DMARC ポリシー変更のためのガイドブック V1.0

迷惑メール対策推進協議会技術ワーキンググループ

目次

1. 用語・略称の一覧

本書では、以下のとおり略称の統一を図る。

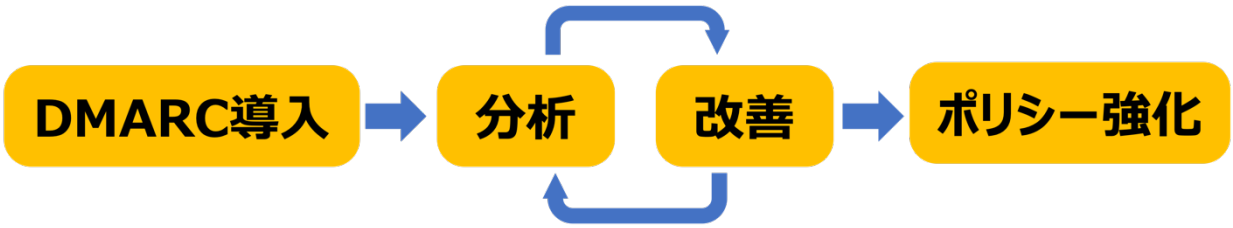
本書での表記	正式名称・意味など
DMARC	Domain-based Message Authentication, Reporting, and Conformance 送信ドメイン認証技術の一つ。SPFとDKIM両者を利用したメールのドメイン認証を補強する技術である。
DKIM	DomainKeys Identified Mail 送信ドメイン認証技術の一つ。送信元が付した電子署名により送信元情報の真偽及び電子メールの本文の改変を検知することができる。
SPF	Sender Policy Framework 送信ドメイン認証技術の一つ。エンベロープ情報の From メールアドレスのドメイン名をチェックし、当該 DNS に確認を行い送信元情報の真偽を確認する。
サブドメイン FQDN	Fully Qualified Domain Name TCP / IP ネットワーク上で、ドメイン名・サブドメイン名・ホスト名をすべて省略せずに指定した記述形式のことを指す。
組織ドメイン	Organizational Domain wwwなどのラベルを持たない登録ドメイン（ネイキッドドメイン）を指す。
集約レポート	Reporting URI(s) for aggregate data DMARC を含む送信ドメイン認証結果について、ある程度の期間分をまとめて受信メールサーバからドメイン管理者にフィードバックされる統計情報。
失敗レポート	Reporting URI(s) for failure data 送信されたメールが SPF または DKIM に一致せず、受信者側で DMARC 認証に失敗した場合に生成されて、受信メールサーバからドメイン管理者にフィードバックされるフォレンジック情報。
アライメント SPF アライメント DKIM アライメント	ヘッダーFromドメインを DMARC 認証が保護するために求めるドメインの一致性を指す。SPF アライメントの場合は、ヘッダーFrom ドメインとエンベロープ From ドメインが一致すれば成立。DKIM アライメントの場合は、ヘッダーFrom ドメインと署名ドメインが一致すれば成立。
DMARC レコード	DNS に所定の形式で設定した TXT レコードを指し、DMARC 認証に失敗した場合の取り扱い方法（ポリシー）を指定。オプションとして、集約レポートの受信先や失敗レポートの受信先が指定可能。
DMARC 導入 DMARC を導入する	DMARC レコードを DNS に設定することを指す。
DMARC 分析 DMARC を運用する	メールを送信する組織が、集約レポートや失敗レポートを収集して、当該ドメインのメール送信状況を把握し、また改善する活動を指す。

DMARC 認証 DMARC で検証する	メールを受信する組織またはメール受信サーバが、DMARC レコードを参照して、当該メールがなりすましかどうかを判定することを指す。
ポリシーに従った処理をする	メールを受信する組織またはメール受信サーバが、あらかじめ DMARC レコードで指示されたポリシーに従って、DMARC 認証に失敗したメールを隔離措置や拒否措置を講じることを指す。
強制力のあるポリシー	DMARC レコードに指定されたポリシーのうち、quarantine や reject を指す。

2. はじめに

インターネット上でのコミュニケーション手段の一つであるメールは、2000 年以降迷惑メールやなりすましメールといった攻撃に晒されており、それらの対抗手段として送信ドメイン認証が技術規格として成立した。メールを送信する組織（以下、送信側）にとって DMARC は、送信元 IP アドレスの真偽を元にした技術である SPF と、送信元が付与した電子署名の真正性を元にした技術である DKIM によって構成されたなりすましメール対策であり、グローバルなメール環境ではデファクトスタンダートである。加えて、グローバルに展開する大手メールサービス提供事業者では、DMARC をはじめとするなりすましメールを見分け、排除するための技術導入を送信側に強く求めており、多くの送信側の組織にとって DMARC は導入しなければならない対策の一つとなった。

一般的に送信側が DMARC に対応するとは、大きく分類して「導入」「運用」「ポリシー強化」というフェーズに分類できる。「導入」では、自組織のメールドメインを特定して、技術仕様に従った DMARC レコードを DNS に設定することである。「運用」では、メールを受信するシステム（以下、受信側）からフィードバックされる情報を元にして、課題を見つけて改善をすることである。「ポリシー強化」では、受信側からフィードバックされる情報を一定期間監視して、ポリシーと呼ばれる設定を「強制力のあるポリシー」に変更することである。これらによって、正規のメールが正しく受信され、なりすましと判定されたメールが隔離や拒否の措置が取られる状態になる。



一方、受信側が DMARC に対応するとは、システムが DMARC の認証処理を実施して、強制力のあるポリシーに従い、なりすましメールを隔離や拒否することである。これを実現し、その効果を最大化するためには、送信側のメールドメインの多くが DMARC に対応している状態が望ましいと言える。

