JEAG
Japan Email Anti-Abuse Group

JEAG Recommendation
～送信ドメイン認証について～

送信ドメイン認証サブワーキンググループ
(Sender Authentication SWG)

JEAG
Japan Email Anti-Abuse Group

目　次

1.　はじめに 2

2.　本提案書の位置付け 2

3.　技術解説 3

3．1．IP アドレス方式 3
3．2．電子署名方式 3

4.　JEAG Recommendation 4

4．1．送信側の設定 4
4．1．1.　SPF Classic の利用 4
4．1．2.　DKIM の利用 5
4．2．受信側の認証 5
4．3．運用方針 6
4．3．1.　メーリングリスト 6
4．3．2.　メールマガジン 7
4．3．3.　第三者サーバ利用 7
4．3．4.　メール転送 8

5.　導入スケジュール 8

参考文献 9

1. はじめに

インターネットのメールサービスは、その利便性から新たなコミュニケーション基盤として急速に普及してきた。迷惑メールの増大は、単に受け手にとっての煩わしさを増やしただけではなく、メールの利便性を損なわせ、コミュニケーションツールとしてのメールの存在自体をゆるがす脅威となってきている。特にフィッシングに代表される詐欺的行為は、もはや迷惑のレベルを超えた犯罪である。

迷惑メール対策が難しい理由のひとつとして、送信元を特定するのが困難であることがあげられる。もし仮に送信元が明確であれば、迷惑メール送信者が利用しているプロバイダに連絡したり、公的な機関へ通報したりすることによって、迷惑メールの送信を停止できる。

しかしながら、現実的には、現在のメール配送の仕組みでは、送信元情報を容易に詐称できる。そのため迷惑メール送信者の多くは、送信元情報を詐称し、送信元の特定が難しくなるよう工夫している。

「送信ドメイン認証技術」は、メールの送信元情報のうち、ドメイン名が送信元に対して正当であるかを確認するための認証技術である。Japan Email Anti-Abuse Group（以下、JEAG）では、送信ドメイン認証サブワーキンググループ（以下、SWG）を設け、これらの技術について検討してきた。その成果として、実用可能な技術が明確になり、今後は送信ドメイン認証技術の普及に取り組む必要があると考えている。本 Recommendation は、送信ドメイン認証技術の導入を促進するため、技術を解説し、また導入時のノウハウや期待される効果などをまとめる。

なお、送信ドメイン認証はあくまでも認証技術であって、その結果だけでは迷惑メールであるか判定はできない。しかしながら、送信元ドメインの詐称判定や、送信元の特定が可能になる。そこで、受信ブロックやフィルタリング技術、レピュテーション技術などを組み合わせることで、迷惑メールを効果的に減少させられると期待できる。また、フィッシングへの抑止効果もあると考えられる。

送信ドメイン認証技術の普及は、迷惑メール対策の大きな一歩である。メールサーバ管理者が理解を深め、プロバイダやホスティング事業者のみならず、広く企業や教育機関などにおける早期対応を切望する。

2. 本提案書の位置付け

本 Recommendation は、これまで送信ドメイン認証 SWG で検討した内容をまとめる。ここで述べる内容は、サブワーキンググループ参加メンバはもちろん、全てのメールサーバ管理者が実施するべき施策を提言している。

送信ドメイン認証は、単一の技術規格の呼称ではなく、それぞれ特徴を持った複数の技術の総称である。認証結果ひとつをとっても、単に認証の成否だけではなくその中間的な状態が定義されており、解釈の仕方によってその取り扱いに違いが発生する恐れがある。そのため、送信ドメイン認証技術を導入しようとしても、どの技術を使うべきなのか、どういった運用をするべきなのか疑問に思うことが多いと思われる。送信ドメイン認証の効果を得るためには、メール送信側と受信側それぞれが同じ技術を用いることが前提となる。また、メール受信側における認証結果の取り扱いを明確にすることにより、メール送信側も安心して設定できるようになる。

