RFC 6377
DKIM and Mailing Lists
概要

- **RFC 6377**

  DKIM and Mailing Lists

- **概要**

  Mailing List Managers (MLM) を含む構成で、DKIM を使用するための
  ガイダンスを提供する。

• 推奨リファレンス

読者は[DKIM] (RFC 6376) と [ADSP] (RFC5617)に精通することを奨励する。
リファレンスには、[DKIM-OVERVIEW] と [DKIM-DEPLOYMENT] の
コアの仕様書と同様に、DKIMの主要チュートリアルドキュメントがある。

• イントロダクション

– この文章で議論される項目

1. メーリングリストに送られたメールに DKIM を適用するためにどのような状況が署名者とその署名者が属する組織にとって望ましいか？

2. MLM に DKIM を検証し活用させることに関するトレードオフは何か？

3. メッセージ再送信型 MLM に既存の DKIM 署名を削除させることに関するトレードオフは何か？

4. MLM に自身の DKIM 署名を加えさせることに関するトレードオフは何か？

• イントロダクション

– カテゴリ

一般的に、 MLM の DKIM に関して 2 つのカテゴリがある :
参加 (participating)、及び、参加しない (non-participating) こと。

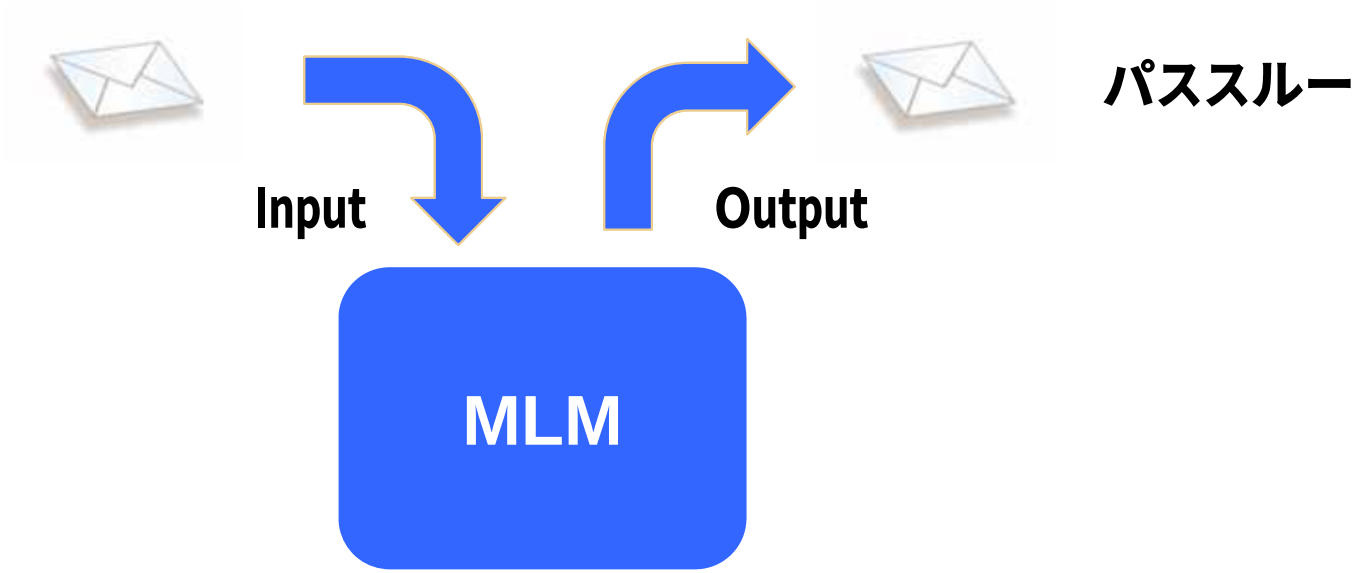
DKIM 署名されたメッセージに関しては、それぞれ固有の問題がある。
それらのタイプに関しては、個別のセクションで議論される。

一般的な MLM に対処するためのベストリコメンデーションは、MLM ドメイン上の
MLM あるいは MTA が転送する各メッセージに MLM 自身の DKIM 署名を適用し、
受信者がそれらの検証をする際に MLM のドメインの署名を考慮するということである。
(第5章 参照、特に 5.2)