日本国内では送信側の DMARC の普及が他国と比較して遅れている。その要因として送信側が DMARC を「導入」「運用」「ポリシー強化」するためのノウハウが不足している点、そして DMARC の適切な「運用」が難しいという点が挙げられる。さらに、メールをどのような目的・方法で利用・送信しているかは組織によって異なることも、DMARC の普及を妨げている要因と言える。

このガイドブックでは、さまざまな組織が送信側として DMARC を「導入」し、かつ適切に「運用」し、そして「ポリシー強化」するための一助となる情報を整理する。

3. ユースケースの分類

自組織がどのようにメールを送信するかという観点で整理すると、以下のような 4 つのユースケースに分類できる。

表 3 ユースケースの分類表とその例示

分類名	分類の定義	例示
コミュニケーション （B to B）	自組織や他組織とメッセージやデータファイルの送付のようなやりとりをするために自組織のドメイン名を名乗って、メールを送信または受信する場合。	企業や組織が従業員向けに提供するメールシステムなど。 図 6.1.1 参照。
メール通知 （B to C）	自組織が個人に対してサービスを提供し、その連絡手段として、自組織のドメイン名を名乗って、個人に対してメールを送信する場合。契約や何らかの通知、重要なお知らせ、一斉にメール送信するようなメールマガジンを含む。	契約やサービス開始の連絡、パスワードや設定変更の通知、広告メールなど。 図 6.2.1 参照。
メールサービス提供 （C to C）	自組織が個人に対して、自組織が管理するドメイン名でメールアドレスを貸与して、メール送受信サービスを提供する場合。	電気通信事業者のメール役務など。 図 6.3.1 参照。
第三者サービス提供 （代行・中継）	自組織が顧客（他組織または個人）に対してクラウドサービスを提供し、その一つの機能として、顧客のドメイン名を名乗って、メールを送信する場合。	メール送信事業者や基幹業務のアウトソーシングサービス、メーリングリストサービスなど。 図 6.4.1 参照。

DMARC を導入する組織は、それぞれのユースケースが該当するかどうかを見極めて、それぞれの特徴に合わせた DMARC の運用を心がける。

4. DMARC 導入のポイント

最初に DMARC を導入する際のポイントを 3 つ挙げる。これらのポイントは、いずれのユースケースにおいても共通である。

DMARC レコードのポリシー設定(p=)は、none を設定して、モニタリングから開始する

ポリシーについては、none はモニタリングを目的とした設定であり、自組織のメール送信状況を把握するまでは、強制力のあるポリシー（quarantine, reject）ではなく、none を設定することが推奨される。ただし、新たなドメイン名を取得した直後であり、これまでにメールを送信していないことが明らかな場合は、ポリシー設定を強制力のある reject にすることを検討するべきである。

可能な場合は、組織ドメイン名に DMARC レコードを設定する

一つの組織ドメイン名を複数の組織が利用する（マルチテナント）などの特段の理由がない限りは、組織ドメイン名に対して DMARC レコードを設定すべきである。マルチテナントの場合は，それぞれの組織でのポリシーやメールの運用方法などを考慮し，組織ドメイン名への DMARC レコードの設定を検討すべきである。

DMARC レコードの集約レポート専用メールアドレスを用意して、DMARC レコードには可能な限り集約レポート受信先(rua=)を設定する

集約レポートは通常は 1 日ごとに DMARC レコードに rua=で指定されたメールアドレスへフィードバックされる。実際に DMARC レコードを設定後に、集約レポートがフィードバックされるまでには数時間から 1 日程度かかる場合がある。

```
v=DMARC1; p=none; rua=mailto:dmarc-rua@example.jp;
```

図 4. DMARC レコード設定例（example.jp ドメイン名の場合）

5. 集約レポートの分析ポイント

DMARC を導入して、集約レポートが指定した受信先にフィードバックされ始めた後、以下のポイントを押さえて自組織のメール送信状況を分析して、DMARC 認証が成功するように改善する。そして、自組織のメール送信状況が十分改善された状態となったのち、強制力のあるポリシーに変更する。

> 集約レポートの分析は、一定期間（数ヶ月）実施して、可能な限り DMARC に対応したメール送信サーバを把握し、その網羅率を高める

基本的には、集約レポートの分析とそれに対応した対策を繰り返して、DMARC 認証が成功する状態に改善する（図 5.1）。この改善サイクルの頻度や期間は組織によって異なるが、定常的に送信されるメール以外に特定の時期にだけ送信するメール（IR に関する通知メール、採用活動に関するメール、安否確認メールなど）を網羅し、分析の見落としを減らすためには、十分な期間（少なくとも数ヶ月）を分析期間とすべきである。

