送信ドメイン認証技術 DMARC 導入ガイドライン

迷惑メール対策推進協議会 技術ワーキンググループ

はじめに

電子メールは，モバイルも含めたインターネットにおけるコミュニケーションの基盤ツールであり，メッセージの交換だけではなく，様々なデータの受け渡しにも利用される情報交換の手段としても広く利用されています．さらに送受信者を示すメールアドレスは，各種認証のための識別子 (ID) として利用されており，重要な情報の 1 つとなっています．しかしながらメールの配送の仕組みでは，当初はメール受信時に送信者を示すメールアドレスが正しいかを検証する手段がありませんでした．そのため，メール利用者は必要の無い迷惑メール，特になりすましメールなどによってもたらされる様々な被害，あるいはその可能性に脅かされてきました．こうした背景から，メールの送信者をドメイン名単位で認証する，送信ドメイン認証技術の仕様が開発され，メールシステムに組み込まれ普及が進んできました．

送信ドメイン認証技術には，認証する送信者情報や認証に用いる仕組みが異なる 2 つの認証方式，SPF, DKIM があります．送信ドメイン認証技術 DMARC は，これら 2 つの認証結果を利用し，メール受信者が一般的に送信者と考える，メールヘッダ上の送信者 (ヘッダ From) との整合性を確認し，認証する技術です．その意味で，DMARC は総合的な送信ドメイン認証技術といえます．

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は，既存のメール配送の仕組みの上に新たに組み込まれた技術であるため，既に普及している幾つかのメール利用形態に対して，正しく機能しない場合もあります．

本ガイドラインは，こうした背景を踏まえて，できる限り多くの正しく送信されたメールが，受信側でも正しく送信ドメイン認証技術によって認証できるために設定すべきこと，考慮すべき事柄をまとめたものです．対象とする送信ドメイン認証技術は，DMARC(Domain-based Message Authentication, Reporting, and Conformance) ですが，DMARC は認証の仕組みとして SPF(Sender Policy Framework) と DKIM(DomainKeys Indentified Mail) を利用しますので，これら二つの送信ドメイン認証技術に関しても，設定すべき事柄を記載しています．本ガイドラインで対象とする仕様は，DMARC が RFC7489[3], SPF が RFC7208[1], DKIM が RFC6376[2] です．これらの送信ドメイン認証技術の仕組みの詳細や導入に際して必要となる各種パラメータ等については，迷惑メール対策推進協議会が発行している送信ドメイン認証技術導入マニュアル (導入マニュアル)[9] を参照してください．

本ガイドラインでは，現時点で設定および導入すべき事柄を，設定しなければならない (Must)，設定した方が良い (Should)，設定を勧める (May)，といった 3 つのレベルで示しています．

迷惑メール対策推進協議会 技術ワーキンググループ 主査
櫻庭 秀次

目次

1　本ガイドラインについて

電子メールシステムには，メッセージの送り手である送信側と，送信側からのメッセージを受け取る受信側が存在します．送信ドメイン認証技術は，送信側と受信側の双方が対応しなければメールを認証することができません．つまりメール受信側で送信ドメイン認証の認証機能を導入したとしても，メールの送り側が送信ドメイン認証に対応した設定をしていなければ，そのメールで示された送信者情報のドメイン名が正しいものであるかを判断（認証）することはできません．逆にメール送信側が設定したとしても，メール受信側に認証機能がなければ，送信者を正しく判断することはできません．多くの場合，メールの受信側はメールの送り手でもあり，逆もまた同様であることから，メールの利用者としては相互にそれぞれの立場で送信ドメイン認証技術に対応すべきです．

メールの送信側が設定すべきこととして，メールの送信者を示す送信ドメイン名に対して，DNS への設定が必要になります．また，DKIM を導入するためには，送信メールサーバへの機能追加が必要になります．そのため，送信ドメイン認証技術 DMARC を送信側で導入するためには，ドメイン名の管理者とメールサーバの管理者の設定作業が必要になります．自組織でメールサーバを運用していない場合には，クラウドサービスなど，利用しているメールサービスの提供機能を確認し，適切な設定を行う必要があります．

メールの受信側が設定すべきこととしては，受信メールサーバでメール受信時に送信ドメイン認証技術によって認証する機能を設定する必要があります．自組織で受信メールサーバを運用している場合は，受信メールサーバソフトウェアへの機能追加が一般的に必要となります．クラウドサービスなど，外部のメールサービスを利用している場合には，提供機能を確認し適切な設定を行う必要があります．さらに，メール受信時に DMARC に対応していないメールに対する受信処理や，DMARC の認証に失敗した場合に，DMARC ポリシーに基づいた受信処理を行うのか，独自の対応を行うのか方針を決めておく必要があります．