本 Recommendation は、送信ドメイン認証技術を普及させるため、これらの問題を解決する運用指針となることも目的としている。本文中では、実施しなければならない内容（提言）については「するべき」、その逆は「するべきではない」と表現する。また、導入の難易度が高い場合や、現

段階では今後の検討課題と思われる内容については、参考情報として「方法がある」と表現する。
送信ドメイン認証技術の普及に伴い、その効果が高まる反面、これまで予想し得なかった問題が表面化する可能性がある。また、いくつかの技術については、未だ仕様策定の段階にある。そのため、本 Recommendation は定期的に見直しを行い、運用実績や経験、標準化動向などにより適宜更新していく予定である。

3. 技術解説

メール配送に使われる SMTP (Simple Mail Transfer Protocol) (参考文献 [7]) やメールヘッダで指定する送信元情報 (参考文献 [8]) は、容易に偽ることが可能である。これが迷惑メールの増大とともに、送信元の特定困難さや、エラーメールが詐称された側に戻ってしまう問題などの原因となっている。
送信ドメイン認証技術は、メールの送信元情報を詐称できなくするため、メールが正しいサーバから送信されていることを認証するための技術である。認証方法の違いによって複数の技術が提案されているが、IP アドレス方式と、電子署名方式の二種類に分類される。いずれも送信元のドメインを特定するための技術で、迷惑メール送信者かどうかを判定するための技術ではない。

3.1. IP アドレス方式

IP アドレス方式は、送信元情報として示されるドメインが DNS で宣言した送信元サーバ情報に、接続元の IP アドレスが含まれているかを認証する方式である。有力視されている方式として、米 Pobox.com の共同創業者である Meng Wong 氏が作成した「Sender Policy Framework」(以下、「SPF」)、と「SPF」を作成した Meng Wong 氏と「Caller ID for E-mail」を提唱する米 Microsoft Corporation 間で統合が合意されたことによって提案された「Sender ID」がある。「Sender ID」は IETF (The Internet Engineering Task Force) で標準化される予定だったが、いくつかの事情により作業部会は解散となった。その後「SPF」(参考文献 [4]) と「Sender ID」(参考文献 [5]) はそれぞれが実験的 RFC (experimental RFC) を目指す ID (Internet-Draft) として再提出され、現在審議中となっている。以後、区別のために実験的 RFC を目指す ID に規定された「SPF」を「SPF Classic」と表記する。「SPF Classic」と「Sender ID」は、それぞれ送信元情報の取り出し方に違いはあるが、送信元ホスト情報は、いずれも DNS 上の SPF レコードによって示される。
SPF Classic は、送信元情報としてメール配送上の情報を使う。具体的には、SMTP の MAIL コマンドで示される、送信元のメールアドレス (エンベロープ From) または HELO/EHLO コマンドに続くサーバ情報である。
Sender ID では、メールヘッダから送信元情報を取り出す。この取り出された送信元情報は、PRA (Purported Responsible Address) (参考文献 [6]) と呼ばれ、ヘッダが示すいくつかの送信元情報の中から、特定の手順によって決められる。Sender ID は、SPF Classic の仕様を取り込んだ背景から、SPF Classic と同様にメール配送上の送信元情報を利用することもできる。どちらを使うかは、送信側の SPF レコードで指定することができる。
IP アドレス方式では、受信時の接続元 IP アドレスを認証に利用するため、送信元からの接続を直接受けとれない場合には認証結果は「詐称」となる。

3.2. 電子署名方式

電子署名方式として有力視されている技術に「DomainKeys Identified Mail」(以下、「DKIM」) (参考文献 [2]) があげられる。DKIM は、米 Yahoo! Inc. が提唱した「DomainKeys」(参考文献 [1]) と米 Cisco Systems, Inc. が提唱した「Identified Internet Mail」を統合している。どちらも、メールヘッダに付与された電子署名を用いて認証する技術である。DKIM も同じ技術を利用してお