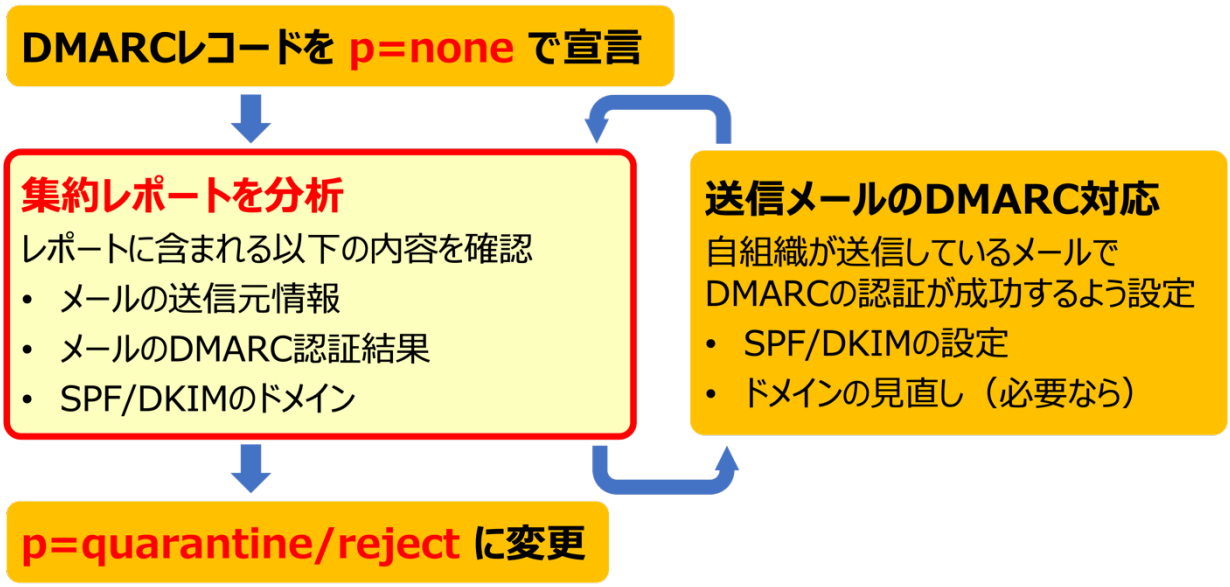


図 5.1 改善サイクルイメージ

> 組織ドメイン名とサブドメイン名を区別して分析し、サブドメインポリシー設定(sp=)を利用するかどうか検討する

組織ドメイン名の DMARC レコードに対しては、任意設定としてサブドメインポリシー設定(sp=)を none、quarantine または reject が指定できる。この設定は組織ドメイン名とは異なるポリシーを全てのサブドメイン名に明示的に設定するためのものである。

もし、組織ドメイン名のみでメール送信している場合は、すべてのサブドメイン名からのメール送信が許可されていないことを意味するため、組織ドメイン名の DMARC レコードに sp=reject を設定することができる（図 5.2）。この設定をすることで、攻撃者がランダムなサブドメイン名をなりすまして悪意のあるメールを送信するような攻撃（レベルスクワッティング攻撃）に効果が期待できる。

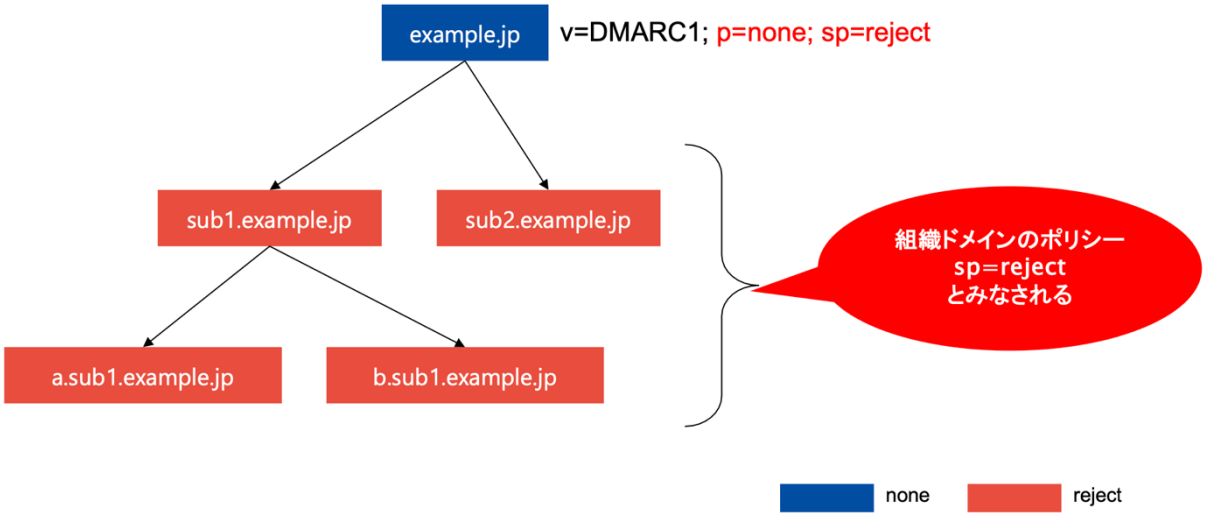


図 5.2 組織ドメイン名に p=none と sp=reject を指定した場合のポリシー適用状況

集約レポートの分析結果から、組織ドメイン名からのメール送信が十分管理されている状態である一方、サブドメイン名については分析が不十分である場合は、組織ドメイン名のポリシー設定を reject とし、サブドメインポリシー設定(sp=)を none にすることが可能である（図 5.3）。