MLM 4つのモードの要約 (3.2)

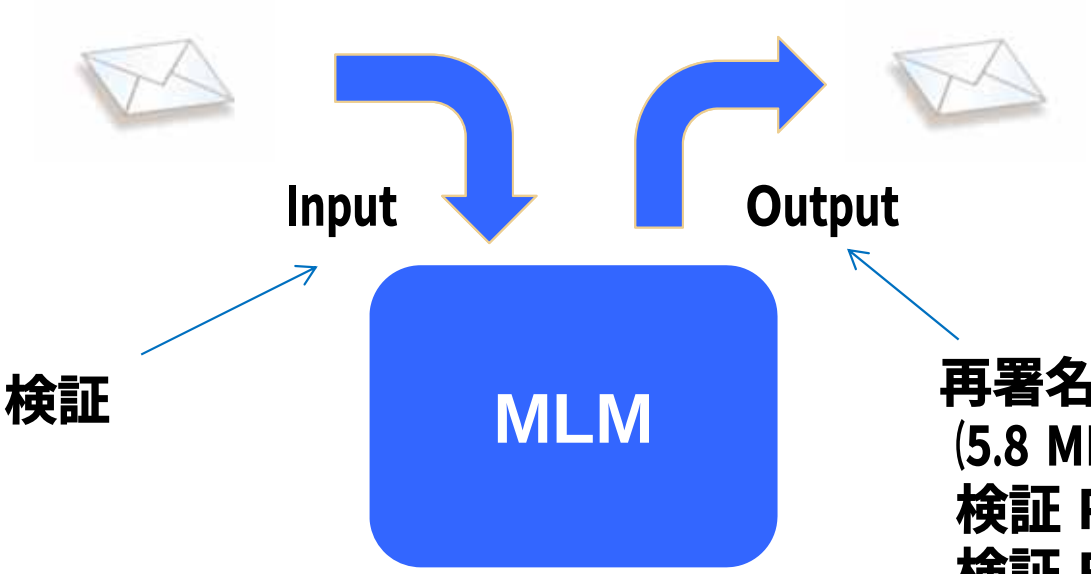
モード	DKIM 適用性	検証	削除	再署名
aliasing (エイリアシング)	○ (pass-through)	不要 (pass-through)	不要 (pass-through)	不要 (pass-through)
resending (再送信)	推奨：再署名	要検証	元の署名を残して削除を推奨 (5.7)	検証が PASS であれば、署名して再送信。FAILであれば、配送しない (5.8)
authoring (オーサリング)	推奨：再署名	要検証	元の署名を残して削除を推奨 (5.7)	検証が PASS であれば、署名して再送信。FAILであれば、配送しない (5.8)
digesting (ダイジェスティング)	推奨：再署名	検証が必要か否かの言及無し	不要	

- aliasing MLM



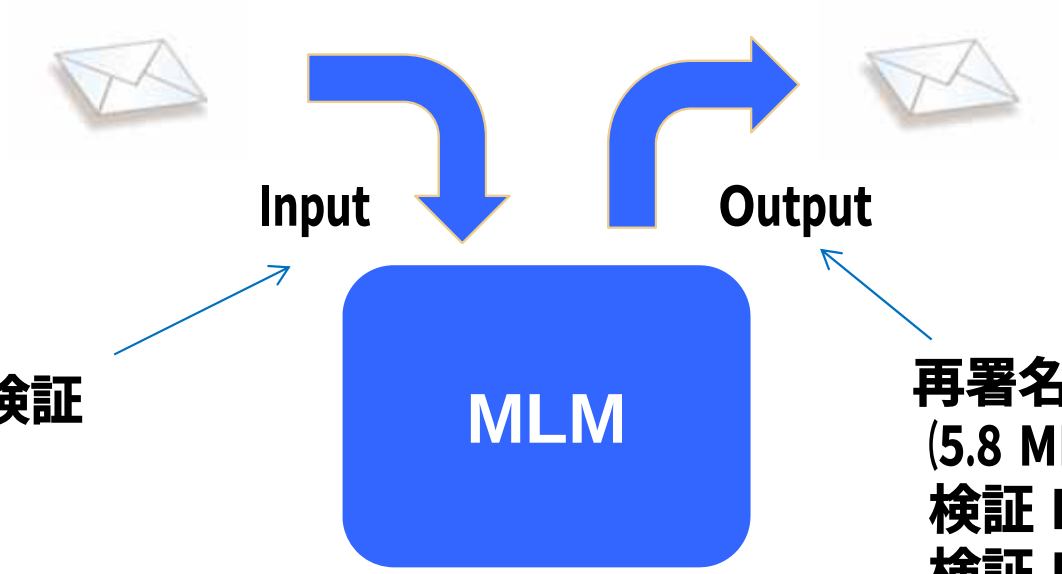
再送信をする際にメッセージそのものに改変をしない
オリジナルメールの DKIM 署名が残るので問題ない。

