参考資料４

【DMARC ガイドライン案】

電子メールのなりすまし対策、迷惑メール対策技術である DMARC 等（SPF、DKIM を含む）のメール認証技術 ガイドライン案

令和６年３月29日版

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 つの方式があります．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機能であるため，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（Domain Keys Identified 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な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．

目次

はじめに i
1　本ガイドラインについて 1
2　メール送信側 3
2.1　送信側の送信ドメイン認証設定 3
2.1.1　送信側の DMARC 設定 3
2.1.2　送信側の SPF 設定 4
2.1.3　送信側の DKIM 設定 4
2.2　DMARC の組織ドメイン名への設定 6
2.3　メールに利用しないドメイン名への設定 7
2.4　DMARC レポートの活用とポリシーの強化 8
3　メール配信事業者の送信ドメイン認証設定 10
3.1　認証ドメイン名の扱い 10
4　メール再配送時の設定 11
4.1　転送メールの設定 11
4.2　メーリングリストの設定 12
5　メール受信者 14
5.1　送信ドメイン認証 14
5.2　認証ドメイン名の評価 15
5.3　フィードバック 16
5.4　メール受信者にわかりやすい認証結果の提示 17
おわりに 19
謝辞 19
付録 A 20
SPF 設定例 20
DKIM 設定例 21
DMARC 設定例 22
付録 B 24
参考文献 28

1　本ガイドラインについて

これまで電子メールでは，メールの送信者を判断する手法として，送信者を示すメールアドレスではなく，送信元の IP アドレスをもとに判断する手法が長い間利用されてきました．例えば，迷惑メールの送信元や，一般のインターネット利用者に割り当てられる動的 IP アドレスの範囲をブロックリストとして収集し提供する仕組みです．こうした手法は，メールの送信者として示されたメールアドレスが，正しい情報であるかを確認する手段が無かったことに起因しています．これを送信者のメールアドレスをドメイン名単位で査証されていないかを確認できるようにする仕組みが，送信ドメイン認証技術です．

メールには，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認証機能を実現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技術の認証機能を導入したとしても，メールの送信側が送信ドメイン認証技術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，メールシステムの利用者としてはお互い受け取るべきメールかどうかを判断するためにも，メール送信側として，またメール受信側として送信ドメイン認証技術に対応するべきです．

送信ドメイン認証技術がメールシステムの中で広く普及すれば，フィッシングなど悪質ななりすましメールも簡単に判断できるようになります．さらに，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ができるようになります．この認証したドメイン名を評価して受け取りを判断する仕組みは，ドメインレピュテーションと呼ばれています．ドメインレピュテーションの利用が広がることで，独自ドメイン名を登録し送信ドメイン認証技術に対応したとしても，評価の低いドメイン名のメールを受け取らないといったことも可能になります．またメール送信側は，管理するドメイン名の評価を下げないように，迷惑メールが送信されていないか，メール送信時の認証情報が悪用されていないかを管理すべきです．

ドメイン名は，メールに限らずウェブサイトやインターネット上の様々なシステムでも利用されている基盤情報です．そのためドメイン名は，会社や団体など組織を識別する統一したブランドとしての役割も担うようになってきています．メールにおいては，そのブランドを模倣されないように，また正しい組織から送信されたメールであることを判断できるように，送信ドメイン認証技術を正しく設定することが必要です．こうした設定も，ドメイン名の評価（レピュテーション）を高める一つの手段です．

送信ドメイン認証技術は，既にメールの仕組みが出来上がった後に，なるべく影響が少ないよう拡張する形で実現している仕組みです．そのため，既にさまざまな形で利用が進んでいるメール配信の仕組みの中には，うまく適合できないような場合もあります．本ガイドラインは，既存のメール配信の仕組みの

中で送信ドメイン認証技術を有効に機能させるために，メールシステムに関わるそれぞれの役割に対して，実現すべき機能や設定を段階的に示したものです．

迷惑メールによる様々な被害がなかなか無くならない状況の中で，送信ドメイン認証などを利用してメールの受信判断を厳しくしていく動きも広がってきています．自組織のメールが受信側に今後も正しく安定的に届いてほしいと考えるのであれば，一過性のドメイン名を安易に利用するのではなく，関連技術を含めて送信ドメイン認証技術に正しく対応したドメイン名を利用することにより，自組織のブランドとしてのドメイン名を高めていくことが，今後より重要になっていくと考えられます．

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を行う，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 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．

2-1.	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 （Must）
2-2.	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 （Should）