メーリングリストやメールの転送サービスを提供している場合は，メールの再配送先でも DMARC の認証ができるように，適切な再配送設定を実施する必要があります．

このように，メールシステムの中で DMARC が機能し利用できるようにするためには，メールの送受信側およびメールの再配送に関わるそれぞれの立場で，関連する機能のそれぞれの担当者が設定や判断を行うことが必要です．本ガイドラインは，これら様々な立場の担当者が，様々な判断や設定のために必要な事柄をまとめたものです．

本ガイドライン案は，令和４年度総務省事業「ISP におけるネットワークセキュリティ技術の導入に関する調査」及び令和５年度総務省事業「ISP におけるネットワークセキュリティ技術の導入及び普及促進に関する調査」の結果として，同実証事業へ参加した実証事業者の意見・有識者検討会メンバーの意見を基に作成されました．本ガイドライン案作成には，同実証事業の有識者検討会メンバーと協力者の合意を基にしています．インターネットにおける様々な技術と同様に，送信ドメイン認証技術についても，利用の過程や新たな技術の開発等により変化していくことが予想されます．そのため，本ガイドラインは，迷惑メール対策推進協議会の技術ワーキンググループで継続して議論を行い，改訂していくことを予定しています．同様に発行している，「送信ドメイン認証技術導入マニュアル」と合わせて，技術仕様の改訂やメールの利用形態の変化等に合わせて，今後も見直していく予定です．

2　メール送信側

本章では，送信ドメイン認証技術におけるメール送信側，すなわちメール送信側が用いるドメイン名に対する各種設定なども行う，ドメイン名の管理者も含めて実施すべき事項を示します．

2.1　送信側の送信ドメイン認証設定

送信ドメイン認証技術 DMARC をメール送信側で導入するためには，SPF あるいは DKIM のいずれかの導入が必要になります．また SPF と DKIM の両方を導入することで，正しく送信されたメールが受信側で DMARC で認証できるメールをより増やすことが期待できます．SPF, DKIM, DMARC いずれの技術も，対象とする送信ドメイン名に対して DNS への設定が必要になりますので，当該ドメイン名の管理者が設定する必要があります．

---

1. メールの送信ドメインに DMARC レコードを設定することで DMARC を導入する，導入に際しては SPF あるいは DKIM を送信側として導入しなければならない
2. メール送信側として DMARC を導入する場合，SPF と DKIM の両方を導入した方が良い

DMARC レコードで設定しなければならない重要な情報にポリシー[*1]があります．これは，認証が失敗したときの取り扱いをメール送信側がメール受信側に示す情報になります．メール送信者がメール受信者に受け取ってほしいと考えるメール全てが，DMARC で必ず認証できる確証がない場合は，ポリシーを none (`p=none`) から設定すべきです．ポリシーの強度をより上げていくことで (`p=quaratine` や `p=reject`)，なりすましメールがメール受信者に届くことを抑制することができます．ポリシーの強度を上げていくためには，DMARC レポートを受信し，送信したメールの DMARC 認証の結果を確認し，SPF, DKIM を含めた設定が正しく認証できるようになっているかを確認するといった方法があります．

---

3. DMARC のポリシー設定は, `p=none` から始めて認証結果を確認することで `p=quarantine`，`p=reject` と強度を上げていく方が良い
4. DMARC のポリシー強度を上げるためには，DMARC レポートを受信し，認証結果を把握した上で判断していくことを勧める

SPF レコードを DNS に設定する際には，設定内容が仕様に沿った正しい SPF レコードであるかを事前に確認しておくべきです．誤った SPF レコードを設定した場合，正規のメールであってもメール受信側では認証結果が `permerror` となり，正しく認証できないことになります．また，SPF レコードで `include` や `redirect` を用いて他の管理元のドメイン名を利用する場合は，当該ドメイン名の SPF レコードの管理元の都合によって変更される可能性があり，それによってエラー（`permerror`）となる可能性もあるため，注意が必要です．

[*1] DMARC のポリシーは，DMARC レコードの `p=`で示すパラメータとして設定します

5. 設定する SPF レコードの内容は，事前にチェックサイト等で確認することを勧める
6. SPF レコードで他の管理ドメイン名を利用する場合は，利用元のドメイン名の状態を含め定期的に確認した方が良い

DKIM は電子署名を認証に用いるため，SPF と比較して，メールの配送経路によらない堅牢な認証方法といえます．その一方で，1 度認証されたメールを再利用する Replay Attack などの手法の懸念もあります．DKIM を送信側として導入する場合は，こうした手法に悪用されないような設定を行うべきです．