り、2006年度末には IETF での標準化を予定している。

電子署名を利用した認証方式の場合、一般的に認証局による証明書という第三者による身分証明が必要なケースが多い。しかし DKIM では、送信元の DNS を用いて公開鍵を公開するため、このような第三者機関を必要としない。身分証明のための第三者機関への支払いが発生しないのも特徴のひとつである。

DKIM はドメイン間の配送におけるメールの完全性を保証しており、その範囲でのメールの改ざんの検知と送信ドメインの真正性を提供する。S/MIME や PGP/MIME は、エンドユーザ間における情報機密を保証するが、DKIM はこれを保証できない。

4. JEAG RECOMMENDATION

送信ドメイン認証技術の目的は、メール送信者のドメインが正しい送信元から送信されているかを認証可能にすることである。受信側の認証処理の導入には、通常新たなコストが必要となるため、送信側の設定がある程度増えて効果の割合が高くならなければ、導入は慎重になると予想される。また、送信側としても、受信側の導入が増えなければ、新たに設定するメリットが少ないと受け取られてしまう。しかも、誤判定される可能性を危惧するあまり、送信側は設定に消極的になりかねない。

JEAG としては、このような硬直状態を避けるため、率先して普及のための提言を公開する必要があると考えている。送信側・受信側のいずれかの対応が進めば、もう一方は自ずと対応が増えるはずである。すなわち、ある一定割合を超えれば、飛躍的に送信ドメイン認証が普及するだろう。

送信ドメイン認証に最も簡単に対応する手段のひとつは、送信側のドメインの DNS に SPF レコードを宣言することである。まずは対応し易い設定から積極的に導入し、徐々に効果を上げていくべきだと考えている。

4.1. 送信側の設定

メール送信側では、正しい送り元からメールが送信されているかを、受信側で認証可能になるように情報を設定する必要がある。提案されているいくつかの送信ドメイン認証技術のうち、ここでは以下の技術を JEAG として提言する。

Recommend 1. 送信側ドメインのドメイン認証に関して

- 送信側のドメイン認証として、以下のいずれかの技術を導入するべきである
  - SPF Classic の DNS での宣言
  - DomainKeys (DKIM) の電子署名作成および DNS での宣言

4.1.1. SPF Classic の利用

SPF レコードの末尾には、それまでの宣言に適合しない場合に参照される “all” を限定子 (qualifier) とともに記述する。この限定子に何を使うべきか問題となる場合が多い。ここでは、ドメインの詐称が明確に判断できるよう以下の記述を SPF レコードの末尾に宣言することを提言する。

Recommend 2. SPF レコードの宣言に関して

- SPF レコードの末尾は “~all” もしくは ”-all” と宣言するべきである
  - 導入時は、”~all” とするのが安全である
- メール送信をしないドメインは “v=spf1 -all” と宣言するべきである

すでに宣言されている SPF レコードには末尾に “?all” と設定されているものも見受けられる。これは多くのメールサーバ管理者が、正当なメールが受信側によって拒否されることを危惧するためと思われる。参考文献 [4] によれば、限定子 “?” に適合した場合の認証結果は、Neutral でありこれは None と同じように扱うべきと決められている。None は SPF レコードを宣言していない状態であるため、詐称されても受信側で判断できない。ここでは、ドメイン詐称された場合、Softfail となって判断できるよう “~all” と宣言することを提言する。

Recommend 3. “-all” への移行時期

- 後述のメール転送問題が解決した後には、すみやかに “~all” から “-all” へ移行するべきである。

SPF Classic では、メール転送時に認証失敗するという問題があるため、プロバイダなどメール転送サービスを提供しているドメインにおいては、“-all” の宣言をすることは困難である。しかしながら、後述の転送問題が解決した後には、すみやかに “-all” へ移行するべきである。