2.1.1 送信側の DMARC 設定

DMARC レコードで設定しなければならない重要な情報に DMARC 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，DMARC ポリシーを none（p=none）から設定すべきです．DMARC ポリシーの強度をより上げていくことで（p=quarantine 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．DMARC ポリシーの強度を上げていくためには，DMARC レポートを受信したうえで，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．

2-3.	DMARC ポリシーの設定は，p=none から始め，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 （Should）
2-4.	DMARC ポリシーの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くことを勧める （May）

[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

2.1.2 送信側の SPF 設定

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エラー（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 を用いて自ドメイン名以外の他の管理元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．

2-5. 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（May）
2-6. SPF レコードで自ドメイン名以外の他の管理元ドメイン名を利用する場合は，自ドメイン名の状態を含め定期的に確認した方が良い（Should）

2.1.3 送信側の DKIM 設定

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より堅牢な認証方法と考えられています．

その一方で，一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．

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 節にも日本語で記載されています．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と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．

2-7. 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，署名対象とするメール本文の長さ（オクテット値）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 （Must）

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 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.

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.

2-8. 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 (Must)
2-9. メールに利用するドメイン名には, 個別に DMARC レコードを設定することを勧める (May)
2-10. メールに利用しない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=あるいは sp=)は, reject として設定することを勧める (May)

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に利用しない場合や，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に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，0 節で述べた 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”
```

図 1 メールに利用しないドメイン名への認証が必ず失敗する設定例

2-11. 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（Should）

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] こうしたドメイン名を Parked と呼びます
[3] A ”Null MX” No Service Resource for Domains That Accept No Mail（RFC7505）

2.4 DMARC レポートの活用とポリシーの強化

DMARC 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と確認できることで，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メールアドレスに送信されます．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，メールにて MIME[4]形式で添付ファイルと同様に送られています．集約レポートの内容は，機械的に処理可能な 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受信し，内容を人の目で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．

DMARC レポートを利用するために，外部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，委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．

2-12. 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 （Should）
2-13. DMARC 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 （Should）
2-14. 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 （May）
2-15. 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 （Must）

[4] Multipurpose Internet Mail Extensions.
[5] Estensible Markup Language.

3 メール配信事業者の送信ドメイン認証設定

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をメール配信事業者とします．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。

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，その性質から外部に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． 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方法の，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．

3-1.	メール配信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 を設定しなければならない （Must）
3-2.	メール配信事業者は、依頼元のドメイン名に対する 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 （Should）
3-3.	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 （Should）
3-4.	メール配信の依頼元は，ヘッダ From: に自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 （Must）

[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

ここでは，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アドレスへ自動的に送信されるメールを再配送（indirect mail flow）とします．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

ここでは，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転送メールとします．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 に設定する方法とがあります．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 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．

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．

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する必要があります．

4-1.	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 （May）
4-2.	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 （Must）
4-3.	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 あるいは DSN）がループしないような処理をしなければならない （Must）

[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

4.2 メーリングリストの設定

ここでは，登録されたメンバーから投稿（送信）されたメールを受信し，それをメンバー全員に再配送する仕組みをメーリングリストとします．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，メンバーへの再配送時には，エンベロープ From:（RFC5321.From）をメーリングリストの運用を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]を付加するほか，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。

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によって，より効果的な場合が多いと考えています．

4-4.	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 （Must）
4-5.	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） （Must）
4-6.	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にしなければならない （Must）
4-7.	メーリングリストのメンバーが ARC[11]に対応している場合は，ARC を導入することを勧める （May）

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

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するほか, 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, これらの情報が充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.

5-1.	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 （Must）
5-2.	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 （May）
5-3.	DKIM 認証ができたとしても, Replay Attack の可能性もあるため, 署名対象の情報が充分であるか等, 確認することを勧める （May）

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．

5-4.	メール受信者は認証結果だけを確認するのではなく，認証対象とされたドメイン名を確認しなければならない （Must）
5-5.	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，メール受信者に届けるかを判断した方が良い （Should）

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（集約レポート（aggregate report）と失敗レポート（failure report））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付加とならないように，送信時には DMARC の仕様[3]に基づいて正しく送信する必要があります．

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，率先して集約レポートを送信すべきです．

5-6.	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 （Must）
5-7.	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 （Must）
5-8.	メール送信側として DMARC 集約レポート（aggregate report）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方が良い （Should）

[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

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．

BIMI[13]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．以下図 2 に，BIMI に対応するために最低限必要な 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”

*1　v= バージョン番号．レコードの最初に DMARC1 とする
*2　p= 受信側に要求するポリシーを記載
　　quarantine　認証失敗時に不審メールとして扱うことを求める
　　reject　認証失敗時に受け取り拒否することを求める
*3　pct=　ポリシー適用割合
　　設定可能な値は 0～100 の数値（省略時は 100 と判断）
　　段階的な導入を促すためポリシーを適用すべきメールの割合を調整できる

*設定の詳細は，マニュアル[9]を参照（付録 A に SPF，DKIM，DMARC の設定例を抜粋）

図 2　BIMI に対応するために最低限必要な DMARC レコードの設定例

DMARC ポリシーは quarantine あるいは reject を設定する必要があります．また，pct=にはポリシーを適用する割合（パーセント）を設定します．ポリシーが quarantine である場合は，ポリシーをすべて適用しなければならないため，pct=100（100% 適用の意味）と設定する必要があります．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．

5-9.　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

[13] Brand Indicator for Message Identification

（Should）
5-10. メール受信システムでは，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 （Should）

おわりに

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」および令和 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である，フィッシング対策協議会/一般社団法人日本ネットワークインフォメーションセンター 木村泰司氏，JPAAWG/株式会社インターネットイニシアティブ 櫻庭秀次氏，JPAAWG/株式会社 TwoFive 末政延浩氏，LINE ヤフー株式会社 中村成陽氏，フィッシング対策協議会/トレンドマイクロ株式会社 野々下幸治氏，フィッシング対策協議会/一般社団法人 JPCERT コーディネーションセンター 平塚伸世氏の各氏による検討の結果，メンバーの合意を得たものです．

謝辞

本ガイドライン案執筆にあたりご協力いただいた，JPAAWG/株式会社 TwoFive 加瀬正樹氏へここに感謝の意を表します．

付録 A

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，原則として，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[9]を参照いただきますが，SPF，DKIM，DMARC の基本的な設定例についてのみ、以下のとおり、引用します．

SPF 設定例

---以下、送信ドメイン認証技術導入マニュアル[9]より引用---

1.3.2 送信側の設定

メールの送信側では，DNS 上で SPF レコードを後悔するだけで SPF の運用を開始できます．RFC4408 では，SPF レコードは DNS の TXT 資源レコード(RR: Resource Record)か SPF RR として公開することが定められていましたが，RFC7208 では，DNS の TXT RR のみを利用することに変更されています．

SPF レコードには，当該ドメイン名に属するメールアドレスを送信者として，そのドメイン名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，IP アドレス(IPv6 を含む)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以下に図 3 示します．

