく DNS の参照回数が発生しないような記述をすべきです．また，SPF レコード設定時点で参照回数が 10 回以下だったとしても，include 先の SPF レコードの管理元の設定変更により DNS の参照回数が増えるような変更をした場合に，include 元で SPF レコードを変更していなくても参照回数が 10 回を超えることもありますので，注意が必要です．

こうした観点から SPF レコードの設定には，以下の事柄に注意するべきです．

- 設定する送信元は IP アドレスあるいはネットワークアドレス（CIDR）を用いてなるべく少ない文字数で記述指定する
- ネットワークアドレスには必ずしもメールサーバに使われるアドレスだけを記述する必要は無く，自組織管理の範囲内であればネットワークアドレスとしてまとめることで記述項目を減らす
- a，mx，ptr，exists などの機構はその部分自体で DNS 参照を伴うので利用時に注意が必要（全体で DNS 参照回数を超えないように）
- 特に機構 mx は，MX レコードの参照とそのドメイン名に対する IP アドレス（A または AAAA レコード）の参照を伴うため最低 2 回の DNS 参照を必要とする（MX レコードには直接 IP アドレスが設定

できない）

SPF レコードでのネットワークアドレスによる指定方法は，送信サーバが複数存在し，それらが送信メールサーバ以外の用途のホストを含む特定のネットワークアドレス内に収まっているのであれば，ネットワークアドレスで送信サーバを指定することで，SPF レコードの記述量を減らすことができます．指定したネットワークアドレスに，送信メールサーバが含まれていなくても，それらの IP アドレス帯域を所有管理しており，メールが送信される可能性が無いのであれば，それらをネットワークアドレスで指定しても問題ありません．

SPF レコードのネットワークアドレス指定

```
mailout1.example.jp.   IN  A    192.0.2.4
mailout2.example.jp.   IN  A    192.0.2.6
example.jp.            IN  TXT  "v=spf1 192.0.2.4/30 -all"
```

メールの利用形態は様々あり，今後の用途の広がり（外部サービスの利用等）も考慮するのであれば，SPF レコードを設定する時点で各種制限（DNS の参照回数や記述文字列数について）に近い設定をするのではなく，余裕を持たせておくことが望ましいといえます．SPF レコードの設定については，運用上の手間を省略したい目的でホスト名を指定する場合もありますので，SPF レコードの設定内容は，全体的な運用負荷と SPF 認証時の DNS 参照回数制限の両方を検討したうえで総合的に判断すべきです．

■SPF レコードの設定エラー　正しく SPF レコードを設定し，最初は SPF 認証できていたとしても，何らかの事情で include や redirect で指定したドメイン名の SPF レコードが無くなっている場合があります．これら指定したドメイン名の SPF レコードが参照できない場合[*1]，SPF としては permerror となります．自組織の管理外の SPF レコード（ドメイン名）を参照先として指定している場合には，その SPF レコードが存在しているか，あるいはメール受信側で SPF の認証結果が permerror となっていないかなど，定期的に確認すべきです．

SPF の認証結果が permerror となってしまう設定例に，同じドメイン名に複数の SPF レコードを設定している場合があります．SPF では，SPF レコードとして TXT 資源レコードを利用するため，複数の SPF(TXT) レコードを DNS の仕様上は設定可能です．しかし，SPF の仕様として同じドメイン名に複数の SPF レコードが存在する場合は permerror となります．

複数の SPF レコードの設定例 (permerror)

```
example.jp.   IN  TXT  "v=spf1 ip4:203.0.113.1/26 -all"
example.jp.   IN  TXT  "v=spf1 ip6:2001:db8::/32 -all"
example.jp.   IN  TXT  "v=spf1 include:mail.example.net -all"
```

上記の例のように，複数のメール送信サーバが存在する場合は，以下のように 1 つの SPF レコードにそれ

[*1] DNS の応答として NXDOMAIN エラーだった場合など

ぞれのメールサーバの情報を記述します.

送信メールサーバの送信経路が複数の設定例

```
example.jp.   IN   TXT   "v=spf1 ip4:203.0.113.1/26 ip6:2001:db8::/32 include:mail.example.net -all"
```

SPF レコードの記述間違いによって，permerror となる事例として記述間違いがあります．良く見られる記述間違いを以下に示します.

- 区切り文字としてセミコロン（;）をつけたり区切り (空白) の記述漏れ，SPF では各項目の区切りは一つ以上の空白文字です
- IP アドレスを示す機構として ipv4 や ipv6 と v を付ける，正しくは ip4，ip6 です
- 限定子と機構の間に空白を入れてしまう（ex. +␣mx）

これら SPF レコードの設定に間違いが無いかを確認するためには，チェックサイトを利用したり，SPF 認証を実施している受け取ることができる宛先に，実際にメールを送信するなどで確認することができます.

■DMARC 認証のための SPF 認証　SPF では，正規のメール送信元以外を対象とするために all を末尾に置いて，その限定子 (qualifier) を −，∼，?の中から選ぶことで，認証失敗の強度を fail，softfail，neutral と変化させることができます．しかしながら DMARC の観点からは，SPF 認証が成功したドメイン名しか扱いませんので，これらの認証失敗の強度の違いは，DMARC としては意味がありません．もちろん，SPF としての認証結果としては意味はありますし，その結果を利用した受信処理を行う可能性があるので，送信側として適切な限定子を設定すべきです.

DMARC 認証のための SPF 認証として気をつけなければならないことは，SPF 認証されるドメイン名 (RFC5321.From あるいは HELO/EHLO のドメイン）と DMARC 認証のドメイン（RFC5322.From のドメイン）との関係です．通常のメール送信において，一般的なメールソフトウェア (MUA) からメール送信する場合，エンベロープ From(RFC5321.From) とヘッダ From(RFC5322.From) の送信ドメインが異なることは，通常ありません．しかしながら，以下のようなメールの利用形態では，それぞれの送信ドメインが一致しないことがあります.

- 何らかのキャンペーンメールやメールマガジン等の送信を外部の送信事業者に配信を委託する場合
- 外部のドメイン名で運営されているメーリングリスト経由で配送される場合
- 共有型のメールサービスの利用時に RFC5321.From が空 (<>) を指定したメール送信の場合（共有型サービスでの独自ドメイン等が HELO/EHLO のドメインとなる）

こうした利用形態では，SPF で認証 (pass) できたとしても DMARC では認証できない (fail) ことがあります．このような場合，DKIM 署名を併用することで解決できる場合があります．また，DKIM を利用した場合でも注意すべき利用形態がありますので，通常のメールの使い方をしていたとしても，メール送信側だけではうまく DMARC 認証できない場合があります．こうした，メール再配送 (indirect email flow) の課題と対策については，**2.4 メール再配送の課題**で述べます.