7. DKIM の署名対象には，必須ヘッダ（From:）以外にも送信者や受信者を示す情報，日付や `Subject:` などの推奨ヘッダを含めるとともに，署名対象の本文を示す情報 `l=`についても，再利用された場合でも区別できるよう十分な長さとしなければならない

DKIM の仕様 [2] では，署名の対象とすべき必須ヘッダは `From:` ヘッダだけですが，署名の対象としないことにより，そのヘッダ情報が書き換えられて再利用されることで，DKIM で認証できるなりすましメールを送られてしまう可能性があります．メール送信時の DKIM 署名の際に `From:` ヘッダが署名すべき情報 (ドメイン名など) であることを確認することは当然ですが，メール内容を示す情報 (`Subject:` ヘッダやメール本文など) や，送信者を示す情報などが改ざんされないよう，署名対象に含めるべきです．DKIM の仕様 [2] の `5.4.1` 節では，署名対象に含めるべき推奨のヘッダが示されています．日本語の情報としては，導入マニュアル [9] の `1.4.3` 節に記載されています．また，署名対象とするメール本文の長さ (オクテット値) を `l=`で示すことができますが，省略した場合はメール本文全体となります．しかしながら，添付ファイルなど大きなデータを含んでいる場合は，本文全体を署名対象をすると署名作成および検証のための負荷が大きくなってしまう可能性があります．署名対象とするメール本文をどの程度の長さとするかは，署名作成機能の処理能力と改ざんされる危険性をそれぞれ考慮し，判断することになります．

2.2 DMARC の組織ドメイン名への設定

送信ドメイン認証技術の SPF, DKIM については，認証対象のドメイン名それぞれに対して，対応する SPF レコードと DKIM 鍵レコードの設定が必要になります．DMARC の場合は組織ドメイン名の仕組みがあるため，組織ドメイン名を含む配下のサブドメイン名全てのドメイン名に対する DMARC の標準的なポリシーを，組織ドメイン名に対して設定することができます．一般的には，登録したドメイン名と参照可能なそのサブドメイン名全体について，悪用されないための標準的な設定をポリシーとして記載し，メールに利用するドメイン名については個別の DMARC レコードを設定します．

8. 組織ドメイン名には DMARC レコードを設定しなければならない
9. メールに利用しないサブドメイン名に対する DMARC ポリシーの設定として，組織ドメイン名以下の DMARC ポリシー (`p=` または `sp=`) は，`reject` と設定した方が良い
10. メールに利用するドメイン名には，個別に DMARC レコードを設定した方が良い

メール受信時に，送信者情報に含まれるドメイン名が存在するか (DNS で名前解決できるか) を確認する手法は，迷惑メール対策として一般的に行われています．しかしながら，メールに使わないドメイン名であっても DNS で参照可能となっている場合，そのドメイン名が悪用されてしまう可能性があります．そのため，送信ドメイン認証技術として明示的に認証が失敗し，受け取らないような設定 (`p=reject` など) をすべきです．

2.3 メールに利用しないドメイン名への設定

登録したドメイン名をメール送受信の用途で利用しない場合や，登録した直後でまだすぐにメールに利用しないようなドメイン名[*2]を，なりすましなどの悪用を防ぐための送信ドメイン認証などの設定方法があります．具体的には，SPF レコードとして認証が必ず失敗する`-all` だけの設定と，DMARC レコードとして `p=reject` を設定する方法です．DKIM は送信側で機能を組み込まなければ認証が pass することはありませんので，特に設定は不要です．また，合わせて Null MX[*3]を設定する方法があります．

```
          example.jp. MX  0 .
          example.jp. TXT "v=spf1 -all"
_dmarc.example.jp. TXT "v=DMARC1; p=reject"
```

---

11. メールに利用しないドメイン名は，SPF 認証が必ず失敗する SPF レコードとポリシーが “reject” である DMARC レコードを設定し，Null MX の設定をした方が良い

サブドメイン名も含めてメールを送信しない場合は，上記 DNS 設定をワイルドカードで設定する方法もあります．しかしながらワイルドカード設定は，いかなるラベルであっても存在するドメイン名として参照できてしまうため，利用には注意が必要です．

2.4 DMARC レポートの活用とポリシーの強化

DMARC のポリシーを強化することで，メール受信者へのなりすましメールの到達を防ぐことができます．また，メール受信者が DMARC によって認証されたことが確認できることで，メールの送信者を正しく確認することができるようになります．しかしながら，送信されたメールがメール受信者に到達する過程で，配送経路の変化等により必ずしも正規のメールが正しく認証されない場合もあります．メール送信側が，メール受信側での認証結果を得る手段として，DMARC レポートがあります．