4.1.2. DKIM の利用

電子署名方式では、メールの送信時に発信者でなければ付けられない署名情報を付加する。そのため、DNS に SPF レコードを宣言すればよい IP アドレス方式に比べて導入の労力を必要とするが、メールの配送に関してはより柔軟な運用が可能である。例えば、IP アドレス方式で問題となる転送されたメールについては、メール中の署名対象部分が改変されない限り認証が可能である。また、署名時に必要な秘密鍵を正しく管理できれば、メールサーバホストに依存することなく、正規の送信元として使用できる。電子署名方式は、導入コストをかけても送信元を明確にしたい場合や、送信元情報を詐称されたくないメール発信者の間で、まず普及していく可能性が高いと考えている。

Recommend 4. DKIM の移行時期

- DomainKeys を利用しているサイトは、DKIM が規格化され次第、すみやかに DKIM の利用に移行するべきである

DomainKeys は、DKIM へ統一された規格とするべく標準化作業が進められている。普及のためには、同じような複数の規格が利用されるような状況は避けるべきであり、規格化された後には、すみやかに DKIM に移行すべきである。DNS 宣言については、認証に必要な公開鍵情報とともに署名ポリシー情報についても適切に宣言するべきである。ポリシーの宣言方法については、参考文献 [3] にしたがった形式とする。なお、宣言するべき内容については、次回の改訂で示す予定である。

4.2. 受信側の認証

迷惑メールによる直接的な被害を受けるのはメール受信側である。送信側の設定が普及するにつれて、受信側の認証効果は得やすくなる。これにより、受信側での認証処理の導入は進むと考えている。

ただし、認証に失敗したメールが必ずしも迷惑メールとは限らない点に注意するべきである。したがって、受信時のポリシーとして以下を提言する

Recommend 5. 認証結果による受け取り拒否について

- 単一の送信ドメイン認証技術の結果が Fail であっても受信を拒否するべきではない
- SPF Classic の Softfail で受信を拒否するべきではない

送信ドメイン認証技術の各方式には、それぞれ長所がある一方で短所も指摘されている。現段階では、明確に迷惑メールと判断するためには、複数の認証技術を組み合わせ、他の迷惑メール判定技術と複合的に判断するなどの処理が必要である。送信側の設定を促進するためにも、安易な判定によるメールの受信拒否は避けるべきである。なお、これは直接メールを受け取るメールサーバに対しての提言であり、メール利用者個々の判断まで制限はしない。

参考情報　1.　　エラーメールの取り扱い

- SPF Classic で Softfail、Fail になったメールで宛先が不明であった場合、エラーメールを作成しない方法がある。

エラーメールのほとんどは、ハーベスティングやウイルスメールによって引き起こされており、ほとんどが無意味である。これを低減するために、SPF Classic の認証結果を積極的に利用するべきと考える。これを実施することで、SPF Classic を宣言しているドメインへの、送信元情報の詐称による宛先不明に対するエラーメールが減っていくことが期待できる。

4．3．　運用方針

近年、メールは単に送信者から受信者へ送られるだけでなく、特定の利用者間でメールを送受信し合うメーリングリストや、複数のメールアドレスを状況に応じて使い分けるなど、利用方法が多様になってきている。こういった環境でも正しく送信ドメイン認証が機能するような考慮が必要である。ここでは、いくつかの運用例を示し、それぞれで注意するべき点を提言する。本章は、提言に当たり具備するべき条件について記述する。

4．3．1．　メーリングリスト

現在提供されているメーリングリスト機能の多くは、通常のメールシステムとは別に専用の配送機能を利用している場合が多い。ここでは、これらメーリングリスト機能を提供する場合に注意するべき点について提言する。

Recommend　6.　　メーリングリストの運用について

- メーリングリストサーバは、送信ドメイン認証を実施し、投稿者の管理をするべきである。
- メーリングリストサーバは、SPF Classic 認証及び DomainKeys 認証の両方を採用するべきである。