この設定をすることで、まずは組織ドメイン名を保護すると同時に、全てのサブドメイン名に対しては影響を及ぼさないようなポリシーを運用できる。

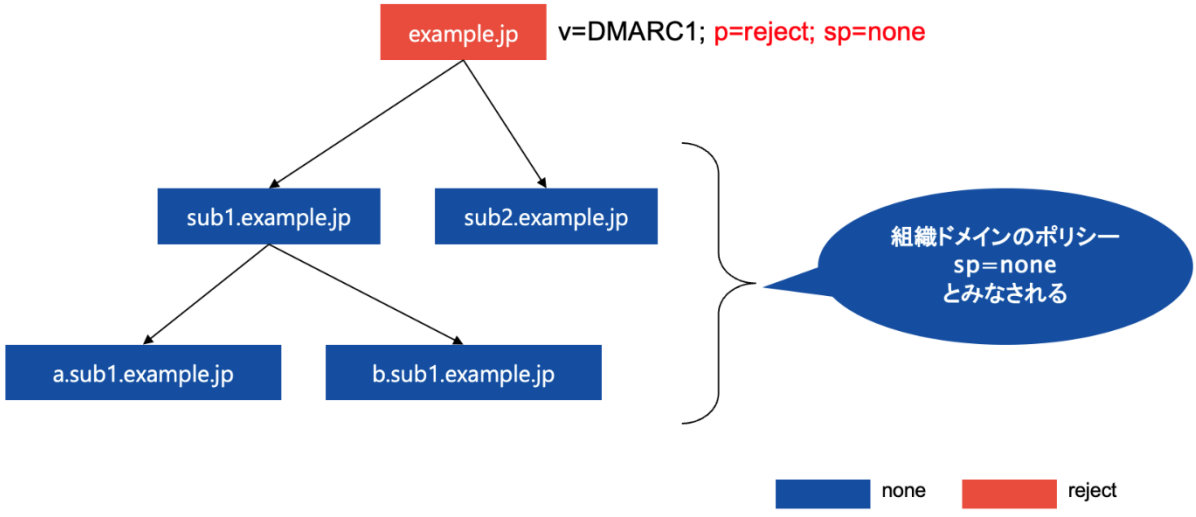


図 5.3 組織ドメイン名に p=reject と sp=none を指定した場合のポリシー適用状況

送信元サーバを分類して分析して、対策の優先順位を決定する

集約レポートは XML 形式で表現されており、そのフィールドの一つである”source_ip”は送信元サーバの IP アドレスを意味する。DMARC 認証が失敗と評価された”source_ip”について、その逆引きホスト名を確認し、それが自組織で管理するメールサーバである場合は、何らかの対策を講じる必要がある（表 5.4）。

表 5.4 送信元サーバが自組織の場合の対応方法

	DKIM 認証	SPF 認証	アライメント	分析・対応方法
1	失敗	失敗	—	(1) 集約レポートから送信元サーバを特定して、そのメール送信サーバで DKIM 署名対応する。 (2) 集約レポートからエンベロープ Fromドメインを特定して、その FQDN の SPF レコードに当該 IP アドレスを追記する。
2	—	成功	不成立	(1) 集約レポートからエンベロープ Fromドメインとヘッダー From ドメインを特定して、SPF アライメントを成立できるか確認する。 (2) SPF アライメントの成立ができないならば、集約レポートから送信元サーバを特定して、そのメール送信サーバで DKIM 署名対応する。 (3) SPF アライメントの成立ができるならば、エンベロープ Fromドメインを変更する。
3	成功	—	不成立	(1) 集約レポートから送信元サーバを特定して、そのメール送信サーバで DKIM 署名対応する。 (2) 集約レポートからエンベロープ Fromドメインを特定して、その FQDN の SPF レコードに当該 IP アドレスを追記する。

DMARC 認証失敗と評価された”source_ip”について、その逆引きホスト名が自組織ではなく、第三者サービス(もしくはクラウドサービス)である場合も、何らかの対策を講じる必要がある(表 5.5)。

表 5.5 送信元サーバが自組織ではない場合の対応方法

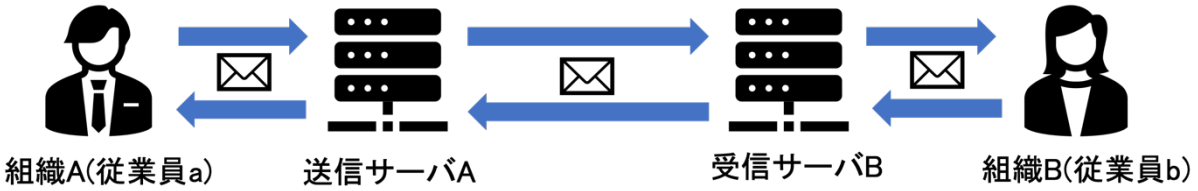
	自社での利用	利用部門が明確かどうか	分析・対応方法
1	**あり**	**明確**	(1) 集約レポートから「送信日」「送信元 IP」「エンベロープ From ドメイン」「ヘッダーFrom」などを集計して、利用部門へ確認する。 (2) 契約している第三者サービスのサポートへ問い合わせするなど、対応方法を検討する。
2	**あり**	不明	(1) 外部サービスやクラウドサービスの利用管理をしている部門に確認する。 (2) 利用部門が把握できた場合は、集約レポートから「送信日」「送信元 IP」「エンベロープ Fromドメイン」「ヘッダーFrom」などを集計して、利用部門へ確認する。
3	不明	—	対応の優先度を下げる、もしくは外部のコンサルティングに相談する。

なお、商用の分析ツールによっては、送信元サーバを分類する機能があり、それらの追加情報をもとにして、対策を講じるかどうかやその優先順位を決定しやすくなる。例えば、分析ツールでの分類が「メール転送サーバ」と評価されている場合は、自組織で直接対策を講じることができないため、優先順位を下げることもできる。

6. ユースケースごとの対策ポイント

6.1.「コミュニケーション（B to B）」の場合

自組織が「コミュニケーション」のユースケースに該当する場合は、基本的には送信者とメッセージの差出人が一致するため、エンベロープ From ドメインとヘッダーFrom ドメインが一致（SPF アライメントが成立）する。また、メール送信サーバや DNS 権威サーバを自組織で管理することができるため、自組織で DKIM レコードの設定や署名処理を実装することができる（DKIM アライメントが成立）。したがって、このユースケースに当てはまる場合は、SPF アライメント・DKIM アライメントの両方が成立するように進めるとよい。



メール送信サーバの管理	自組織もしくは自組織が契約したサービス事業者が管理。
DNS 権威サーバの管理	自組織もしくは自組織が契約したサービス事業者が管理。
SPF アライメント	基本的には成立する。 自社で管理するメール送信サーバを SPF レコードとして設定する。
DKIM アライメント	基本的には成立する。 なお、自組織が DKIM レコードを公開し、メール送信サーバで DKIM 署名を実装する必要がある。

図 6.1.1「コミュニケーション」のユースケースについて

以下に、「コミュニケーション」のユースケースで注意する、あるいは推奨するポイントを挙げる。

> メール本文の書き換えが発生した場合は、書き換え後に DKIM 署名する

外部へメール送信する際にウイルス検疫や添付ファイルの監査・分離をするソリューションがあるが、その処理中にメール本文の書き換えをする場合がある。その際に、DKIM 署名対応をする場合はこのソリューションが提供する DKIM 署名機能（メール本文の書き換え後に DKIM 署名する機能）を利用することが望ましい。