DMARC レポートには，集約レポート (aggregate report) と失敗レポート (failure report) の 2 種類があります．いずれのレポートもメールとして DMARC レコードに設定された送信側に送信されます．失敗レポートは，メール受信側で DMARC 認証が失敗した場合にその都度送信されるレポートですが，レポート送信の負荷や情報の取り扱いの懸念などから，現時点ではまだそれほど多くのメール受信側が対応していません．メールの認証状況を把握するには，現時点では集約レポートが有益な情報となっています．集約レポートは，メールで MIME[*4]形式で添付ファイルと同様に送られてます．集約レポートの内容は，機械的に処理可能な

[*2] こうしたドメイン名を Parked と呼びます．
[*3] A “Null MX” No Service Resource Record for Domains That Accept No Mail (RFC7505)
[*4] Multipurpose Internet Mail Extensions.

XML[*5]形式となっており，圧縮されたファイルとして添付されます．そのため，集約レポートをメールとして人が受信し，内容を確認することは一般的に困難であるため，何らかのツールや解析機能を提供するサービスの利用を検討すべきです．

---

12. DMARC レポートを受信し送信メールの DMARC などの認証状況を把握するために DMARC レポート，特にレポート数の多い集約レポート (aggregate report) を受信した方が良い
13. DMARC のポリシーは `reject` まで設定できることを目指し，そのために受信側の SPF, DKIM, DMARC の認証状況を把握した方が良い
14. DMARC レポートの受信および分析にはツールや分析サービスを利用して認証結果を把握することを勧める
15. 送信ドメイン名（管理ドメイン名）以外の宛先で DMARC レポートを受信する場合は，DMARC レポートの受信先で委譲されていることを示す設定をしなければならない

DMARC レポートを利用するために，外部のサービス等を利用してメール送信に使われるドメイン名以外のレポート宛先を設定する場合，レポート宛先のドメイン名側で，移譲されていることを示す設定が必要です．この設定方法は，DMARC の仕様 [3] の 7 章，および導入マニュアル [9] の `1.5.5` 節に示されています．これは，勝手に第三者のメールアドレスを設定し，不要な (DMARC レポート) メールを大量に送信させる DDoS のような悪用を防ぐための仕組みです．

[*5] Extensible Markup Language.

3　メール配送事業者の送信ドメイン認証設定

メール配信事業者とは，ここではメールマガジンなど多数のメール受信者へのメール送信を，依頼元に代わって送信する事業者としています．メール配信事業者は，多くの場合短時間で大量のメール送信が可能な設備を有するため，大量のなりすましメール送信に加担しないような運用が必要です．そのためメール配信事業者は，メール配信の依頼元の信頼性の確認や，場合によっては送信するメールの内容などを事前に確認できることが望ましいといえます．またメール受信側に対して，メール送信元を判断できるよう送信ドメイン認証技術を正しく設定すべきです．

3.1　認証ドメイン名の扱い

メール配信にあたり，依頼元のドメイン名をヘッダ `From:` (RFC5322.From[*6]) に用いる場合，DMARC の認証が失敗しないよう SPF や DKIM の認証ドメイン名が依頼元のドメイン名となるよう設定する必要があります．ここでは，メール配信が配信事業者のホスト (設備) を利用し，DKIM 署名を配信事業者のメールサーバ等を用いて行う場合の設定について示します．

---

1. メール配送事業者が送信するメールは，DMARC の認証ができるよう SPF, DKIM, DMARC の設定しなければならない
2. メール配信事業者は，依頼元のドメイン名の SPF レコードの設定のために，`include` 用の SPF レコードを作成し提供した方が良い
3. メール配信事業者は，依頼元に対して DKIM の公開鍵の情報を提供するか，CNAME 参照用の DKIM 鍵レコードとセレクタ名等の情報を提供した方が良い
4. メール配信の依頼元は，ヘッダ `From:` に自組織のドメイン名を設定する場合，配信事業者からの情報に基づき，SPF, DKIM, DMARC が正しく認証できるよう設定しなければならない

送信メールが DKIM に対応するためには，DKIM 署名のための秘密鍵が必要です．秘密鍵は，その性質から漏れないよう厳重な管理が必要ですが，メール送信の依頼元とメール配信事業者のどちらが用意 (管理) するかを考える必要があります．通常は DKIM 署名作成に秘密鍵が必要なため，メール配信事業者側が管理する方法が一般的であり，その場合，秘密鍵と対になる公開鍵を DKIM 署名ドメイン名の管理側に提供する必要があります．これには公開鍵の情報を直接渡す方法と，DNS の仕組みとして CNAME を利用して参照可能にするか，いずれかの方法でメール配信事業者側が提供することになります．