2.2.3 DKIM の設定

DKIM の公開鍵は，DKIM-Signature ヘッダに示された d，s タグの情報を利用し，参照するドメイン名のテキスト資源レコード (TXT RR) に設定します．そのため，署名時の処理（利用する秘密鍵）と DNS に設定されている DKIM の公開鍵は必ず連動（ペア）しなければなりません．少なくとも，メール受信側にメールが届き DKIM 署名を検証する時点で，DNS から DKIM の公開鍵が正しく取得できるよう予め設定しておく必要があります．

■DKIM の鍵管理　DKIM レコードに設定する公開鍵とペアとなる秘密鍵は，DKIM 署名の作成時に必要となりますので，外部に漏れないよう適切に管理する必要があります．DKIM 署名の秘密鍵が漏れると，ドメイン名の管理元と無関係な第三者が，当該ドメイン名で認証できる DKIM 署名が作成可能となり，DKIM 認証ができる詐称メールが送信できてしまいます．また，DKIM 認証ができれば DMARC 認証できるメールも送信できることになります．このため，DKIM 署名の秘密鍵を漏洩しないように管理するとともに，万が一漏れてしまったり類推できる状態となった場合には，速やかに新しい鍵ペアに交換すべきです．そのため新しい鍵の生成や鍵交換のための手順と運用体制を準備しておくべきです．

メール送信の一部を外部に委託するような場合，できれば利用する鍵はそれぞれで管理運用すべきです．そのためには，サブドメイン名を利用するなどそれぞれで別ドメイン名とするか，セレクタ名を変えるなどの手法を用います．これらの手法では，公開鍵情報を含む DKIM レコードの位置が変わりますので，それぞれ別の鍵情報を利用できます．DKIM レコードの設定については，DNS 設定をする側が公開鍵の情報を受け取ったり，ネームサーバの委譲や別名定義をするなどの方法があります．

以下にメールの送信を別組織で行う場合の手法を示します．

- 送信委託先で鍵ペアを作成，公開鍵を入手し DNS に DKIM レコードを設定する（別セレクタ，サブドメインの利用）
- 鍵ペアを作成し，安全な方法での秘密鍵を委託先に渡し管理運用してもらう（別セレクタ，サブドメインの利用）
- サブドメインを作成し，委託先に管理を委譲する（但し，DKIM 以外のレコードも作成される可能性があるので注意が必要）

メール送信委託先が利用する鍵ペアを別にすることで，秘密鍵が漏れた場合の責任や影響をある程度限定させることができます．

■署名鍵の交換方法　DKIM 署名に用いる秘密鍵は，DNS の DKIM レコードに示される公開鍵とペアになっています．これらの鍵ペアは，鍵の安全性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．鍵ペアを変更する場合，受信側が認証する際に参照する，DKIM レコードに設定されている公開鍵を参照するタイミングも考慮しなければなりません．これらのことから，一定の期間の間，新旧の鍵ペアを共存させておく必要があります．

新しい DKIM レコードがメール受信側で参照できるようになるまでの時間（TTL 等）も考慮しておく必要があります．DKIM 署名に新しい秘密鍵を使う場合は，十分な時間的余裕をもって，対応する DKIM レコードを設定しておく必要があります．

DKIM では，セレクタを複数用意しておくことで，複数の鍵を共存させることができます．一般的な DKIM

の署名鍵の交換手順について示します.

1. 新しい鍵ペアを作成する
2. 新しいセレクタ名を作成し，鍵ペアの公開鍵を含む新しい DKIM レコードを新しいセレクタ名に設定する
3. 十分な時間の経過ののち，新しい鍵ペアの秘密鍵を DKIM 署名に利用する．新しいセレクタ名を DKIM-Signature ヘッダに記述する
4. さらに十分な時間の経過後，古いセレクタ名の DKIM レコードを削除する

■署名機能の外部利用　メール送信の一部を外部委託する場合の DKIM 署名のための鍵の管理については既に述べました．ここでは，外部委託先に DKIM レコードを委譲するもう一つの方法，CNAME 資源レコードを利用する方法について述べます.

CNAME は，正式名称に別名を付けるために利用される資源レコードで，これを DKIM の鍵管理および DKIM 署名を行うドメイン名を示す別名として設定すれば，あたかも自分のドメイン名で DKIM 署名および鍵管理を行っているようにみせることができます．例えば，鍵の管理および署名を行っているドメイン名を example.com とし，example.jp ドメイン名が鍵の管理及び DKIM 署名を委譲しているとします．この場合，example.jp ドメイン名の本来の DKIM レコードが設定されるドメイン名 (key1._domainkey.example.jp) に対して，DKIM レコードを設定する代わりに，委譲先の DKIM レコードを CNAME で別名定義します.

DKIM レコードの委譲

```
key1._domainkey.example.jp.   IN   CNAME   key1.example.com
...
key1.example.com.             IN   TXT     "v=DKIM1; p=ADfe34556..."
```

この設定により，メール受信側で example.jp ドメイン名の DKIM レコードを取得するために，key1._domainkey.example.jp の問い合わせを行った場合，結果として key1.example.com に設定された DKIM レコードが得られることになります．このような設定により，DKIM として認証された場合，DKIM 認証ドメインが example.jp ドメインとなります．これにより，DMARC 認証時にもヘッダ上の送信ドメイン名と一致させることができるようになります.

実際には，既に述べた通り DKIM の鍵交換のために複数のセレクタによる複数の鍵の共存期間が必要となりますので，CNAME で委譲する DKIM レコードも複数必要となります．通常は，以下に示すように，最低限 2 つの DKIM レコードが同時にアクセスできるようになっている必要があります.