- resending（再送信） MLM



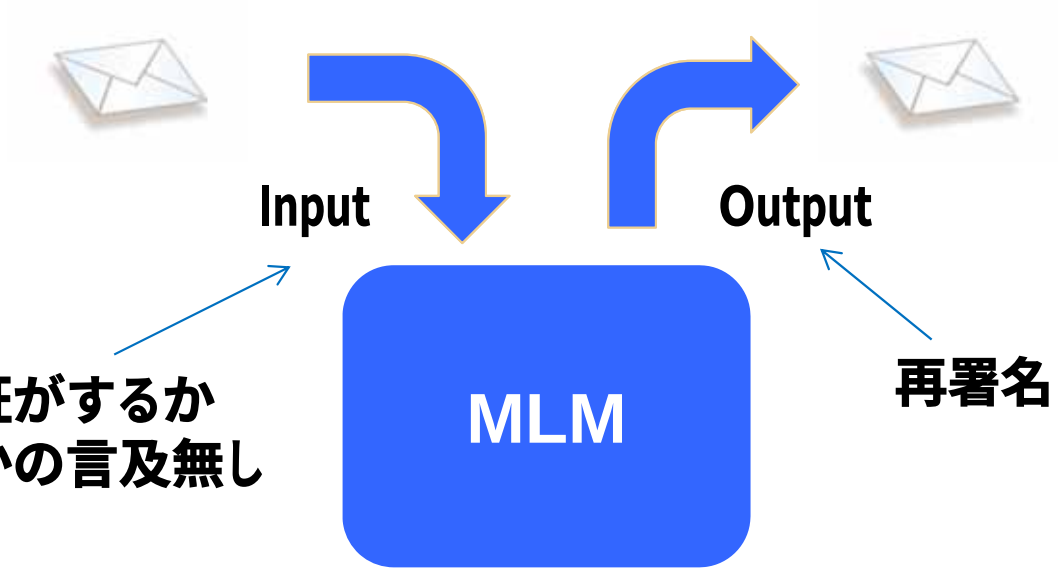
本文/ヘッダを少ししか改変しないもの
改変が ML 独自の新しいヘッダを付けるだけなら1.と同じである。
Subject タグや Reply-To を追加して再署名せずそのまま配送すると、
送信者の ADMD の DKIM-ADSP が「discardable」の場合、配送先で検証して
5xx を返すと MLM はその配送先をリストから削除してしまう。

- authoring MLM



メール本文の形態を大幅に改変するもの
受け取った元メッセージを改変するのではなく、
コンテンツを作成して、メッセージを送信する一つの形態である。
サンプル例としては、ニュースレターやマーケティング・メール等がある。
添付ファイルを取っ払ったりするものを想定している。
例えば、本文改変を != で逃げるのはMIMEなメッセージに対しては
リスクとなるので推奨できない。 再署名が前提である。

- digesting MLM



MIME マルチパートを使ったサマリ配送
これは明らかに新しいメッセージである。
しかし、それは DKIM 署名されたオリジナルメッセージのシーケンスを
含んでいるかもしれない。

以降参考情報

3.2 4つの MLM モード①

- MLM は4種類に分類される

1. aliasing（エイリアシング)

   aliasing MLM は、再送信をする際にメッセージそのものに改変をしないものである。どんな修正でも SMTP envelope recipient list（RCPTコマンド）に対する改変のみに限定される。MAIL のわずかな ヘッダ･フィールドの付加以外、メッセージヘッダーあるいはメール本文に対する変更が全くない。