[*6] メール形式の仕様である RFC5322 からヘッダ From をこのように表記する場合があります

4　メール再配送時の設定

メール作成者によって送信されたメールが，送信先のメールアドレスから別のメールにアドレスに自動的に送信されるメールをここでは再配送 (indirect mail flow) と呼びます．具体的には，転送メールやメーリングリストに投稿されたメールなどが該当します．

4.1　転送メールの設定

受信したメールを機械的に別のメールアドレスに送信するメールを，ここでは転送メールと呼びます．転送メールの送信時の SPF 認証に関わる設定方法として，受信時のエンベロープ From(RFC5321.From[*7]) をそのまま転送時にも利用する方法と，転送元のドメイン名を RFC5321.From に設定する場合があります．受信時の RFC5321.From をそのまま転送時にも利用する場合，転送先で SPF の認証が失敗します．転送元のドメイン名を RFC5321.From に設定する場合，転送先で SPF は認証できますが，ヘッダ `From:` を書き換えない場合，通常は DMARC の認証が失敗してしまいます．

---

1. 送信するメールが転送される場合は，DKIM 認証に対応しなければならない
2. 転送先のメール受信側が SPF 認証できるメールを受け取る場合は，転送時に RFC5321.From を転送元ドメイン名に書き換える設定を勧める
3. 転送時に転送元ドメイン名を書き換えて転送する場合は，エラーメール (NDR[*8]あるいは DSN[*9]) がループしないような処理をしなければならない

送信したメールが最初の宛先以外に転送されるかどうかを事前に判断することは一般的に困難です．そのため，SPF の認証にだけに依存するのではなく，あらかじめ DKIM にも対応したメールを送信すべきです．

4.2　メーリングリストの設定

メーリングリストは，登録されたメンバから投稿 (送信) されたメールを受信し，それをメンバ全員に再配送する仕組みです．メーリングリストでは，Mailman などのメーリングリストソフトウェアを利用している場合，メンバへの再配送時には，エンベロープ `From:`(RFC5321.From) をメーリングリストを運用しているドメイン名に設定して送信するため，SPF では認証できますが，ヘッダ `From:` の書き換えを行わない場合，SPF の認証ドメイン名と異なることことから DMARC 認証が失敗することになります．また，古いメーリングリストソフトウェアを利用していて，RFC5321.From をメーリングリスト投稿者のメールアドレスをそのまま利用するような場合，SPF の認証自体も失敗します．

メーリングリストでは，メーリングリストからのメールであることを受信者が判断しやすくするため，`Subject:` ヘッダに情報[*10]を付加したり，本文の末尾にメーリングリストに関する情報を付加することが行わ

[*7] メール配送の仕様である RFC5321 からこのような表記をする場合があります

[*8] Non-Delivery Report

[*9] Delivery Status Notifications

[*10] `Subject: [mailing list 101]` **メーリングリストの例**

れます．こうした場合，メーリングリスト投稿者が DKIM に対応したメールを送信したとしても，メーリングリスト参加者が受信するメールは DKIM の認証が失敗します．

---

4. メーリングリストからの再配送時には，RFC5321.From と RFC5322.From にはメーリングリストのドメイン名を設定しなければならない
5. メーリングリストからの再配送時には，メーリングリストのドメイン名による DKIM 署名を付加しなければならない (DKIM 再署名)
6. メーリングリストのドメイン名では，SPF レコードと DKIM 鍵レコード，DMARC レコードを公開し，それぞれに対応した設定をしなければならない
7. メーリングリストのメンバが ARC[*11] に対応している場合は，ARC を導入することを勧める

ARC はメールが再配送されるメールでも認証できるように作られた仕様ですが，再配送の各経路で ARC 認証と再署名が必要になりますし，最終的な受信者への到達時にも ARC 認証とこれまでの経路の認証結果を信頼するための何らかの評価が必要です．こうした複雑性もあり，ARC は普及しているとは言い難い状況がありますが，メーリングリストなど参加者が限られた範囲で十分に機能するのであれば，導入を検討すべきです．一方で，ARC 署名と DKIM 署名はそれぞれ同じような処理を行いますし，DKIM 認証を行うメール受信者も ARC に比べれば多いと考えられますので，現時点ではメーリングリストによる再配送を行う際には，SPF, DKIM および DMARC に対応した処理を行うことが，より効果が得られる場合が多いと考えています．

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

5　メール受信者

受信したメールが，なりすましメールであるかどうかを判断するために，メール受信時に DMARC 認証します．DMARC 認証するためには，SPF 認証と DKIM 認証を実施する必要があります．迷惑メール特にフィッシングは，さまざまな手法で特定のサービスや事業者をなりすまそうとするため，DMARC などの送信ドメイン認証技術で認証できたとしても，なりすましメールでないとは限りません．認証されたドメイン名が受け取るべきメールであるかを確認する必要があります．

