なりすましメール撲滅プログラム

～送信ドメイン認証技術普及工程表（改訂版）～

２０１２年7月

迷惑メール対策推進協議会

第１章　理想的なメール環境の整備に向けて

１　電子メールの利便性

インターネットは、一般への開放から 10 年余のうちに、世界中で広く利用される主要な情報伝達手段となっている。その中でも、電子メールは、簡便で安価なコミュニケーションの基礎的な手段として、様々な社会・経済・文化活動にとって、不可欠の基盤となっている。

２　現在の状況

電子メールの基礎的な技術は 1970 年代に作成されたものであり、広く利用されることになった現在では、当初想定していなかった問題が顕在化している。

近年、電子メールでは、そのプロトコル上認証機能が脆弱で、送信者情報が容易に偽装できることから、受信者側で送信者を確実に確認することができず、それによって、フィッシングや不当・架空請求、迷惑メール、最近では標的型攻撃メールなど、様々な問題が引き起こされている。

３　技術的な対応の可能性

電子メールのプロトコルは広く普及し、それ自体の大きな修正は事実上困難である。このため、なりすましの問題への対応として、現在のプロトコルを修正することなく認証機能を追加する技術が提案されている。その一つに、送信ドメイン認証技術がある。

送信ドメイン認証技術は、既存のメール配送の仕組みを変えることなく、受信側メールサーバーにおいて、メールの送信者情報が偽装されているかどうかをドメイン単位で確認することを可能とする技術である。具体的な方式は、大きく分けて、SPF/SenderID と DKIM の２つがあり、いずれの方式も、IETF で標準規格化されている。

４　なりすまし対策の効果

(1)　送信側

送信ドメイン認証技術に対応することにより、送信側では、自らのドメインがメールで詐称されるのを防ぐことが可能となる。特に企業にとってドメインは信頼の基礎となるため、その信頼性が毀損されないようにすることは重要である。

また、受信側が送信ドメイン認証技術に対応して認証を行っている場合には、送信側として送信ドメイン認証技術に対応することで、自ら発信するメールが受信してもらいやすくなる。さらに、受信側での対応が進んできた段階では、送信側で送信ドメイン認証技術に対応しないと、自ら発信するメールを受信してもらえなくなることも考えられる。

(2) 受信側

送信ドメイン認証技術に対応することにより、受信側では、受け取ったメールがなりすまされているかどうかの確認が可能となる。その結果を活用してフィルタリングをすることなどにより、メールの仕分けの手間の軽減などが期待される。

また、なりすましに起因するエラーメール誤配送の問題などにも対処できるなど、様々な場面で、この技術は、メールの配送の信頼性を高めるために活用できる。

さらに、この技術の活用により、なりすまされているかどうかが確認できるため、なりすまされていないことが確認されたメールに対してホワイトリストやコンテンツフィルタを適用するなど、他の技術と組み合わせて活用することにより、より効果的な迷惑メール対策を講ずることが可能となる。

5 理想的なメール環境の整備に向けて

送信ドメイン認証技術の活用には、送信側メールサーバーと受信側メールサーバーの双方での対応が必要となる。一方、この技術は、導入したメールサーバーから活用できるため、準備ができた者から順次対応することが可能である。

関係者が送信ドメイン認証技術に対応し、なりすましメールを検知可能とすることにより、迷惑メールへの効果的な対策を図るなど、失われかねない電子メールの信頼性を取り戻していくことが期待される。

このプログラムは、送信ドメイン認証技術を広く普及させるための工程を明らかにし、それに沿って具体的な取り組みを実施していくことにより、なりすましのない電子メール環境の整備を図っていくことを目的とするものである。

第2章　これまでの取り組み

1　現在の普及の状況

我が国では、送信ドメイン認証技術について、送信側での普及は一定程度進んできている。具体的には、全ドメインの約 45%が SPF/SenderID に対応している。その一方で、受信側は、主要なインターネットサービスプロバイダーにおいても対応していないところもあり、まだ普及が進んでいるとはいえない状況である。

2　関連組織でのこれまでの取り組み

(1)　WIDE・JPRS

WIDE プロジェクト及び JPRS では、共同して、2005 年４月以降、我が国のドメインでの送信ドメイン認証技術の送信側の DNS への設定状況を公表してきている。

(2)　インターネット協会

財団法人インターネット協会では、毎年開催している迷惑メール対策カンファレンスの中で、2005 年～2007 年、2009 年に、送信ドメイン認証技術の普及を議題としている。

(3)　JEAG

JEAG（Japan Email Anti-abuse Group）では、2006 年 2 月の送信ドメイン認証に関するレコメンデーションの作成・発表、各所での講演活動の実施など、送信ドメイン認証技術の普及のための取り組みを実施してきている。

(4)　政府

政府では、セキュリティ対策の年度計画の中で、2008 年度版以降、迷惑メール対策の一環として送信ドメイン認証技術の普及に取り組むことを定めており、最新の「情報セキュリティ 2012」では、政府機関において受信側においても送信ドメイン認証技術の採用を推進することを定めているほか、地方公共団体及び独立行政法人等が発信する電子メールについて、なりすまし防止として送信ドメイン認証技術の普及に取り組むことを定めている。