> メール転送する場合は、メール本文を書き換えない

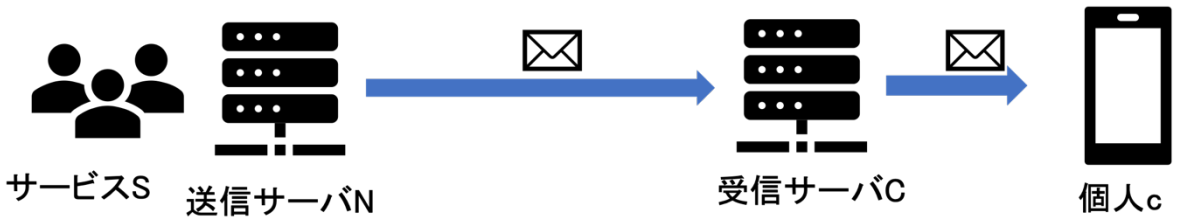
他組織からのメールを受信し、そのメールを外部へ自動転送する場合は、SPF 認証が失敗する。そのため、メール転送先で DKIM アライメントが成立するように、メール本文の書き換えは実施しないことが望ましい。なお、メールに DKIM 署名がない場合は、メール転送先で DMARC 認証が失敗するため、メール転送先には届かない可能性を念頭に入れておくべきである。

DMARC ポリシー処理をする場合は、集約レポートの機能を有効化する

受信側での対応になるが、集約レポートには認証失敗の情報や DMARC ポリシー処理の結果が記載されており、他組織の DMARC 導入および運用に大いに寄与できる。さらに、自組織の集約レポートとしても活用できる。自組織が利用している受信メールサーバやセキュリティゲートウェイに集約レポートの機能がある場合は、有効にすべきである。

6.2.「メール通知(B to C)」の場合

自組織が「メール通知」のユースケースに該当する場合は、多数の利用者へ一斉送信するため、一部の利用者には不達となること(エラーメールが返送されること)を考慮しなければならない。その場合は、メッセージの差出人とエンベロープ From ドメインが必ずしも一致しない場合が考えられる。その際は、SPF アライメントの成立ではなく、DKIM アライメントの成立によって DMARC が成功するような措置が必要である。また、メール送信サーバや DNS 権威サーバを自組織で管理することができるため、自組織で DKIM レコードの設定や署名処理を実装することができる。したがって、このユースケースに当てはまる場合は、DKIM アライメントを優先して成立するように進めるとよい。



メール送信サーバの管理	自組織もしくは自組織が契約したサービス事業者が管理。
DNS 権威サーバの管理	自組織もしくは自組織が契約したサービス事業者が管理。
SPF アライメント	成立しない場合がある。
DKIM アライメント	基本的には成立する。 なお、自組織が DKIM レコードを公開し、メール送信サーバで DKIM 署名を実装する必要がある。

図 6.2.1「メール通知」のユースケースについて

以下に、「メール通知」のユースケースで注意する、あるいは推奨するポイントを挙げる。

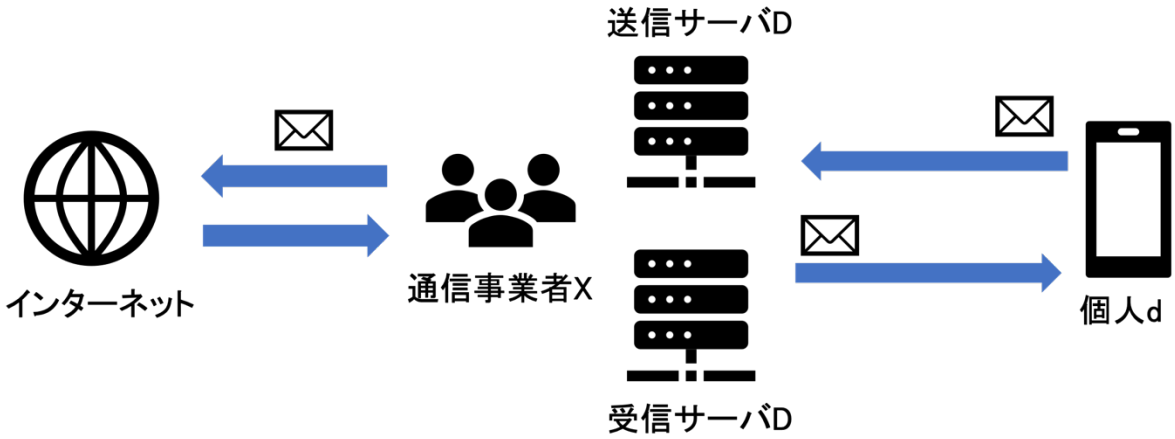
すべての送信メールに対して DKIM 署名対応する

通知情報は、個人利用者がメール転送することを想定して、すべてのメールに対して DKIM 署名することが望ましい。

6.3.「メールサービス提供(C to C)」の場合

自組織が「メールサービス提供」のユースケースに該当する場合は、基本的には送信者とメッセージの差出人が一致するため、エンベロープ From ドメインとヘッダーFrom ドメインが一致(SPF アライメントが成立)する。しかし、これらのドメイン名が不一致であること(ヘッダーFrom ドメインが提供メールサービスとは別ドメイン名であること)を認めるメールサービスであるならば、SPF アライメントは成立しない。また、メール送信サーバや DNS 権威サーバを自組織で管理することができるため、自組織で DKIM レコードの設定や署名処理を実装することができる。したがって、このユースケースに当てはまる場合は、SPF アライメント・DKIM アライメントの両方が成立するように進めるとよい。

ただし、メールサービス提供を他社に委託している場合もあるため、その場合はメール送信サーバの管理は委託先のサービス事業者となる。



メール送信サーバの管理	自組織もしくは自組織が委託したサービス事業者が管理。
DNS 権威サーバの管理	自組織が管理。
SPF アライメント	基本的には成立する。 自社で管理するメール送信サーバを SPF レコードとして設定する。
DKIM アライメント	基本的には成立する。 ただし、利用者がヘッダーFrom ドメインを自由に設定できる場合は、成立しない。