5.1　送信ドメイン認証

メール受信側は，SPF, DKIM, DMARC による送信ドメイン認証を行い，メール受信者に認証結果を提示するべきです．なりすましメールは，メール受信者に対して様々なトラブルを発生させる要因でもあるため，送信ドメイン認証技術を利用してなりすましメールが届かないような受信処理をすべきです．

---

1. メール受信時に SPF, DKIM, DMARC 認証を行い，送信側の DMARC ポリシーに対応した受信処理を行わなければならない
2. SPF 認証ができたとしても，不正な SPF レコードを設定して pass した可能性もあるため，SPF レコードの内容についても確認することを勧める
3. DKIM 認証ができたとしても，Replay Attack の可能性もあるため，署名対象の情報が十分であるか等確認することを勧める

SPF レコードでは，より大きな範囲のネットワークアドレスをメール送信元として設定したり，いかなる送信元からのメールでも SPF 認証が pass となるような設定をすることができます．こうした SPF レコードの設定をしているドメイン名は，逆に送信ドメイン名のレピュテーションとして低くすべきですし，こうした設定内容を認証時に判断できるような仕組みも有効です．DKIM 署名対象のヘッダは，`DKIM-Signature:` ヘッダに記載することになっていますので，これらの情報が十分であるかをメール受信時に確認するなどの対策も有効です．

5.2　認証ドメイン名の評価

受信したメールが，DMARC などの送信ドメイン認証技術で認証された場合でも，そのメールが受け取るべき正しいメールであるとは限りません．フィッシングなどの迷惑メールの多くも DMARC などの送信ドメイン認証技術に対応してきていますが，認証されたドメイン名やメールの内容をメールフィルタ等で確認することで，受け取るべきかどうかを判断することができます．

---

4. メール受信者は認証結果だけを信頼するのではなく，認証されたドメイン名を確認しなければならない
5. メール受信側は，認証されたドメイン名の評価 (ドメインレピュテーション) を行い，受信者に届けるかを判断した方が良い

5.3 フィードバック

メール配送は，メール送信側から受信側へのネットワーク接続が開始となり，配送中の応答コードによって受け取られたかどうかを判断してきました．メール受信側での迷惑メール対策が進むにつれて，送信したメールがメール受信側でどのような処理をされたのか，メールが受信者に届いているのかがわかりにくくなってきています．送信ドメイン認証技術 DMARC では，メール受信側からメール送信側に対して認証結果等を含む DMARC レポート (aggregate, failure) を送信する機能があります．いずれのレポートも，レポート受信側にとって極端な負荷とならないように，送信時には DMARC の仕様に基づいて正しく送信する必要があります．

---

6. DMARC レポートを外部ドメイン名[*12]に送信する場合は，正しく委譲設定されているか確認しなければならない
7. DMARC の失敗レポート (failure report) を送信する場合は，当該メールに個人情報など重要な情報が含まれていないようにしなければならない
8. メール送信側として DMARC 集約レポートを利用している場合は，メール受信側として集約レポートを送信したほうが良い

特に DMARC の失敗レポートの送信に関しては，日本国内においては個別同意の取得が難しく，事前の包括同意によって実施する必要があるため，総務省による「DMARC 導入に関する法的な留意点」[8] に沿った形で行う必要があります．

DMARC の集約レポートは，送信ドメイン認証技術の設定が正しく行われているか，途中で再配送されるメールが適切に再署名等の処理を行っているかを確認することができる，重要な情報です．そのため，多くのメール受信者が集約レポートを送信すべきで，特に送信側として集約レポートを活用している場合，活用できるようなサービスを提供している場合は，積極的に集約レポートの送信を検討すべきです．

5.4 メール受信者にわかりやすい認証結果の提示

メール受信時の送信ドメイン認証技術による認証結果は，`Authentication-Results:` ヘッダに記録することになっています．しかしながら，通常このヘッダはメール受信者に提示されない場合が多く，参照するためには詳細表示など別途表示させる手順を必要とします．またメールの送信者情報である `From:` ヘッダについても，本来のメールアドレスではなく表示名 (`display-name`) を優先して表示するなど，DMARC を含む認証されたドメイン名が明確に提示されない場合があります．

---

9. メール受信システムでは，送信ドメイン認証技術による認証結果と認証したドメイン名をわかりやすく提示した方が良い
10. メール受信システムでは，送信側が BIMI[*13]に対応している場合で規格に沿っている場合，Brand Indicator を表示してメール受信者に送信者をわかりやすく提示した方が良い