```
a.example.com.   IN TXT “v=spf1 -all”
b.example.com.   IN TXT “v=spf1 +ip4: 192.0.2.1 -all”
c.example.com.   IN TXT “v=spf1 +ip4: 198.51.100.1/28
~all”
```

図 3 SPF レコードの記述例

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)は，メールサーバ等の IP アドレスの記述が無いことから，全てのメールが SPF の認証が失敗(fail)します．このことから a.example.com は，メールを送信しない(送信者情報として利用しない)ドメイン名であり，詐称に利用されないための SPF レコードを設定していると考えられます．

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.esample.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，c.example.com をドメイン名として持つメールアドレス（例えば user@.example.com）からのメールは 198.51.100.1/28 のネットワークのホスト（例えば 192.51.100.4 など）からのみ送信されるという意味を持ちます.
記述方法の詳細は，1.3.3 で解説します.

DKIM 設定例

---以下、送信ドメイン認証技術導入マニュアル[9]より引用---

1.4.2 公開鍵の公開

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する公開鍵を公開します. 公開鍵は，署名ドメイン名に対する TXT 資源レコード（DKIM レコード）として DNS に登録します.

多くの受信側のメールサーバでは，鍵の長さが 1,024bit から 2,048bit までをサポートしています. 企画（RFC）では 2,048bit より長い鍵を利用する場合もあるとされています. なお，1,024bit より短い鍵は，オフラインでの解読行為に対して脆弱ですので，利用を避けてください.

公開鍵を登録するドメイン名は次の図 4 の通りです. _domainkey ラベルは，固定の文字列です.

<selector>._domainkey.<ドメイン名>

図 4 公開鍵を登録するドメイン

*セレクタ（<selector>）は，DKIM-Signature ヘッダの s タグに指定したラベル（サブドメイン名）です. あるドメイン名に対して，サブドメイン名（ラベル）を複数設定することで，セレクタを複数用いることができます. これにより，同じドメインに対して複数の鍵ペアを運用することが可能になります. こうした運用は，メールの用途の違い等で複数の鍵ペアを同時に利用することが可能となり，例えばそれぞれで鍵長や暗号方式を変えるといった運用もできます. また電子署名で利用する鍵ペア（公開鍵と秘密鍵）は，セキュリティの観点から定期的に鍵ペアの交換（ロールオーバー）をする必要があります. セレクタを利用することで，鍵ペアのロールオーバーをスムーズに実施できます. **<ドメイン名>** は，DKIM-Signature ヘッダの d タグに指定したドメイン名になります.*

DMARC 設定例

---以下、送信ドメイン認証技術導入マニュアル[9]より引用---

1.5.3 送信側の設定

メール送信側では, メール受信側で DMARC 認証ができるように, SPF や DKIM を導入します. 確実に DMARC として認証できるようにするためには, 両方を導入することが推奨されています. 送信側として, SPF あるいは DKIM が導入されていれば, 送信側で DMARC の導入に必要な作業は対象のドメイン名に対して DMARC レコードを設定することです. DMARC レコードは, DNS 上のテキスト(TXT)資源レコードに設定します. 設定するドメインは, _dmarc サブドメイン名です. 例えば, example.jp ドメイン名に DMARC レコードを登録する場合は、以下の図 5 のような設定となります.