鍵交換のための DKIM レコードの委譲

```
key1._domainkey.example.jp.   IN   CNAME   key1.example.com
key2._domainkey.example.jp.   IN   CNAME   key2.example.com
...
key1.example.com.             IN   TXT     "v=DKIM1; p=ADfe34556..."
key2.example.com.             IN   TXT     "v=DKIM1; p=A783Fg4556..."
```

DKIM レコードを委譲される側は，DKIM 署名および検証に必要な鍵ペアを独自に生成管理することができます．また，委譲元が DKIM レコードとして CNAME を設定するドメイン名及びセレクタ名を予め把握しておく必要があります．これらのドメイン名及びセレクタ名を，送信するメールに追加する `DKIM-Signature` ヘッダのパラメータ (`d`，`s`) タグに設定することになります．

■鍵交換の頻度　DKIM の署名および検証に利用する鍵ペアは，安全性の観点から定期的な変更が望ましいことを示しました．では，その変更頻度はどの程度の期間が望ましいでしょうか．運用の負担からは，なるべく鍵の交換が少ない方が良いはずですが，基本的には秘密鍵が十分安全である期間はそのまま維持しても良いでしょう．安全性の観点では，秘密鍵の保管方法やそれを守っているシステムの安全性，暗号の強度（鍵の長さやアルゴリズム）によって違いがありますし，鍵を求める新しい手法やそれを実行する計算機能力の向上など，鍵の安全性の期間については，今後も変化も含めて複合的な要因で決まるパラメータであると考えます．

とはいえ，現時点で DKIM 署名を運用していくためには，何らかの指標が必要であることも事実です．グローバルなセキュリティ団体である M^3AAWG では，DKIM の鍵交換に関する BCP[*2](Best Common Practices) を発行し，その中で幾つかの前提を述べた上で，現実的には 2 回/年は変更すべき，と述べています．

■署名の無いメール　DKIM では，DKIM 署名（`DKIM-Signature` ヘッダ）があるメールだけが認証の対象となります．`DKIM-Signature` ヘッダは，メールヘッダとしては必須ではないため，`DKIM-Signature` ヘッダが無いメールは単に DKIM 認証ができないだけで，それ自体が不正なメールと判断することはできません．そうした DKIM 署名が無いメールは，そもそも最初から DKIM に対応していない送信元からのメールかもしれませんし，たまたまそのメールが何らかの事情により DKIM 署名がつけられなかったのかもしれません．また，当然ながら詐称メールなど第三者が勝手に送信したメールである可能性も十分に考えられます．

こうした背景から，DKIM ADSP(DomainKeys Identified Mail Author Domain Signing Practices) が仕様として作られました．DKIM ADSP は，簡単に言えば必須ヘッダである `From` ヘッダのドメイン名 (Author Domain) から得られる特定のドメイン名に対して，ADSP レコードを設定できるようにし，その ADSP レコードに，DKIM の署名状況と署名が無いメールの取り扱い (`unknown`，`all`，`discardable`) を記述できるようにした仕様です．

DKIM ADSP の仕様が作られたあとに DMARC の仕様が作られました．DMARC では DKIM ADSP と同様に，認証のために `From` ヘッダのドメイン名を利用すること，認証ができないメールの取り扱いを DNS を利用して示す機能を実現します．そのため，現在では DMARC が DKIM ADSP に代わる技術仕様として

[*2] M^3AAWG DKIM Key Rotation Best Common Practices. https://www.m3aawg.org/sites/default/files/m3aawg-dkim-key-rotation-bp-2019-03.pdf

認識され利用されつつあります.

■DMARC 認証のための DKIM 認証　DMARC では，SPF および DKIM 認証できたドメイン名を利用しますが，送信側としてどちらか一方だけでも，正しく認証できれば DMARC として認証することができます．つまり，送信側として導入がしやすい SPF だけを導入（SPF レコードを設定）しても DMARC 認証は可能になりますが，SPF 認証の仕組み上，最終的なメール受信者に届くまでの経路を最初のメール送信側で制御することはできません．そのため，メール転送時など SPF だけでは正しく DMARC 認証できない場合があります．こうしたメール転送時の SPF 認証失敗による DMARC 認証の失敗を防ぐためには，送信側での DKIM の導入（DKIM 署名）が必要です.

DKIM を導入し，DMARC レコードを設定すれば，確実に DMARC 認証できるとは言えない場合もありますが，DKIM を導入することで，格段に DMARC 認証が成功する割合を増やすことができます．これは，受信側での SPF, DKIM, DMARC によるそれぞれの認証結果の組み合わせをみても，現時点では明らかな結果です.

■他の電子署名を利用したメール認証技術との違い　メールで電子署名を利用して認証する技術には，DKIM 以外にも S/MIME[*3] や OpenPGP[*4] があります．いずれもテキスト以外の情報をメールに取り込む MIME の仕組みを利用して，MIME パートに電子署名を取り込んだり，メッセージパート部分を暗号化し，復号化のための情報を別の MIME パートに示す仕組みです．電子署名には，DKIM と同様に公開鍵暗号技術を利用するため，S/MIME によるメールを送信する前に予め公開鍵に関する情報を渡しておく必要があります．OpenPGP も基本的には同じ手順が必要です．ここでは，S/MIME を例に DKIM との違いについて解説します.

S/MIME の歴史は古く，最初の仕様 (Version 3) が作られてから 20 年以上が経過しています．にもかかわらず，実用的に普及が進んでいるとは言い難い状況であるのには，理由があります．S/MIME は，メール送信者とメール受信者との間，End-to-End で共通した仕様によって基本的には利用される技術です．そのため，まず MUA やウェブメールシステム等などメール利用者が直接利用するシステムで機能が実装され，さらにそのメールの送受信者の間で利用することや方式が一致していることが前提です．その上でメールを送信する際には，メール送信先毎に証明書を予めメール等で受け取っておくなど，事前に入手する必要があります．メール受信時にもメール送信者が S/MIME に対応しており，メール受信者の証明書を既に保持していることによって，電子署名や暗号化の機能が利用できることになります．こうしたやりとりは，メールを送受信する相手の数だけ必要であり，相手毎に予め証明書を入手しておく必要もあります．証明書の信頼性を高めるためには，信頼性の高い認証局が発行した証明書の利用が推奨されますが，例えばメール利用者の数だけ証明書を発行する必要があるとすれば，かなりのコストを伴うことになります．また，安全性の観点から一定期間毎に証明書を更新する必要がありますので，導入時の一時的なコストということにもなりません．また，暗号化に利用した場合，受信時の処理方法にもよりますが，復号化せず暗号化したままメッセージを保管していた場合，復号のための鍵を更新して古いものを保持しない運用をしていた場合，元のメッセージを参照することもできなくなってしまいます.