図 6.3.1「メールサービス提供」のユースケースについて

以下に、「メールサービス提供」のユースケースで注意する、あるいは推奨するポイントを挙げる。

可能な限り利用者のヘッダーFrom の変更は禁止する

利用者がメール送信する際に、提供するメールサービスとは異なるメールアドレスやドメイン名をヘッダーFrom ドメインに指定すると、SPF アライメント、DKIM アライメントいずれも成立しない。さらに、他組織のメールアドレスやドメイン名を指定することでなりすましメールの送信を許可することにもなり得る。可能な限りメールサービス仕様として禁止することが望ましい。

ヘッダーFromドメインが適切なメールには DKIM 署名対応する

利用者の送信先がメールを転送することを想定して、ヘッダーFrom ドメインが提供するメールサービスと一致する場合には DKIM 署名対応すべきである。

DMARC 認証失敗したメールは、利用者の設定の有無に関わらずメール転送しない

提供するメールサービスが受信した時点で DMARC 認証に失敗したメールは、たとえ外部へ転送したとしても同様に DMARC 認証に失敗してしまう。加えて、DMARC ポリシー設定が強制力のあるポリシーの場合は、転送したとしても隔離措置や拒否措置が取られることが推測できるため、このような場合メールは転送すべきではない。

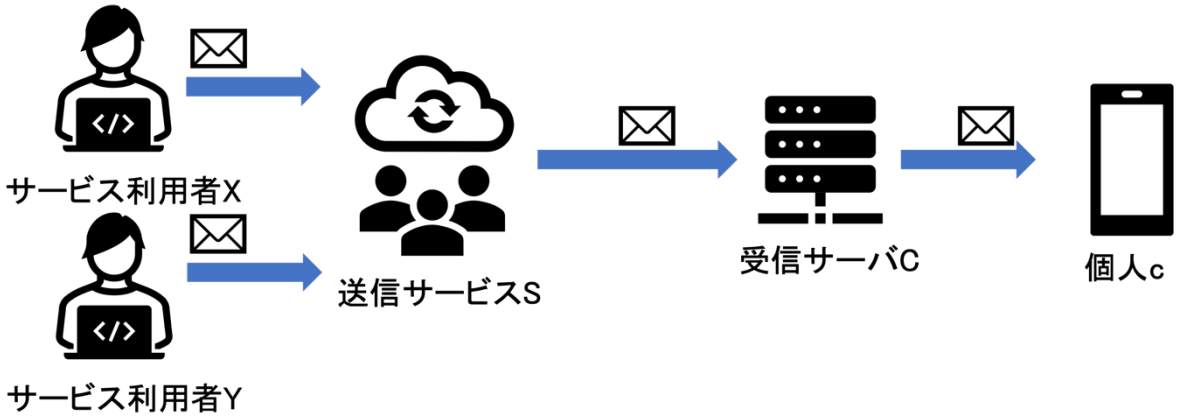
DMARC ポリシー処理をする場合は、集約レポートの機能を有効化する

受信側での対応になるが、集約レポートには認証失敗の情報や DMARC ポリシー処理の結果が記載されており、他組織の DMARC 導入および運用に大いに寄与できる。さらに、自組織の集約レポートとしても活用できる。自組織が利用している受信メールサーバやセキュリティゲートウェイに集約レポートの機能がある場合は、有効にすべきである。

6.4.「第三者サービス提供（代行・中継）」の場合

自組織が「第三者サービス提供」のユースケースに該当する場合は、基本的にはメッセージの差出人（ヘッダーFromドメイン）はサービス利用側組織のドメイン名であり、SPF アライメントを成立させるためには、エンベロープ From ドメインもサービス利用側組織のドメイン名を

設定する必要がある。また、DKIM アライメントを成立させるためには、DKIM 署名ドメインをサービス利用側組織のドメイン名とする必要があり、その DKIM レコードの設定はサービス利用側組織の DNS 権威サーバへの設定となる。このユースケースに当てはまる場合は、DKIM アライメントを優先して成立するように進めるとよい。



メール送信サーバの管理	自組織が管理。
DNS 権威サーバの管理	サービス利用側組織が管理。
SPF アライメント	基本的には成立しない。
DKIM アライメント	基本的には成立する。 ただし、自組織が DKIM 鍵ペアを生成し、メール送信サーバで DKIM 署名を実装する必要があり、一方でサービス利用側組織が DKIM レコードを公開する必要がある。

図 6.4.1「第三者サービス提供」のユースケースについて

以下に、「第三者サービス提供」のユースケースで注意する、あるいは推奨するポイントを挙げる。

すべてのメールに対して DKIM 署名対応する

第三者サービス提供の場合は、DNS 権威サーバの委任などをしなければ、基本的には SPF アライメントは成立しない。すべてのメールに対して DKIM 署名することが望ましい。

DKIM 署名対応が困難な場合にかぎり、ヘッダーFrom ドメインを第三者サービス側に書き換える一時的な措置を講じる

利用側組織のドメイン名で DKIM 署名する機能がない場合は、救済措置として第三者サービス側ドメイン名にヘッダーFrom ドメインを書き換えるような措置を取る場合がある。この措置によって、DMARC でアライメントを成立するためのドメイン名が、利用者側ではなく第三者

サービス側に切り替わり、DMARC 対応がしやすくなると言える。ただし、可能な限りヘッダーFromドメインを利用者側のドメイン名に変更できる機能を提供すべきである。

> メーリングリストサービスの場合は、「DKIM 署名の維持」「差出人の書き換え」「ARC 対応」のいずれかの回避方法を提供する

従来のメーリングリストサービスは、仕組み上 DMARC 認証に失敗しやすいため、以下の3つの回避方法が知られている。

一つ目の回避方法は「DKIM 署名の維持」である。メーリングリストに投稿されたメールは、メーリングリストに到達した時点では DKIM アライメントも成立する。また、DKIM-Signature に利用されるヘッダー（Subject など）や本文を書き換えるが、それを実施しなければ、メンバーへの配信においても、DKIM 認証が成功し、ヘッダーFrom ドメインも投稿者のドメイン名であるため、DKIM アライメントも引き続き成立する。そのため、メーリングリストからの配信もDMARC 認証が成功する（図 6.4.2）。