```
_dmarc.example.jp. IN TXT “v=DMARC1; p=none;
 rua=mailto:report@example.jp”
```

図 5 DAMRC レコードの設定例

DMARC レコードの記述内容や設定できるパラメータについては, 1.5.4 で解説します.

DMARC では, メールに利用する RFC5322.From のドメイン名以外に, 組織ドメイン名に対して DMARC レコードを設定することができます. 組織ドメイン名については既に説明しましたが, そこに DMARC レコードを設定する利点は, その組織ドメイン名の配下のドメイン名全てに同じポリシーを適用できることです. もちろん, 特定のサブドメイン名に対して固有のポリシーを設定する場合にはそのサブドメイン名に対してのみ, DMARC レコードを設定することになります.

```
_dmarc.mail.example.jp. IN TXT “v=DMARC1; p=reject”
_dmarc.example.jp.      IN TXT “v=DMARC1; p=none”
```

図 6 組織ドメインと DMARC レコード

例えば図 6 の例では, RFC5322.From のドメイン名が, magazine.example.jp である場合, magazine.example.jp に対する DMARC レコードは設定されていないので、その組織ドメイン名である example.jp の DMARC ポリシーである(p=none)が適用されます. 一方で, mail.example.jp ドメイン名の DMARC レコードは宣言されていますので、その DMARC ポリシーp=reject が適用されます. 逆に組織ドメイン名にのみ特定の

DMARC ポリシーを設定し、サブドメイン名には適用させない, という方法もあります. これは, SPF および DKIM それぞれの認証手法毎に指定可能で, strict モードとして設定すれば, その組織ドメイン名に対してのみ認証結果が適用されます. 指定しない場合は, サブドメイン名に対しても適用する relaxed モードとして解釈されます。

付録 B

表 1 対象者ごとの要求項目と要求レベル

掲載章と対象者	No.	要求項目	Must	Should	May
2 （第 2 章 ドメイン管理者）	-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 ポリシーの設定は, p=none から始め, 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 ポリシーの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 レコードで自ドメイン名以外の他の管理元ドメイン名を利用する場合は, 自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:などの推察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	メールに利用するドメイン名には, 個別に DMARC レコードを設定することを勧める			○
	-10	メールに利用しない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 と設定することを勧める			○

	-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		○	
	-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	○		
3 (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 の設定を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に対する 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	○		
4 (第 4 章 メール再配送事業者)	-1	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			○
	-2	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	○		

	-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，NDR(エラーメール）がループしないような処理をしなければならない	○		
	-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			○
5 （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確認するのではなく，認証対象と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，メール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，正しく移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(aggregate report)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は，送信ドメイン認証技術による認証を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		○	

＊ 受信したメールの送信ドメイン以外にレポートを送信する宛先のドメイン名

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://datatracker.ietf.org/doc/html/rfc8617, 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] M3AAWG, M3AAWG Email Authentication Recommended Best Practices, https://www.m3aawg.org/sites/default/files/m3aawg-email-authentication-recommended-best-practices-09-2020.pdf. 2020.09

[7] M3AAWG, M3AAWG 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/data/anti_spam/meiwakumanual3/manual_3rd_edition.pdf