DKIM は，基本的にメールサーバ間で電子署名の作成と検証を行いますので，個々のメールの利用者が何か新たな設定や作業は必要ありません．電子署名の検証に必要な公開鍵は，DNS の仕組みを利用して取得で

[*3] 最新の仕様は RFC8550(Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Certificate Handling) と RFC8551 (Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification)

[*4] RFC4880 (OpenPGP Message Format)

きますので，たとえばメールサーバ間で予め受け渡し等をしておく必要もありません．

最近では，こうしたDNSを利用して公開鍵の受け渡しをするプロトコルが増えており，メールサーバ間での通信の暗号化を行うTLS(STARTTLS)では，DNS上のTLSA資源レコードに証明書に関連した情報を設定するDANE(DNS-based Authentication of Named Entities)があります．S/MIMEやOpenPGPについても，DNS上にSMIMEA，OPENPGPKEY資源レコードを利用する仕組みが提案されています．

2.2.4 DMARC の設定

DMARC レコードを設定する際に重要なことは，ポリシー (p) タグの内容を検討することです．ポリシーには，none，quarantine，reject の 3 種類の値のうちいずれかを設定できます．メール受信側でなりすましメールを受け取らないようにするためには，より強いポリシーの値（quarantine もしくは reject）を設定すべきです．しかしながら，受け取ってもらうべき正規のメールが，SPF と DKIM で認証できない場合があったり，認証したドメイン名がヘッダ上の RFC5322.From のドメインと組織ドメインも含めて異なる場合がある場合は，メールが届かなくなってしまう場合があります．より強いポリシーを DMARC レコードに設定する場合は，DMARC レポートを受信し認証結果を参照することで，受信側での認証状況を事前に確認しておくべきです．

■DMARC レポートについて　DMARC レポートの送信先は，DMARC レコードに集約レポート（aggregate report, rua タグで指定）や失敗レポート（failure report, ruf タグで指定）それぞれに対するメールアドレスとなります．これらのメールアドレスが記述される DMARC レコードは，DNS の仕組みにより誰でも参照できる情報です．また，ドメイン名がわかれば，そのドメイン名に対する DMARC レコードの設定される場所も容易に類推できます．そのため，レポートの宛先に対しては，DMARC レポート以外にも不要な迷惑メールや偽の情報を含んだ悪意ある DMARC レポートが送信される可能性があります．DMARC レコードに記述するレポートの宛先（メールアドレス）では，通常のメール受信と同様に，送信ドメイン認証技術で認証したり必要に応じて悪意ある送信元であるかどうかを判断するなど，正しいレポートだけを受信できるよう対策をしておくべきです．

2.2.5 メールに利用しないドメイン名に対する設定

ドメイン名を取得したとしても，それを Web サイトにだけ利用するなど，メールに利用しない場合もあります．しかし，ドメイン名が存在（例えば A 資源レコードが参照できる等）する場合，それが送信ドメイン名に悪用される場合があります．こうした実在するドメイン名を悪用し，なりすましメールを送らせないための対策としても，送信ドメイン認証技術を利用することができます．

■送信ドメイン認証技術の利用　まず，SPF ではメールを送信しないドメイン名，という意味を示す SPF レコードの設定ができます．

```
example.jp.  TXT  "v=spf1 -all"
```

この設定では，SPF 認証が pass する送信元の IP アドレスの指定が無いため，全て末尾の-all に適合します．prefix が-（ハイフン）なので，いかなる送信元からのメールであっても認証失敗となります．

続いて，DMARC レコードとして以下を記述します．

```
_dmarc.example.jp.  TXT  "v=DMARC1; p=reject"
```

例で示した example.jp ドメイン名は，SPF 認証が失敗しますので，そのドメイン名での DKIM 署名がなければ，DMARC としても認証失敗します．上記の設定では，DMARC レコードのポリシーが reject ですので，DMARC ポリシーに基づいた受信処理を実施している場合，その受信側に届かないことになります．

結果として，example.jp ドメイン名のなりすまし（詐称）利用を防ぐことができます．また，このようなメールに利用しないドメイン名をなりすましている送信者の情報については，DMARC レポートの設定（rua タグまたは ruf タグ）をすることで得ることができます．

■MX レコードへの設定　送信ドメイン認証技術とは直接関係ありませんが，ドメイン名のなりすまし利用を防ぐもう一つの方法があります．null MX と呼ばれる MX 資源レコードの設定方法で，RFC7505 で規格化もされています．

```
example.jp.  MX  0 .
```

上記の通り，MX 資源レコードの優先度を示す数値 (preference number) として，最も優先度の高い 0 を指定し，さらに受け取り先を示すラベル（ホスト名）を長さ 0 に設定します（設定方法によっては ‘‘.’’）．この設定により送信先のメールサーバは，宛先ドメイン名の配送先が見つからない (Null MX) と判断することができます．これにより，メール送信時に送信メールアドレスが実在するかを確認するような送信メールサーバや，メール受信時に送信ドメイン名の MX レコードを確認するような受信メールサーバで，null MX であるかどうか判断すれば，送信ドメイン名がなりすましているかどうかを判断することができます．

送信メールサーバは，メール配送に際し宛先ドメイン名に対して MX 資源レコードを参照します．MX 資源レコードが取得できなかった場合には，A あるいは AAAA 資源レコードを参照し，SMTP の接続先の IP アドレスを得ようとします．上記のように，null MX レコードを設定しておけば，その後の A あるいは AAAA 資源レコードを参照することなく，送信処理を中断することができ，送信メールサーバにとっても必要の無い DNS 参照を軽減することで，処理の負荷を下げることができます．

2.3 メール受信側の設定

メール受信側で送信ドメイン認証を行うためには，SPF, DKIM, DMARC それぞれの認証機能を受信側のメールサーバに組み込む必要があります．DMARC 認証を行うためには，SPF, DKIM それぞれの認証結果が必要ですので，事前に認証しておく必要があります．

いずれの送信ドメイン認証技術でも，認証されたドメイン名は，間違いなくその送信元であることを示しているだけですので，認証が通った（pass した）メールだから受け取るべきメールである，とは必ずしもいえません．迷惑メール送信者が，取得した独自のドメイン名に正しく送信ドメイン認証の設定を行い，認証するメールを送信していることも十分考えられますし，実際にそうしたメールも多く存在します．そうした一方で，認証が通ったメールはそのドメイン名は詐称されていないわけですから，その認証したドメイン名から受け取るべきかどうかを判断することはできます．但し，よくあるドメイン名と字形的に紛らわしい誤読してしまうような文字列を利用している場合も考えられます（`m` の代わりに `r` と `n` を使う `rn` など）ので，視覚的な判断に頼るだけでは十分とはいえません．こうした認証したドメイン名を評価し受け取るべきかどうかを判断することが，送信ドメイン認証技術の活用方法の一つです．

こうしたドメイン名に対する判断の基準（評価）を，ドメインレピュテーションといいます．紛らわしいドメイン名には，視覚的なもの以外にも何らかの時限的なキャンペーン（*ex.* example2020.jp）を連想するような数値等を既存ドメイン名と組み合わせる方法など，様々ななりすまし手法があります．こうしたドメイン名が取得できないような対策を，ドメイン名のレジストラ側も実施すべきですし，そうした基準があいまいなドメインレジストラは，それ自体の評価にも影響するようになるでしょう．認証したドメイン名に対するドメインレピュテーションについても，今後検討していくべきと考えます．