ー オリジナルメールの DKIM 署名が残るので問題ない。

3.2 4つのMLM モード②

2. resending (再送信)：本文/ヘッダを少ししか改変しないもの

再送信する MLM（第5.2, 5.3章を参照）は、メッセージに対する改変を
行うものである。 このような MLM のアウトプットは新しいメッセージであると
考えられる。 このようなメッセージはリスト購読者の間での討論を促進するための
リスト固有のヘッダ・フィールド等のように再フォーマットされる。

- 改変が ML 独自の新しいヘッダを付けるだけなら1.と同じである。
  Subject タグや Reply-To を追加して再署名せずそのまま配送すると、
  送信者の ADMD の DKIM-ADSP が「discardable」の場合、配送先で検証して
  5xx を返すと MLM はその配送先をリストから削除してしまう。
  再署名するなら第三者署名になるので ATPS で対応する必要がある。

3.2 4つのMLM モード③

3. authoring（オーサリング）: メール本文の形態を大幅に改変するもの

authoring MLM は受け取った元メッセージを改変するのではなく、
コンテンツを作成して、メッセージを送信する一つの形態である。
従って、MLM がメッセージを生成するので、それは「mediator」ではない。
サンプル例としては、ニュースレターやマーケティング・メール等がある。

- 添付ファイルを取っ払ったりするものを想定している。
  例えば、本文改変を l = で逃げるのはMIMEなメッセージに対してはリスクとなるので
  推奨できない。再署名が前提である。

3.2 4つのMLM モード④

4. digesting（ダイジェスティング）: MIME マルチパートを使ったサマリ配送

再送信型 MLM の特殊なケースは、直近の MLM サブミッションの集合を含むシングルメッセージを送るものである。
それは MIME タイプ「マルチパート/ダイジェスト」のメッセージかもしれない。
これは明らかに新しいメッセージである。しかし、それは DKIM 署名されたオリジナルメッセージのシーケンスを含んでいるかもしれない。

3.3 署名に対するMLMの影響 ①

- 3.2 で記載されたように aliasing MLM は既存の署名に影響を与えない、
  そして authoring MLM は毎回新しいコンテンツを作っているため、既存の署名がない。
  しかしながら、再送信型 MLM が一般的に行う変更は、RFC5322.Subject
  ヘッダーフィールド、いくつかのリストに特定されたヘッダ・フィールド、
  あるいはメッセージ本体の改変等に影響を与える。
  DKIM 検証に対するこれらの影響について、以降で議論する。

3.3 署名に対するMLMの影響 ②

- Subject タグ：MLM の人気が高い機能は、フィールドのコンテンツに「タグ」と呼ばれる
  メーリングリストの「[サンプル]」のような、メーリングリストの名前を付加すること
  によって、RFC5322.Subject フィールドに「タグを付ける」ことである。
  メーリングリストに特定された接頭辞あるいは接尾辞を加えることによって、
  新しい投稿でRFC5322.Subject フィールドを変更することは、
  もしそのヘッダーフィールドが、その署名を作る時にハッシュが含まれていたなら、
  作成者の署名を無効にするであろう。
  DKIM の 5.5 章 が RFC5322.Subject に、それがユーザーの目に見える重要な
  文字列を含んでいる時、そのような変更をするメーリングリストで問題があることが
  予想される。

3.3 署名に対するMLMの影響 ③

- List-specific ヘッダーフィールド：いくつかのメーリングリストで [LIST-ID] と
  [LIST-URLS] あるいは [MAIL] で定義された「Resent - 」フィールド等の
  特殊なヘッダ・フィールドをメーリングリストの管理機能として加えることがある。
  又、一般的な MUA がオリジナルのメッセージのこのようなフィールドを含むこともある。
  そして DKIM が一般的なヘッダーフィールドの付加には柔軟に対応できる。
  ([DKIM] の 3.5章「h ＝」タグを参照)
  そのために、これは懸念としては見受けられない。

3.3 署名に対するMLMの影響 ④

- 他のヘッダ・フィールド： いくつかのメーリングリストは、リストが識別されるように、メッセージがメーリングリストという環境で送られている（「Sender」）ことを確定するために「Reply-To」を 又は、「Sender」のようなヘッダ・フィールドを加えるか、あるいは置き換えるであろう、そしてどのようなユーザーからの返信でもリスト（「Reply-To」）に行くようにする。 もし、これらのフィールドがオリジナルのメッセージに含められたなら、それらの1つ以上が署名のハッシュに含まれていたかもしれないため、署名が壊れる可能性が予想される。