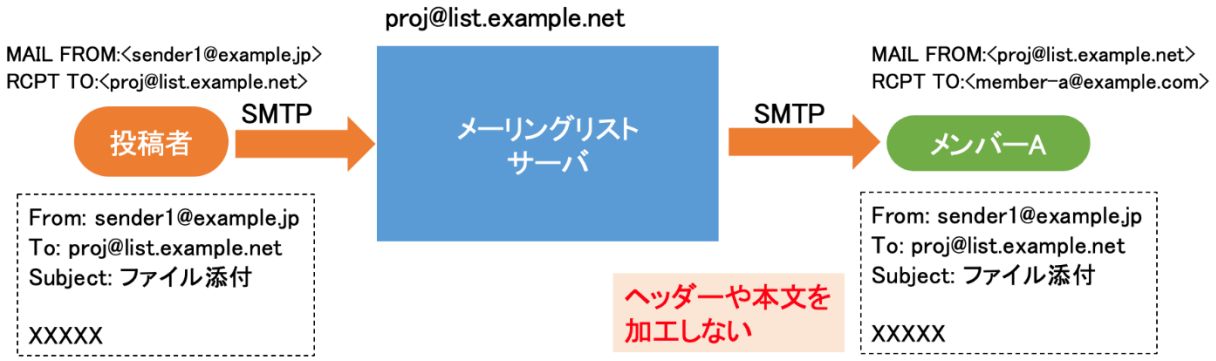


図 6.4.2 メーリングリストにおける「DKIM 署名の維持」

二つ目の回避方法は「差出人の書き換え」である。メーリングリストからメンバーへ配信する際に、DKIM 再署名は可能である。メーリングリストは、DKIM 再署名の前にヘッダーFromドメインをメーリングリストのドメイン名に書き換えることで、DKIM 再署名した後もヘッダーFromドメインと署名ドメインが一致し（DKIM アライメントが成立し）、DMARC 認証が成功する（図 6.4.3）。

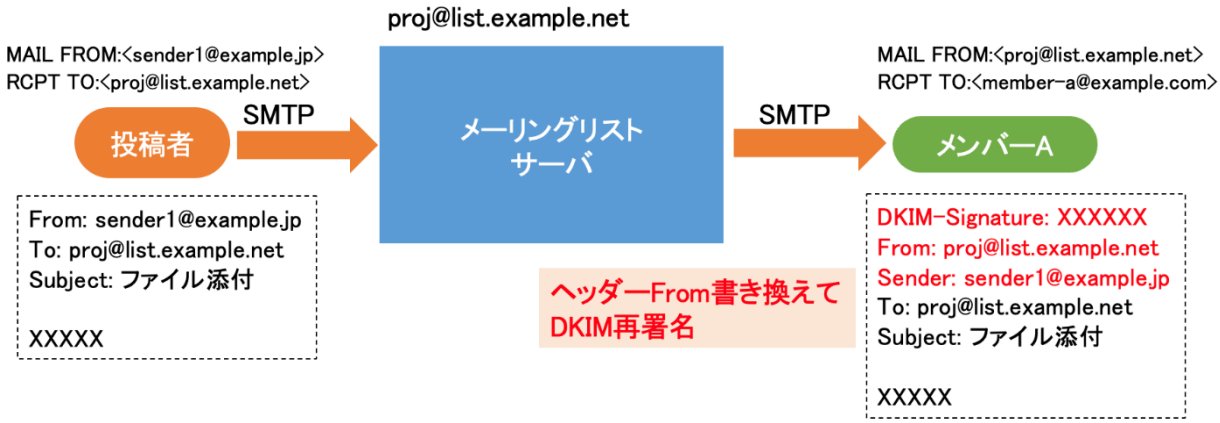


図 6.4.3 メーリングリストにおける「差出人の書き換え」

三つ目の回避方法は「ARC 対応」である。ARC（Authenticated Received Chain）は、DKIM と同様の電子署名の技術を利用し、メールが再配送された場合でも認証結果を示す Authentication-Results ヘッダーを辿れるようにすることで、認証の連鎖を帰納的に確認できるようにする技術である。投稿者からのメールは、直接送信されることが想定されるため、メーリングリストに到達した時点では DKIM 認証が成功し、かつ DKIM アライメントも成立する。ARC により、その認証結果（Authentication-Results ヘッダー情報）が連鎖的にメンバーへの配信でも維持された場合、メンバー側に到達した時点では DMARC 認証が失敗していたとしても、実際には成功扱いにすることが可能である（図 6.4.4）。ただし、全てのメンバーの受信側で ARC 対応している必要があるため、ARC 対応することで必ずメールが届くとは限らないことに留意する必要がある。

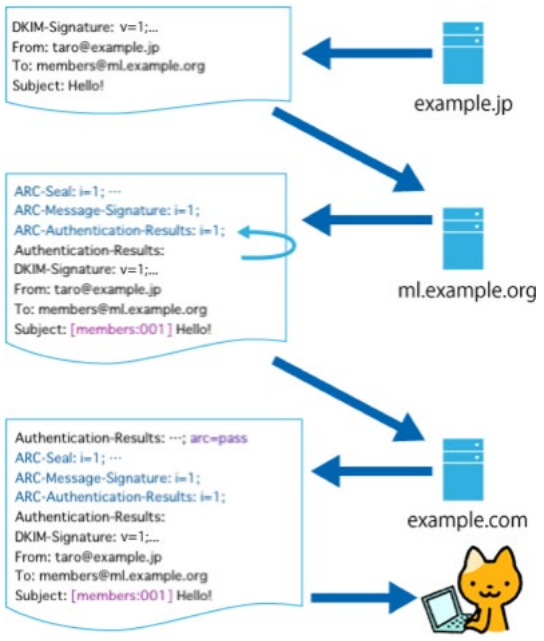


図 6.4.3 メーリングリストにおける「ARC 対応」

7. 強制力のあるポリシーへの切り替え

DMARC を導入して、集約レポートを分析し、必要な対策を講じてメール送信状況が十分改善された状態となったのち、強制力のあるポリシーに変更する。その際に以下のポイントについて留意する。