ここでは，それぞれの認証時に注意すべき事柄について，まとめます．

2.3.1 SPF 認証

SPF 認証には，メールの送信元（受信するメールサーバへの直接の通信元）の IP アドレスが必要です．そのため，一番最初に受信するメールサーバ上で SPF 認証する機能を組み込む必要があります．但し，一番最初に受信するメールサーバから何らかの方法で送信元 IP アドレスを受け渡しできる場合（例えばメールヘッダ上の `Received:` ヘッダが付与する情報で判断できる場合等）には，最初のメールサーバ以降でも認証できる場合があります．利用する SPF 認証機能について，確認しておく必要があります．

■SPF レコードの意味的判断　SPF レコードは，単なる IP アドレスやネットワークアドレスだけではなく，ホスト名やマクロを利用した記述などもできることから，送信元の範囲がわかりづらい場合があります．そのため，実際は送信元 IP アドレスの範囲が広大であったり，どんな送信元でも認証が通ってしまうような SPF レコードであるかもしれません．こうした SPF レコードが設定されているドメイン名は，Botnet 等を利用したなりすましメールの送信ドメイン名に利用されている可能性があります．

メール受信側としては，SPF の認証が成功 (pass) したか失敗したかといった結果だけでなく，可能であればこうした SPF レコードの内容に基づく意味的な観点からの認証判断ができると良いでしょう．

■DNS への過度な負荷の軽減　SPF 認証のために，DNS への問い合わせが通常は複数回行われます．そのため，DNS 側への負荷を過度に高めることを目的とした DoS 攻撃，あるいは広範囲なメール受信者を利用し

た DDoS 攻撃などに SPF 認証が悪用（そうした目的を持った SPF レコードの設定）されることも考えられます．

SPF では DNS の参照回数に上限（10 回）が設けられていますが，その範囲内でも特定のドメイン名に過度の負担を強いるような攻撃が行われる可能性があります（送信量や設定している SPF レコードの内容等）．メール受信側で，こうした DoS 攻撃元となることを予測して防御することは簡単ではないですが，何かあった場合に DNS 参照を抑制できるような仕組みを用意しておくことは有益です．

■DNS を利用した受信側への負担　上記は，SPF レコードを設定する側が，関係のないドメイン名等に対する攻撃の手法ですが，DNS を管理する側で，意図的に応答を遅くしたりタイムアウトさせるなどの手法によって，SPF 認証するメール受信側に対して，認証処理の負荷を増やす方法も考えられます．

大量にメールを受信するメールサーバにとって，受信処理するメールが多く滞留してしまうことは，通常はメールサーバの負荷を増やすことになります．メール受信側としては，こうした異常状態が発生した場合に検知できる仕組みがあると対策がたてやすくなります．

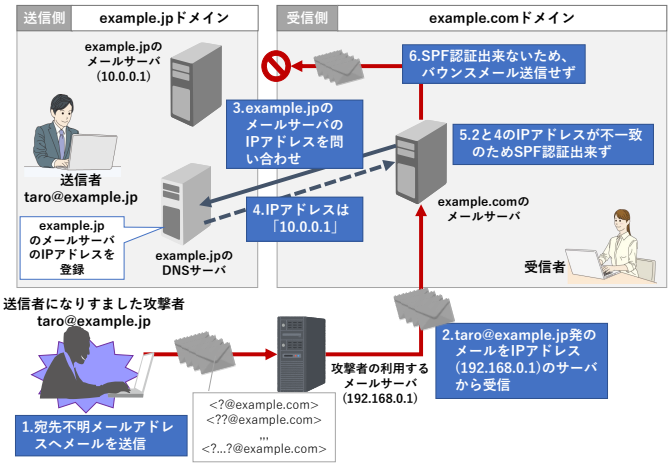

図 2.2　バックスキャッタと SPF 認証による抑制

■バックスキャッタ対応のための SPF 認証　メール配送のプロトコル SMTP では，一旦受け取ったメールが宛先不明等の理由により配送できなかった場合，送信元にエラーメール (Non-Delivery Notification) として返信（バウンス）します．現在では，こうしたバウンスメールの仕組みが，余計なトラフィックを増やしたり，これを悪用した迷惑メール送信や攻撃（バックスキャッタ）が発生しています．例えば，エラーメールを送信する受信側に対して，意図的に宛先不明となるメールアドレスを設定し，大量にメール送信することで，エラーメールの送信先に対して大量のエラーメールを送信し DoS 攻撃することができます．

バウンスメールの送信先は，SMTP 上の送信者，つまり RFC5321.From であり SPF が認証するドメインのメールアドレスです．メール受信側がバウンスメールの送信時に，元のメールの SPF 認証結果を利用し，認証できなかった（pass ではない）場合にバウンスメールを送信しないという仕組みができれば，バックスキャッタ攻撃を抑制できますし，不要なトラフィックを減らすことができます．

メール転送時に，転送先では SPF 認証が失敗してしまうため，転送先でバックスキャッタ対策としての SPF 認証結果利用を実施すると，本来エラーメールが送られる正規のメールに対しても，エラーメールが抑制されてしまう，という危惧も考えられます．しかしながら，そもそも転送先に配送できなかったメールにつ

いて元の送信者にエラーメールとして送信することの是非もあるので，こうしたエラーメールを抑制したとしても影響は限定的と言えます．さらにこうしたバックスキャッタの懸念等から，そもそもエラーメール自体を全く送信しない受信側も増えています．エラーメールは，ちょっとした宛先指定の間違いを気づかせることもできる機能ですので，全く送信しないよりは，現段階では限定的に活用していくべきと考えます．また，メール受信の最初のメールサーバで，宛先が存在するかどうかを確認することができれば，その処理（SMTP 上の）の途中でエラーコードを返すことができるはずですので，そもそもエラーメールを送信する必要もありません．こうした仕組みが実現できるかを検討するべきでしょう．

2.3.2 DKIM 認証

DKIM 認証は，メールの内容から作成される電子署名を検証することで認証を行います．そのため，メールの内容が電子署名作成時から変更されていなければ，いつでも DKIM での認証ができます．ただし，DKIM の認証（電子署名の検証）には公開鍵の情報が必要になるため，DNS で公開されている DKIM レコードにアクセスできる間は認証可能，ということになります．そのため，なるべくメール受信時に DKIM 認証するか，DKIM レコードを取得し保存しておく必要があります．

■署名作成方法の確認　DKIM 認証は，メールヘッダに付けられた DKIM 署名（電子署名）を検証することによって行われます．メール受信側では，この電子署名の作成方法についても注意する必要があります．

DKIM 署名の対象は，`DKIM-Signature` ヘッダの `h` タグで指定されたヘッダと，メール本文です．署名対象に含まれるメールヘッダとして，`From` ヘッダは必須となっています．メール受信者にとってもメールの送信者と考える情報であり，DMARC にとっても認証対象となる情報です．そのため DKIM 署名の検証の際は，`From` ヘッダが改変されていないことを検証するうえでも，`h` タグに `From` ヘッダが含まれていることを確認すべきです．