大量配送を望む迷惑メール送信者にとって、メーリングリストはその性質上都合の良いシステムである。安易に迷惑メールを大量配布させないため、メーリングリスト機能には、投稿メールが迷惑メールであるかどうかの判定が必要であると考える。したがって、メーリングリストサーバで、積極的に送信ドメイン認証技術を導入するべきである。また、採用する認証方法についても、送信側が宣言に依存しないように、二つの方式を採用するべきである。

メーリングリストサーバで、メールを配送する場合には、SPF Classic と DomainKeys のどちらを用いても、メール配送時に認証が失敗する場合があるため、対応するべき内容について提言する。

Recommend　7.　　メーリングリストにおける SPF Classic の利用に関して

- メーリングリストサーバから参加メンバへ配送する際の送信元（エンベロープ From）はメーリングリスト管理者のアドレスとするべきである
- メーリングリストサーバは、投稿されたメールの受信時に認証処理をするべきである

メーリングリストは、投稿者からのメールを参加メンバへ再配送する。そのため、送信ドメイン認証が失敗しないよう再配送時のエンベロープ From にはメーリングリスト管理者のアドレスを利用するべきである。これは、SMTP の規格である参考文献［7］でもすでに述べられている。実際に、多くのメーリングリストで、このような実装となっている。

Recommend 8. メーリングリストにおける DomainKeys（DKIM）の利用に関して

- メールヘッダ情報や本文を改変する場合は再署名するべきである

電子署名方式における問題として、署名対象データ（ヘッダおよび本文）の改変があげられる。現在よく使われているメーリングリスト機能は、表題（Subject）への連番情報の挿入や、本文の末尾にメーリングリスト情報をフッタとして追加するなど、署名対象となる部分を改変することが多く見受けられる。電子署名方式は、転送など再配送に影響を受けないのが特徴であるが、こういったメーリングリストでは投稿者が署名情報を付けた場合、受信側で認証が失敗してしまう。このような場合を考えると、再署名処理をするべきである。

4．3．2． メールマガジン

メールマガジンとは、会員向け情報配信をするために、特定ユーザに対して一斉にメールを配送するサービスである。このサービスを提供するにあたって、注意するべき内容を提言する。

Recommend 9. メールマガジンにおける SPF Classic の利用に関して

- 配送上の送信元（エンベロープ From）はメールマガジン管理者用アドレスとするべきである

メールマガジンは、ヘッダアドレス、エンベロープ From を変えて送信するケースが多い。このような場合でも、送信ドメイン認証が失敗しないように、エンベロープ From にはメールマガジン管理者のアドレスを利用するべきである。

4．3．3． 第三者サーバ利用

第三者サーバ利用とは、利用者がインターネット接続しているプロバイダの管理外にあるメールサーバを経由してメールを送信する行為をいう。旅行先のホテルや外出先の公衆無線 LAN を利用して、利用者が契約しているプロバイダのメールサーバを使ってメールを送る場合など、容易に起こりうる。

例として、利用者が A と B という二つのプロバイダと契約し、A で利用しているメールアドレスを B が提供するメールサーバで利用する場合がある。たとえ B の接続回線を利用していたとしても、A のメールサーバを利用するべきである。その場合の問題点として B のプロバイダが OP25B を導入している場合が考えられるが、A のメールサーバの投稿ポートを利用すれば問題はない。詳細は、OP25B SWG の Recommendation（参考文献［9］）を参照して頂きたい。ここでは、投稿ポートの利用普及の過程における対策として、以下を提言する。

また、ホスティングサーバの利用も、インターネットの接続回線とホスティングサーバの契約先のプロバイダが異なれば、第三者サーバ利用に該当すると言える。

Recommend 10. 第三者サーバ利用について

- 送信者が指定するドメインを管理しているメールサーバは、SMTP 認証の必須な投稿ポートを用意するべきである
- エンベロープ From は自ドメインのアドレスを利用するべきである