[*12] 受信したメールの送信ドメイン名以外にレポートを送信する宛先のドメイン名．

[*13] Brand Indicators for Message Identification

BIMI は，現在仕様が検討されている新しい技術ですが，ブランド (Brand Indicators, ロゴなど) を表示させるためには，BIMI としての準備のほかに，DMARC としてもより厳しいポリシーの設定が必要になります．以下に BIMI に対応するための最低限の DMARC レコードの設定例を示します．

```
_dmarc.example.jp.  IN TXT  "v=DMARC1; p=quarantine; pct=100"
```

DMARC のポリシーは `quarantine` あるいは `reject` を設定する必要があります．`pct=` は設定したポリシーを適用する割合 (パーセント) を設定するものですが，ポリシーが `quarantine` である場合は，`pct=100` (100% の意味) である必要があります[*14]．なお，BIMI の仕様は現時点で Internet-Draft の段階であり，今後 RFC として発行された場合，上記の仕様を含め変更される可能性があることに留意が必要です．また BIMI 以外にも，送信ドメイン認証技術を利用してメール送信者をわかりやすく提示する独自の機能を提供するメールサービスもあります．

[*14] DMARC の次の RFC 改訂では，pct パラメータは廃止されることが検討されています．

付録 A　本ガイドラインにおける要求項目と要求レベル

掲載証と対象者	番号	要求項目	Must	Should	May
第 2 章 メール送信側	1	メールの送信ドメイン名に DMARC レコードを設定することで DMARC を導入する．導入に際しては SPF あるいは DKIM を送信側として導入しなければならない	○		
	2	メール送信側として DMARC を導入する場合，SPF と DKIM の両方を導入した方が良い		○	
	3	DMARC のポリシー設定は，`p=none` から始めて認証結果を確認することで `p=quarantine`，`p=reject` と強度を上げていく方が良い		○	
	4	DMARC のポリシー強度を上げるためには，DMARC レポートを受信し，認証結果を把握した上で判断していくことを勧める			○
	5	設定する SPF レコードの内容は，事前にチェックサイト等で確認することを勧める			○
	6	SPF レコードで他の管理ドメイン名を利用する場合は，利用元のドメイン名の状態を含め定期的に確認した方が良い		○	
	7	DKIM の署名対象には，必須ヘッダ（From:）以外にも送信者や受信者を示す情報，日付や `Subject:` などの推奨ヘッダを含めるとともに，署名対象の本文を示す情報 `l=`についても，再利用された場合でも区別できるよう十分な長さとしなければならない	○		
	8	組織ドメイン名には DMARC レコードを設定しなければならない	○		
	9	メールに利用しないサブドメイン名に対する DMARC ポリシーの設定として，組織ドメイン名以下の DMARC ポリシー (`p=` または `sp=`) は，`reject` と設定した方が良い		○	
	10	メールに利用するドメイン名には，個別に DMARC レコードを設定した方が良い		○	
	11	メールに利用しないドメイン名は, SPF 認証が必ず失敗する SPF レコードとポリシーが “reject” である DMARC レコードを設定し，Null MX の設定をした方が良い		○	

掲載証と対象者	番号	要求項目	Must	Should	May
第 2 章 メール送信側	12	DMARC レポートを受信し送信メールの DMARC などの認証状況を把握するために DMARC レポート，特にレポート数の多い集約レポート (aggregate report) を受信した方が良い		○	
	13	DMARC のポリシーは `reject` まで設定できることを目指し，そのために受信側の SPF, DKIM, DMARC の認証状況を把握した方が良い		○	
	14	DMARC レポートの受信および分析にはツールや分析サービスを利用して認証結果を把握することを勧める			○
	15	送信ドメイン名（管理ドメイン名）以外の宛先で DMARC レポートを受信する場合は，DMARC レポートの受信先で委譲されていることを示す設定をしなければならない	○		
第 3 章 メール配送事業者	1	メール配送事業者が送信するメールは，DMARC の認証ができるよう SPF, DKIM, DMARC の設定しなければならない	○		
	2	メール配信事業者は，依頼元のドメイン名の SPF レコードの設定のために，`include` 用の SPF レコードを作成し提供した方が良い		○	
	3	メール配信事業者は，依頼元に対して DKIM の公開鍵の情報を提供するか，CNAME 参照用の DKIM 鍵レコードとセレクタ名等の情報を提供した方が良い		○	
	4	メール配信の依頼元は，ヘッダ `From:` に自組織のドメイン名を設定する場合，配信事業者からの情報に基づき，SPF, DKIM, DMARC が正しく認証できるよう設定しなければならない	○		
第 4 章 メール再配送事業者	1	送信するメールが転送される場合は，DKIM 認証に対応しなければならない	○		
	2	転送先のメール受信側が SPF 認証できるメールを受け取る場合は，転送時に RFC5321.From を転送元ドメイン名に書き換える設定を勧める			○
	3	転送時に転送元ドメイン名を書き換えて転送する場合は，エラーメール (NDR, DSN) がループしないような処理をしなければならない	○		