3.3 署名に対するMLMの影響 ⑤

- マイナーボディチェンジ：いくつかのメーリングリストは加入者に定期購読契約の更新等で、メーリングリストポリシー管理用の URLを通知する為にメッセージに少数の文字列を加えることがある。 それらはメッセージ本文に対する改変がDKIM 検証者側で計算されてボディハッシュ値を変更するであろう。
  これらはメッセージ本文のそれらの部分をカバーするどのような既存の署名でも立証できないようにするであろう。
  付加された文字列が署名の検証を妨げないように、[DKIM] はそのメッセージ本文のハッシュによってカバーされたメッセージ本体の長さを制限する能力を含んでいる。
  しかし、これはセキュリティの意味合いを持っている。

3.3 署名に対するMLMの影響 ⑥

- メジャーボディチェンジ：再配信のために [MIME]パート、オリジナルのメール本文の中にHTMLメッセージを挿入、 ヘッダーを加える、削除、再整理、再フォーマット、HTMLメッセージ内のフッターを加える等の加工を行う場合、
  メール本文に本質的な変更を加えるいくつかの MLM がある。
  それらの変更の大部分あるいは全てが DKIM 署名を無効にするであろう。

3.3 署名に対するMLMの影響 ⑦

- MIME パート削除：いくつかの MLM は大きな MIME パートをサブミッションから
  取り除き、そしてメッセージを分割された形式のサイズに縮小し、
  不適切に自動化されたマルウェア配信を防ぐためにそれらをURLに取り替えるであろう。
  メッセージボディの制限が DKIM 署名の生成に適用されるいくつかのケースを除いて、
  署名は壊されるであろう。

4. Non-Participating MLM

- このセクションでは、DKIMに配慮していないメーリングリストについて議論する。
  そのようなMLMには DKIM ヘッダも Authentication-Results ヘッダも何の意味ももたない。

4.1. 作成者関連署名

- Discardable 等の制限の強い ADSP レコードを公開するドメインは、
  一対一のメールとそれ以外の MLM に投稿するようなメールのメール経路を
  分けるべきである。
  Discardable 等の制限の強い ADSPは一対一のメールに対して有効なもので、
  MLM に投稿するようなメールにはその制限を当てはめるべきではない。

4.2. 受信側での認証結果

- MLM に参加するようなユーザが存在するドメインでは、そのようなユーザのメールのやり取りには、DKIMに関する強い制限を適用しないようにするべきである。

4.3.受信側での処理方法

- メーリングリストの受信者は送信者のポリシーを尊重し、
  署名がない、または照合できないメールの受信拒否するべきである。

4.4. Wrapping a Non-Participating MLM

- Non-Participating MLM にDKIM サポートを加えるための1つのアプローチは、MLM をラップすることである。もしくは、本質的にいくつかのDKIMサービスを提供するものを他の DKIM を考慮する (MTAのような) コンポーネントの間に置くことである。例えば、Non-Participating MLM を定義する ADMD は、MLM を代表して第5章の機能およびリコメンドのうちのいくつかを施行して、リスト加入者からのメッセージ上のDKIM 検証をすることができる。また、MLM アウトプットを受け取る MTA か MSA は、MLM ドメインのための DKIM 署名を加えることができる。

5．Participating MLMs

- このセクションでは、DKIM に配慮したMLMを通過する DKIM署名メールに関連した問題についての議論を含む。

5.1. General

- LIST-ID, LIST-URLS や MAIL などで指定されているようなヘッダを
  単に追加する場合は、一般的に、DKIM を利用している電子メールインフラストラクチャ
  に対して最もフレンドリーである。しかし、メールにヘッダーやフッターを加えるような
  処理をやめることは期待できない。

5.2. DKIM ADSP

- 再送信型の MLM では、参加者からの投稿メールを受信するとき、
  その参加者のドメインの ADSP レコードをチェックして、discardable のようなポリシーを
  公開している場合、その時点でメールを受信拒否すべきである。
  上記のような動作が MLM で適用されず、該当のメールが MLM の参加者に
  配布された場合、受信者は、そのメールを廃棄するか、5xx エラーで受信拒否
  するべきである。