署名対象のメール本文についても注意が必要です．署名対象のメール本文の長さは `l` タグで指定します．指定する数値は Octet 値 (いわゆるバイト数) です．本文の長さ `l` タグを省略した場合は，メール本文全体になりますが，近年は添付ファイル等の利用も増えておりメールサイズも大きくなっているため，本文全体を署名対象に含めるような設定は非効率な場合があります．しかしながら，署名対象の長さの値が小さすぎる場合には，その長さ以降の本文を改変した場合でも検証できてしまいますので，ある程度の長さを設定しておくべきです．特に，次項で述べる replay attacks（再演攻撃）でも悪用される可能性がありますので，署名対象となる本文の長さにも注意すべきです．

■再演攻撃対策　再演攻撃 (replay attacks) とは，DKIM 署名を作成するメールサーバからの送信メールを再利用し，別のメール受信者に大量送信等することで，最初の署名ドメイン名のレピュテーション等を利用して届きやすくしようとするメール送信攻撃です．例えば，大手のフリーメールを利用して自分自身に送信したメールを再利用すれば，最初のフリーメールのメールサーバを経由させなくても，任意の宛先に大量に送信することができます．フリーメール側で迷惑メール送信防止策として送信数制限を設定していても，その制限によらず送信することができます．また，DKIM 署名付きの重要なメールを手に入れることができてその本文が短かった場合，その本文以降を利用して replay attacks により重要なメールを悪用することもできるかもしれません．

こうしたことからも，メール送信側は署名対象のメールヘッダと本文については何らかの配慮が必要であり，メール受信側は簡単に悪用されそうな状態の電子署名だったり，同じ電子署名のメールが大量に届いたり

する場合には，SPF の認証結果や送信元のドメイン名を確認するなど，別の方法を組み合わせるなどの対策が必要です．

2.3.3 DMARC 認証

DMARC は，SPF や DKIM で認証されたドメイン名とヘッダ上の送信者（`From` ヘッダ, RFC5322.From）が一致か同じ組織ドメインであるかどうかを認証します．組織ドメインとは，ドメイン名の登録事業者に登録されるドメイン名のことですが，実際には TLD(Top Level Domain) ごとにルールが異なっており，統一されたルールで組織ドメインを決めることは難しいため，現時点では public suffix リストを用いて判定することになっています．

DMARC では，ヘッダ上の送信者のドメイン名を認証しますが，なりすましメールや迷惑メールの送信者は，ヘッダ上の送信者欄（`From` ヘッダ）の補助情報であるディスプレイネームを悪用します．例えば，任意の文字列が設定できるディスプレイネーム部分になりすますメールアドレスやブランド名などの表示名を設定し，DMARC の認証対象であるディスプレイネームに続くメールアドレス (`<local-part@domain>`) 部分に，DMARC 認証が pass する全く別のドメイン名を設定することで，なりすまそうとしているドメインがあたかも認証できたように思わせようとします．これは，メールソフト (MUA) や Web Mail などが，利用者の利便性のためにディスプレイネーム部分を優先して表示する場合が多いことも悪用の要因となっています．

```
Subject: 請求書の送付
From: forged_mail_address@example.jp <real@example.com>
```

■認証ドメインの評価判定　DMARC に限らず SPF や DKIM でも同様ですが，送信ドメイン認証の結果が pass であっても，そのメールが迷惑メールではないということではもちろんありません．ただこれらの送信ドメイン認証技術で認証されたドメイン名については，送信者として識別できる情報であるということは，現在のところ十分に信用できる情報であるといえます．これら認証されたドメイン名，つまり送信者の情報を用いて，受け取るべきメールであるかどうかを判断することはある程度可能なはずです．この認証されたドメイン名を利用した判断，つまりドメイン名の評価の基準をレピュテーションと呼びます．

現在のところ，ドメイン名のレピュテーションに関する明確な基準といったものや，広く使われているサービス等はまだ無いと思いますが，今後の送信ドメイン認証技術の普及とともに迷惑メール判定の手法として期待される分野です．

■DMARC ポリシーと受信処理　DMARC レコードでは，DMARC ポリシーとして 3 つの値 (`none`，`quarantine`，`reject`) を設定することができます．これらの値は，ドメイン管理者がメール受信者に求める動作ですが，一般的に `none` 以外の 2 つがより強いポリシーと考えられています．また設定できるポリシーの中では，`none` や `reject` は理解しやすい動作ですが，`quarantine` は隔離の意味ですが一般的にそうした機能を持たないメール受信側は多いと思います．`quarantine` の意味するところは，DMARC 認証が失敗 (`fail`) した場合，そのメールは怪しいものとして取り扱うことを受信側に求める，メール受信者にそう思わせることを求める設定です．つまり例えば，迷惑メールフォルダといった機能があるのであればそこに保存するといった動作や，`[spam]` といった表示や何らかのマークをそのメールに付けるような動作が期待されるものです．

■DMARC レポートの送信　ポリシーの表明以外の DMARC の特徴の一つに DMARC レポートがあります．これまでの SPF や DKIM などの送信ドメイン認証技術では，送信側での設定が正しく機能しているのかを確認する方法がありませんでした．そのため，例えば SPF レコードの記述内容にフォーマットとしての間違いが無いか，設定したメールサーバ以外のところから正規のメールが送信されていないか，DKIM の電子署名が正しく作成されているか等について，送信側からでは把握することができず，また効果も見えづらいことなどによって，送信ドメイン認証技術の設定を躊躇する要因の一つと考えられてきました．

DMARC レポートでは，メール受信側からドメイン管理者側（正確には DMARC レコードに記述されているレポート送信先）へ，集約 (aggregate) レポートであればメール送信元（IP アドレス）や SPF, DKIM, DMARC の認証結果などを伝えます．これらの DMARC レポート情報から，正規に送信されたメールの認証状況や，それ以外のドメイン名をなりすますメールの送信数や送信元の情報を得ることができます．こうした DMARC レポートを多くのメール受信元から受け取ることで，送信ドメイン認証技術の設定状況や，なりすましメールの状況などをドメイン管理者は把握できるようになります．