第三者サーバの利用に限らないが、利用者のメール送信状況を常に把握可能なよう、SMTP 認証(SMTP-AUTH) によって利用者の特定をするべきである。

何らかの事情によって、第三者サーバを利用して SPF Classic 宣言されたメールアドレスを使用する場合、エンベロープ From をその第三者サーバで利用可能なメールアドレスにすることが望ましい。これにより、受信側での認証失敗を防ぐことができる。これは、あくまで一時的な対策であり、本来は利用するメールアドレスに対する本来のメールサーバに投稿することを推奨する。

4．3．4．　メール転送

SPF Classic による送信ドメイン認証においては、メールの転送を行った場合に転送先サーバでの認証が失敗する問題があることが判っている。ここでは、それを回避するための方策を参考情報として示す。

参考情報　2.　メール転送時のエンベロープ From について

- メール転送時に、転送元のユーザのメールアドレスでエンベロープ From を書き換える方法がある。
- エラーメールについては、以下のいずれかの案に対応する方法がある。
  - エラーメールについては転送元に保存し、転送を行わない。
  - エラーメールについては、エンベロープ From を書き換えずに転送する。

SPF Classic において、メール転送時の認証失敗を回避するためには、転送時でも正しいドメインのエンベロープ From で送る必要がある。具体的には、転送元のサーバでエンベロープ From を転送したユーザのメールアドレスに置き換えることで、実現が可能となる。

しかしながら、転送時に転送先で何らかのエラーが発生してエラーメールを返すと、転送元ユーザにメールが送信されることとなり、結果としてメールがループすることとなる。これを回避するためには、エラーメールを転送元に保存して転送しないか、エラーメールのエンベロープ From の書き換えをせずにそのまま転送し、エラーメールに対するエラーメールを作成しないという２つの方法が考えられる。前者は、送信者がエラーを確認できない、受信者が転送元サーバのメールも確認していないとエラーを確認できない、という欠点がある。後者は転送先で受信後エラーが発生すると、送信者、受信者ともエラーが発生したことを確認できないという欠点がある。

5．導入スケジュール

４．１章で述べた通り、送信ドメイン認証の普及には送信側設定の普及が重要と考えている。

Recommend　11.　Recommend 1 の実施時期に関して

- 2006 年 3 月末までに、送信側の対応を実施するべきである
- 2006 年 12 月までに、“?all” の宣言をやめ “~all” へ移行するべきである

JEAG 送信ドメイン認証 SWG 参加組織は原則実施することとする。他のメールサーバ管理者についても、できるだけ早く設定することを期待する。

参考文献

[1] Delany, M., "Domain-based Email Authentication Using Public-Keys Advertised in the DNS (DomainKeys)", draft-delany-domainkeys-base-03, September 2005.

[2] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and Thomas, M., "DomainKeys Identified Mail Signatures (DKIM)", draft-ietf-dkim-base-00 (work in progress), February 2006.

[3] Allman, E., Delany, M., Fenton, J., "DKIM Sender Signing Policy", draft-allman-dkim-ssp-01 (work in progress), October 2005.

[4] Wong, M., Schlitt, W., "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-MAIL, version 1", draft-schlitt-spf-classic-02, June 2005.

[5] Lyon J., Wong, M., "Sender ID: Authenticating E-Mail", draft-lyon-senderid-core-01, May 2005.

[6] Lyon J., "Purported Responsible Address in E-Mail Messages", draft-lyon-senderid-pra-01, May 2005.

[7] Klensin, J., "Simple Mail Transfer Protocol", RFC 2821, April 2001.

[8] Resnick, P., "Internet Message Format", RFC 2822, April 2001.

[9] JEAG OP25B SWG., “JEAG Recommendation ～ Outbound Port 25 Blocking について” (work in progress), February 2006.

JEAG Recommendation (Sender Authentication Sub Working Group)

2006 年 2 月 23 日　　初版発行

JEAG Recommendation 利用に際しての条件

連絡先：contact@jeag.jp