5.3. サブスクリプション

- 再送信型のMLMでは、新規参加者が参加するとき、そのADSPレコードをチェックするべきである。上記のチェックの結果、新規参加者が、"discardable"などの制限の強いポリシーを公開している場合、参加を許可しないようにするか、
そのポリシーによってメールが届かない場合があることを警告するべきである。

5.5. 作成者関連署名

- 転送されたり、MLMに投稿されたりすることのない 一対一のメールやビジネスのトランザクションメールは別のメールストリームで DKIM 署名されるべきである。

5.6. MLMでの認証結果

- 再送信型 MLM は投稿時に署名の認証に失敗したメールの処理を
  モデレータに任せるか、その場で受信拒否してもよい。
  投稿時に署名の認証を実施した場合、その認証結果をヘッダに追加すべきである。

5.7. 署名削除問題

- MLMが投稿された DKIM 署名付きメールの内容を大きく変更する場合、
  既存の DKIM 署名を削除することを推奨する。
  受信者は、自分が持っている信頼しているサイトのリストにのっているサイトの
  authserv-id が記録されており、かつ、同じく信頼しているサイトのリストにのっている
  サイトにより署名された DKIM 署名のヘッダハッシュに含まれている
  Authentication-Results ヘッダを参考するべきである。

5.8. MLM の署名

- DKIM対応した再送信型 MLM と作成型 MLM は、メールを (メンバに) 配布する時に
  署名をつけるべきである。署名する MLMは、元のメッセージが署名されていない場合、
  自身のローカルな設定やポリシーにしたがって、(メンバへの) 配布をしない
  こともできる。そのようなメールに署名はせずに、再配送することもできる。
  しかしながら、選択的な署名 (署名したりしなかったり) は奨められない。
  DKIM 対応した再送信型MLMは再配布のための処理が終わった後、
  そのメール全体に対して署名するべきである。

5.9. 最終的な受信サイトでの認証結果

- 一般的に、照合者や受信者は、MLMからの署名されたメールも
  他の署名されたメールと同様に扱うべきである。

5.10. FBLの利用

- オペレータは、正当な署名をつけたレポートをそれぞれのドメインに送るべきである。
  そのような方法でFBLを利用することは、メーリングリストの加入者に明らかにして
  おくべきである。例えば、MLM の ADMD が、問題となるメールの明らかな
  送信者であるユーザをリストの加入解除することにより、FBLアイテムを処理する場合、
  そうした対応を行うことをあらかじめ加入者に知らせておくことで、
  後のトラブル発生を回避するのに役立つであろう。

5.11. 受信者の処理

- 受信者は、自身が信用できる ADMD によって署名されておらず、
  また、全く署名されていない、外部により付与された Authentication-Results ヘッダは
  無視するか、削除するべきである。

  SMTP 通信中の DKIM と ADSP の認証において、エージェントは
  その SMTP セッション中にメールを受信拒否することもできる。

6. DKIM レポート

- MLM は DKIM 失敗レポートメカニズムを、DKIMインフラストラクチャの問題を
  署名作成者にフィードバックするための方法として適用すべきである。
  これは特に、加入者からのリスト設定コマンドや投稿を認証するための方法として
  DKIM認証を実施しているような MLM において特に重要である。

7 .セキュティ 考察事項

7.1. DKIM と ADSP からのセキュリティ考察事項

読者は、[DKIM]、[ADSP]および[AUTH-RESULTS]の中の「セキュリティ考察」
に記載されている資料に精通しているべきである。

7.2. リレー時の Authentication Results ヘッダー

第5章は、MLMインプットとしてメッセージの認証ステータスを受け取られることを
示すために Authentication Results ヘッダー・フィールドの追加をサポートするであろう。
[AUTH-RESULTS] の第7.2 章では、受信者は、一般にMLMのADMDへの演繹的な
合意や十分な理由のないそのようなデータを信頼するべきではない。
そのような合意は、MLM の ADMD によって加えられた DKIM 署名によって
それらのヘッダー・フィールドがカバーされるという要求を含めるように強く助言する。