あらかじめ強制力のあるポリシーへの変更の指標と基準を定める

集約レポートで検出した DMARC 認証失敗に対して、すべて解決できるわけではなく一定量のメールが改善されない状態となりうる。これは、自組織で解決できない他組織が管理するメーリングリストや DMARC 認証に対応できていない第三者サービスの利用などがあるためである。強制力のあるポリシーへの変更判断には、あらかじめ指標と基準を定めて、関係者で合意するべきである。

以下に、指標と基準の例を挙げる。なお、例示した定量的・具体的な条件については組織によって異なる。

- ✓ 組織が定める期間（例：数ヶ月～半年）で計画した改善策が実行された
- ✓ 改善策の実行後、一定期間の DMARC 認証成功率が一定割合（例: 90%）を超えた
- ✓ 改善策の実行後、SPF レコードに指定された送信元 IP アドレスからの送信において DMARC 認証成功率が一定割合（例: 95%）を超えた
- ✓ 正規メールの DMARC 認証失敗についての課題が全て解消された
- ✓ 正規メールの DMARC 認証失敗についての未解決な課題が適切にリスクとして管理された

強制力のあるポリシーへの変更後に想定されるリスクを理解し、万が一の場合の切り戻し方法・切り戻し判断の指標や基準を定める

仮に十分改善された場合であったとしても、優先順位が低いメール送信サーバへの影響や分析期間中に集約レポートに記載されなかったメール送信サーバへの影響、未知のサブドメイン名への影響もありうる。事前に、これらの情報を整理しておき、業務への影響が発生した場合の手順をまとめておく必要がある。切り戻しが必要と判断するためには、その指標や基準をあらかじめ用意しておくべきである。

以下に、切り戻し判断の指標や基準の例を挙げる。なお、例示した定量的・具体的な条件については組織によって異なる。

- ✓ ポリシー強化後試験で予期しない結果が発生した場合（例: 主要メールサービスで DMARC 認証が失敗する）
- ✓ 一定量のメール送信において DMARC 認証が失敗して受信側に届かない場合
- ✓ 重要と定めるメール送信において DMARC 認証が失敗して受信側に届かない場合
- ✓ メールが届かないと判断された後、メールを再送しても解決しない場合

8. 想定問答集

Q：DMARC レコードにおいて、ポリシー設定を p=none にした場合にメール送受信に影響を及ぼすか

（A）いいえ。 DMARC レコードのポリシー設定として none を選択した場合は、受信側が DMARC 認証に失敗した場合も取り扱いに変化はない。ただし、受信側が DMARC 認証以外の条件で迷惑メール判定をする場合もあることを留意する必要がある。

Q：サブドメイン名の DMARC レコードにおいて、サブドメインポリシー(sp=)は有効か

（A）いいえ。 サブドメインポリシー(sp=)は組織ドメイン名のみに有効である。

Q：DMARC レコードにおいて、それぞれのパラメーターの間に半角空白は認められるか

（A）はい。 半角空白は認められるが、mailto:とメールアドレスの間に半角空白がある場合は、一部の集約レポートが届かなくなる場合がある。

Q：DMARC レコードにおいて、集約レポート受信先(rua=)を設定しなくても問題ないか

（A）はい。 DMARCレコードに含めなければならない設定はバージョン(v=)とポリシー(p=)の 2 つです。ただし、強制力のあるポリシーに変更するためには、集約レポートの分析が重要であるため、集約レポート受信先(rua=)は設定を推奨する。

Q：DMARC レコードにおいて、失敗レポート受信先(ruf=)を設定しなくても問題ないか

（A）はい。 DMARCレコードに含めなければならない設定はバージョン(v=)とポリシー(p=)の 2 つです。

Q ： DMARC レコードにおいて、集約レポート受信先(rua=)や失敗レポート受信先(ruf=)を複数指定できるか

（A）はい。 カンマ区切りで指定が可能です。その場合は、すべての受信先メールアドレスの先頭に mailto:を付与する必要がある。

Q ： 集約レポートのメール通数合計が、実際のメール送信通数の合計よりも少ない（多い）のはなぜか

（A） 集約レポートは、DMARC 認証に対応し、かつ集約レポートのフィードバックに対応したメール受信サーバのみから届く。そのため、集約レポートの合計メール通数が実際のメール送信通数よりも少ないことがある。

一方、なりすましメールの流通が増えた場合は、自組織で把握している送信メール通数だけでなく、なりすましメールに関する集約レポートが届く。そのため、集約レポートの合計メール通数が実際のメール送信通数よりも多いことがある。

Q ： DMARC レコードにおいて、集約レポート受信先(rua=)を指定したにもかかわらず、集約レポートが届かないのはなぜか

（A） 可能性は三つある。第一に、集約レポート受信先のメールアドレスのドメイン名が DMARC レコードのドメイン名と異なる際に必要な委任設定がされていない場合が考えられる。第二に、集約レポート受信先の先頭に mailto:が付与されていない場合が考えられる。第三に、すべてのメール送信先（宛先ドメイン名）が DMARC 認証や DMARC 集約レポートのフィードバックに対応していない場合が考えられる。

Q ： DMARC レコードにおいて、失敗レポート受信先(ruf=)を指定したにもかかわらず、失敗レポートが届かないのはなぜか

（A） 2025 年時点では、失敗レポートに対応したメール受信サーバやメールサービスは極端に少ないため、失敗レポートが届かない場合がある。

以上

DMARC ポリシー変更のためのガイドブック v1.0

2026 年 1 月発行

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/