これらの DMARC レポートは，例えば集約 (aggregate) レポートであれば，メール受信側が受信メールの状況を記録し，定期的に集計して DMARC レコードにレポート送信先を設定しているドメイン管理元に送信する必要があります．メール受信側にとっては，本来行うべきメール受信以外に必要となる新しい処理であり，受信側にとっては直接的には有益ではない処理と捉えられるかもしれません．しかしメール送信側やドメイン管理者側にとって DMARC レポートは，送信したメールがどのように認証されているか，管理しているドメイン名がどの程度なりすまされているかを知る有益な情報です．メール受信側が，DMARC レポートを送信することでメール送信側がこれらの情報を得ることができ，このことが送信側で送信ドメイン認証技術を導入する動機付けにもなり，受信側にとって送信ドメイン認証技術に対応したメールが増えることで，なりすますメールが検知しやすくなったり，ドメインレピュテーションを用いることでメールの振り分けができるようになるわけです．こうした循環となるよう，メール受信側での DMARC レポートを送信すべきです．

DMARC レポートの送信については，悪意ある DMARC レコードに注意する必要があります．関係の無い第三者に DMARC レポートが大量に送信されることで，DoS 攻撃とならないよう，DMARC レポート受信の委譲が設定されているか，送信頻度は適切か，失敗 (failure) レポートを送信している場合，それらが悪用されていないか等，ある程度の確認も必要となります．

2.4　メール再配送の課題

最初のメール作成者から，最後に届けられるメール受信者へ直接メール配送が行われない場合，最後のメール受信者での送信ドメイン認証技術 SPF, DKIM, DMARC が正しく認証できない場合があります．このようなメールの配送先が異なるようなメール配送の流れを，ここではメール再配送 (indirect email flow) と呼びます．こうした課題は，配送の途中に存在する中間者の処理の仕方によって，認証結果も異なってきます．ここでは，それぞれの再配送の場合ごとに，認証が正しく行われない原因とその対策について述べます．

2.4.1　メール転送

最初のメール送信者が，宛先に指定したメールアドレスに配送された後に，別のメールアドレスに配送するメール転送の仕組みが，メールがインターネット上で利用された初期の頃から利用されてきました．具体的には，メールボックス（メールの宛先）で".forward"（ドットフォワード）ファイルに転送先メールアドレスを記述するメール転送や，メールの受信側で実際の宛先を設定するエイリアス機能などです．

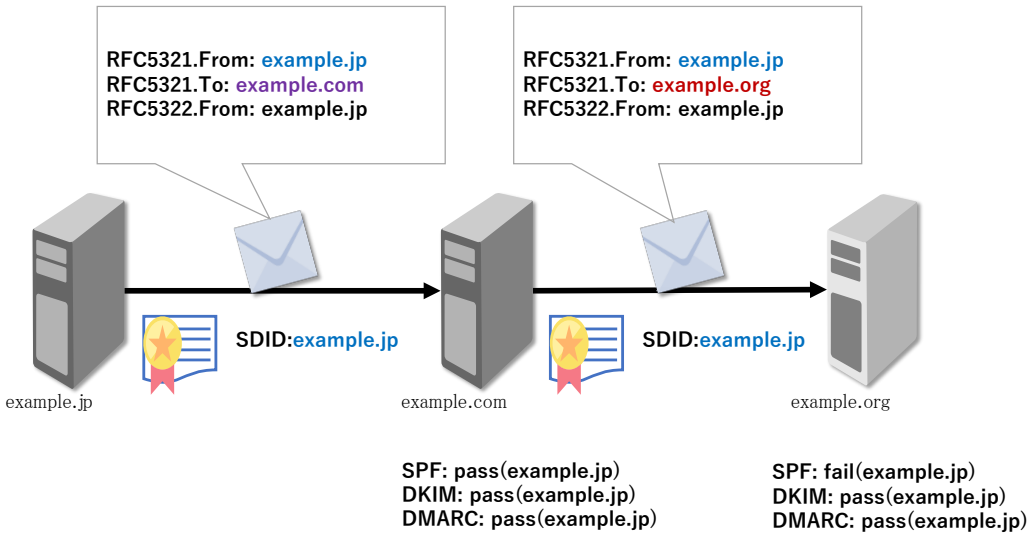

図 2.3　メール転送

メール転送による再配送の場合，メール本文の変更はほぼ行われず，メールヘッダ上の Received: ヘッダに経由したことが記される程度で転送先に送られます．この場合の送信者情報は，SPF の認証対象の RFC5321.From (envelope from) は，最初のメール送信者のままとなり，宛先の RFC5321.To のみが転送先と指定されたメールアドレスとなって転送先に配送されます．最終的な転送先 (example.org) では，SPF の認証対象となるドメインが RFC5321.From のままであるため，最初のメール送信者 (example.jp) を認証しようとしますが，転送先 (example.org) の配送元は，転送元 (example.com) であるため通常は SPF の認証が失

敗します．

最初のメール送信者 (example.jp) が DKIM 署名を付けていれば，転送でメール本文等はほぼ改変されませんので，最終的な転送先 (example.org) でも DKIM 署名は検証できます．この場合，DKIM の署名者 (SDID, Signing Domain Identifier) とメールヘッダの送信者 (RFC5322.From) のドメインが一致するか同じ組織ドメインである場合は，DMARC の認証も pass することになります．つまり，メール転送が行われる可能性があるメール配送経路については，最初のメール送信時に DKIM 対応（署名付加）しておけば，転送先でも正しく DMARC 認証できることになります．

2.4.2 メーリングリスト

メーリングリストは，特定のメールアドレスに届いたメールを，登録された複数のメールアドレスに再配送する仕組みです．前述のエイリアス機能を使った簡易的な方法でも実現できますが，現在では専用のソフトウェア[*5]を利用した運用が一般的となっています．

メーリングリストソフトウェアは，再配送先のメンバの管理（宛先不明となったメンバを配送保留や削除等を行う）を行うため，投稿者 (Submitter) から送信されたメールを一旦受け取り，エラーメールを受け取るために RFC5321.From (envelope from) をメーリングリストを運用しているドメインに設定し，メーリングリストのメンバ (Subscriber) 宛てにそれぞれ配送します．メーリングリストとして SPF を認証させるためには，メーリングリストのドメイン名 (example.com) に SPF レコードを設定し認証できるようにします．最終的なメール配送先であるメーリングリストのメンバ (example.org) では，SPF の認証は pass しますが認証されるドメイン名はメーリングリスト (example.com) となります．そのため，メールのヘッダ上のドメイン名は最初のメール投稿者 (example.jp) のままのため，DMARC としてはドメイン名が一致しない (example.jp ≠ example.com) ため，DMARC 認証としては失敗します．投稿者側で DKIM 署名をしていれば，メール本文等の改変が無ければメーリングリストメンバ側では DKIM の認証ができますし，メールヘッダ上のドメイン名も同じですので，DMARC も認証できます．