掲載証と対象者	番号	要求項目	Must	Should	May
第 4 章 メール再配送事業者	4	メーリングリストからの再配送時には，RFC5321.From と RFC5322.From にはメーリングリストのドメイン名を設定しなければならない	○		
	5	メーリングリストからの再配送時には，メーリングリストのドメイン名による DKIM 署名を付加しなければならない (DKIM 再署名)	○		
	6	メーリングリストのドメイン名では，SPF レコードと DKIM 鍵レコード，DMARC レコードを公開し，それぞれに対応した設定をしなければならない	○		
	7	メーリングリストのメンバが ARC に対応している場合は，ARC を導入することを勧める			○
第 5 章 メール受信者	1	メール受信時に SPF, DKIM, DMARC 認証を行い，送信側の DMARC ポリシーに対応した受信処理を行わなければならない	○		
	2	SPF 認証ができたとしても，不正な SPF レコードを設定して pass した可能性もあるため，SPF レコードの内容についても確認することを勧める			○
	3	DKIM 認証ができたとしても，Replay Attack の可能性もあるため，署名対象の情報が十分であるか等確認することを勧める			○
	4	メール受信者は認証結果だけを信頼するのではなく，認証されたドメイン名を確認しなければならない	○		
	5	メール受信側は，認証されたドメイン名の評価 (ドメインレピュテーション) を行い，受信者に届けるかを判断した方が良い		○	
	6	DMARC レポートを外部ドメイン名に送信する場合は，正しく委譲設定されているか確認しなければならない	○		
	7	DMARC の失敗レポート (failure report) を送信する場合は，当該メールに個人情報など重要な情報が含まれていないようにしなければならない	○		

掲載証と対象者	番号	要求項目	Must	Should	May
第 5 章 メール受信者	8	メール送信側として DMARC 集約レポートを利用している場合は，メール受信側として集約レポートを送信したほうが良い		○	
	9	メール受信システムでは，送信ドメイン認証技術による認証結果と認証したドメイン名をわかりやすく提示した方が良い		○	
	10	メール受信側システムでは，送信側が BIMI に対応している場合で規格に沿っている場合，Brand Indicator を表示してメール受信者に送信者をわかりやすく提示した方が良い		○	

参考文献

[1] S.Kitterman, *Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1*, https://www.rfc-editor.org/rfc/rfc7208.txt, 2014.04.

[2] D.Crocker, Ed., et al, *DomainKeys Identified Mail (DKIM) Signatures*, https://www.rfc-editor.org/rfc/rfc7208.txt, 2011.09.

[3] M.Kucherawy, Ed., et al, *Domain-based Message Authentication, Reporting, and Conformance (DMARC)*, https://www.rfc-editor.org/rfc/rfc7489.txt, 2015.03.

[4] K. Andersen, et al, *The Authenticated Received Chain (ARC) Protocol*, https://www.rfc-editor.org/rfc/rfc8617.txt, 2018.07.

[5] S. Blank, et al, *Brand Indicators for Message Identification (BIMI)*, https://www.ietf.org/archive/id/draft-brand-indicators-for-message-identification-04.txt, 2023.09.

[6] M^{3}AAWG, *M^{3}AAWG Email Authentication Recommended Best Practices*, https://www.m3aawg.org/sites/default/files/m3aawg-email-authentication-recommended-best-practices-09-2020.pdf. 2020.09

[7] M^{3}AAWG, *M^{3}AAWG Protecting Parked Domains Best Common Practices Update 2022-06*, https://www.m3aawg.org/sites/default/files/m3aawg_parked_domains_bcp-2022-06.pdf. 2022.07

[8] 総務省 総合通信基盤局 電気通信事業部消費者行政第二課, *DMARC* **導入に関する法的な留意点**, https://www.soumu.go.jp/main_content/000495390.pdf.

[9] 迷惑メール対策推進協議会 技術ワーキンググループ, **送信ドメイン認証技術導入マニュアル 第** *3.1* **版**, https://www.dekyo.or.jp/soudan/aspc/report.html#dam.

送信ドメイン認証技術 DMARC 導入ガイドライン
2024 年 7 月発行 (一部修正 8 月)
編集 · 発行　迷惑メール対策推進協議会
(事務局)
一般財団法人 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 ホウライ巣鴨ビル 7 階
TEL: 03-5907-5371
MAIL: q-meiwaku-mail-kyogikai@dekyo.or.jp
URL: https://www.dekyo.or.jp/soudan/aspc/