しかしながら，現在のメーリングリストの使われ方の多くは，メールの件名（Subject ヘッダ）にメーリングリストであることを示す文字列を挿入したり，メール本文の最後にフッタとして文字列を追加するといった運用がよく行われています．メーリングリスト側で，こうしたメール改変の処理を行うと，投稿者の DKIM 署名が合わなくなり DKIM の認証が失敗します．これを回避するために，メーリングリスト側でメールの改変後に DKIM で再署名を行えば，DKIM としては認証できますが，署名を作成できるのはメーリングリストのドメイン名 (example.com) としてです．よって DMARC としてはヘッダ上の送信者のドメイン名と署名ドメイン名とが一致しなくなるため (example.jp ≠ example.com) 認証が失敗します．

こうしたメーリングリストによるメール再配送の課題を解決する方法としては，以下の三つの方法があります．

- メール内容の改変をしない
- メーリングリストドメイン名での DKIM 再署名と RFC5322.From の変更
- ARC の利用

DKIM 署名対象となっているメールヘッダや本文を変更しなければ，メーリングリストへの投稿者が付け

[*5] Mailman などが広く使われています

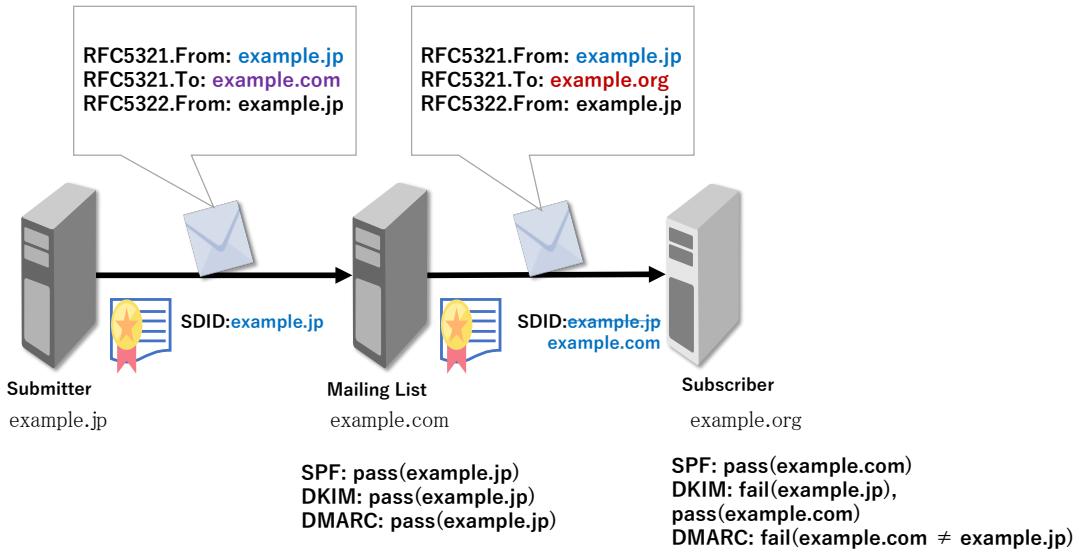

図 2.4　メーリングリストによるメール再配送

た DKIM 署名はそのまま検証できますので，メーリングリストメンバ側でも DMARC は認証できます．但し，これはメール転送によるメール再配送の課題でも同様ですが，最初のメール送信側で DKIM 署名に対応している必要があり，DKIM の普及に依存した解決方法と言えます．

メーリングリスト側でメールヘッダ上の送信者 (RFC5322.From) 情報をメーリングリストのドメイン名に変更し，DKIM で再署名すれば，メーリングリストのメンバ側では SPF も DKIM もメーリングリストのドメイン名 (example.com) で pass できますし，そのドメイン名は RFC5322.From のドメイン名とも一致しますので DMARC も pass します．この方法の利点は，メーリングリスト側の処理の変更だけで対応できる点で，メーリングリストへの投稿者やメンバ側は通常のメール送受信と変わらない動作となる点です．つまり，メーリングリストへの投稿者が必ず DKIM に対応していなくても良い（メーリングリスト側は別途正しい投稿者からのメールであるかを確認すべきですが）ですし，メーリングリストのメンバ側で送信ドメイン認証を導入していれば正しく送信ドメイン名を認証できることになります．一方で従来の運用方法と異なる点としては，メーリングリストメンバからみてメールの投稿者がわかりづらくなる部分です．こうしたデメリットを緩和するために，メーリングリスト機能側で最初の投稿者の情報を RFC5322.From のディスプレイネーム部分に残しておく処理も行われます．ただこの方法では，メール投稿者の最初のディスプレイネームの情報が失われてしまいますので，いずれにしても全く従来の方法と遜色が無いとは言い切れません．メーリングリストソフトウェアとして広く使われている Mailman では，こうした RFC5322.From の書き換えによる DMARC への対応方法の機能が最新版では利用できるようになっています．

ARC[*6]は，メールが再配送などメールサーバを経由する都度，認証を行いそれらを繋いでいくことで認証の連鎖 (Chain) を構成していく仕組みです．原理的には，メールを受け取る時にその送信元が信頼できる送信

[*6] The Authenticated Received Chain (ARC) Protocol, RFC8617

元である場合，その信頼する送信元が認証したその前の送信者も信頼できる，といった連鎖をつないでいきます．信頼の連鎖を構築するために，以下の 3 種類のヘッダが新たに提案されました．

AAR (ARC-Authentication-Results)： 従来の Authentication-Results ヘッダと同様の認証結果を示すものだが，ARC ヘッダセットを区別する Instance Tag（数値で示される）が追加された
AMS (ARC-Message-Signature)： 従来の DKIM-Signature ヘッダと同様に再署名に関する情報を示す
AS (ARC-Seal)： ARC 関連ヘッダを順番ごとに連結したデータから生成される電子署名

ARC は技術的には DKIM と同じ電子署名を利用しますが，仕組みとしては DKIM やそれを利用する DMARC とは関連しない別の仕組みとなっています．例えば，DMARC としては認証が失敗 (`fail`) する場合でも，ARC としては `pass` することがある，むしろそうした認証結果が不一致となる場合に信用の連鎖を用いてメールを認証するための新たな仕組みです．この信頼の連鎖を実現するためには，少なくとも直前のメール送信者（認証および署名者）が何らかの方法で信用できていることが前提となります．

送信ドメイン認証技術は，メール配送に関わるメールサーバ（送信側と受信側）それぞれでの導入によって認証が実現します．メーリングリストの課題に対する対策として 3 つの方法を述べましたが，これまでのメールの利用形態をなるべく維持したまま，メールシステム全体として変更する部分をなるべく少なくするためには，現時点ではメーリングリストサーバ側の修正（DKIM 再署名と RFC5322.From の変更）が望ましい手法といえるでしょう．