(5) 日本データ通信協会

一般財団法人日本データ通信協会では、2009 年 5 月以降、主要な ISP 等における送信ドメイン認証技術の送信側・受信側の対応状況について調査し、その結果をウェブページで公表している。

特に、2011 年 6 月からは、年に２回調査し、その結果をウェブページで公表している。

(6) 迷惑メール対策推進協議会

迷惑メール対策推進協議会では、2009 年 10 月の「送信ドメイン認証技術ワーキンググループ」の設置などにより、2010 年 7 月から「送信ドメイン認証技術導入マニュアル」の策定・公表、2011 年 1 月から一般向けのパンフレットの策定・公表、2010 年 9 月から送信ドメイン認証技術に関する説明会の実施など、送信ドメイン認証技術の普及のための様々な取り組みを実施してきている。

第3章　具体的な工程表

1　第1段階

(1)　目標

送信ドメイン認証技術により、受信側で、なりすましを簡単に見破ることができる環境の実現を目指す。ホワイトリストやコンテンツフィルタ等とあわせて利用することにより、迷惑メール対策が、より効果的に実施できるようになる。

この目標は、2012 年度中を期限とする。

(2)　送信側の取り組み

① 主要なドメインが、送信ドメイン認証技術のうち SPF/SenderID に対応するよう、一般企業、ISP 等への周知、導入支援を強化する。また、信頼性を求められる主体などでは DKIM への対応が望ましいことから、その周知、導入支援を実施する。

② SPF/SenderID に対応しているドメインでも、そのポリシーによっては受信側で認証結果が十分に活用できない場合があることから、”-all”化の促進など運用ポリシーの改善に関する周知を行う。また、SPF/SenderID での転送時の誤認証に対応するため、転送するメールサーバーでの対応等を促す取り組みを実施する。

③ DKIM の導入や運用には、相対的に多くの手間がかかることから、導入や運用が容易にできるよう、関係情報の提供などの取り組みを実施する。

④ 政府部門や大学等でも普及のため、関係者と協力して取り組みを実施する。

(3)　受信側の取り組み

① 大部分の利用者が送信ドメイン認証技術による認証結果を利用可能となるよう、主要な ISP 等での受信側での認証の実施を促進するとともに、認証結果のラベリングを元にしたメールクライアントソフトでのフィルタリング等の対応やセキュリティソフトでの認証結果の利活用を進める。

② 送信側の対策に関する周知とあわせ、一般企業等に対する受信側の対応に関する周知を実施する。

③ なりすまされていないことが確認されたメールに対して、ホワイトリストやコンテンツフィルタ等を適用するなどの対策を組み合わせて実施す

ることによる効率的な迷惑メール対策の実施方法について整理し、周知する。

④　エラーメール誤配送の問題への対応など、受信側メールサーバーにおける送信ドメイン認証技術のさらなる利活用によるメール利用環境の向上方策について、検討し、周知する。

(4)　利用者への周知の取り組み

利用者に対して、送信ドメイン認証技術の概要や、具体的な利活用の方法について周知する。その際、ホワイトリストやフィルタリングなどと組み合わせることなど、迷惑メールへの効果的な対応方策を分かりやすく解説する。

2　第2段階

(1)　目標

送信ドメイン認証技術により、我が国において、ドメイン単位でのなりすましメールがないインターネット環境の実現を目指す。具体的には、送信ドメイン認証技術が広く普及することにより、受信側のメールサーバー段階で、送信ドメイン認証技術で認証されない国内の電子メールをブロックすることが可能となるような環境の整備を実現する。

これにより、国内のドメインになりすまして送信される迷惑メールを撲滅し、より一層効率的な迷惑メール対策を行うことが可能となる。

(2)　送信側の取り組み

① 我が国のドメインのすべてが送信ドメイン認証技術に対応するよう、さらなる周知、導入支援の活動を実施する。

② メール転送に係る問題やメーリングリスト関連の問題など、誤判定が起こる可能性がある場合に対して、受信側ではなく、送信側で対応するように、運用ポリシーの改善等の働きかけを実施する。

③ 政府部門や大学等でも普及が進むよう、引き続き、関係者と協力して取り組む。

(3)　受信側の取り組み

① 利用者のすべてが送信ドメイン認証技術による認証を利用可能な状態になるよう、主要な ISP 等での受信側の対応を促進する。さらに、判定不能や誤判定が起こらないことを確認された場合には、ISP 等の段階での必要に応じた送信ドメイン認証技術による認証がされない国内発の電子メールをブロックする取り組みの実施について検討する。

② なりすましメールがないことを前提とし、送信ドメイン認証技術と他の対策とを組み合わせることによる効率的な迷惑メール対策の実施方法についての周知を強化する。

③ 引き続き、一般企業等に対する周知を実施する。

(4)　利用者への周知の取り組み

引き続き、利用者に対する送信ドメイン認証技術を活用した迷惑メール対策の具体的な利活用の方法についての周知を実施する。

3　最終段階

(1)　目標

インターネットは広く世界に開いていることから、我が国のみならず、全世界における、ドメイン単位でのなりすましメールがないインターネット環境の実現を目指す。

これにより、世界中で、なりすまして送信される迷惑メールが撲滅されるとともに、なりすましがないことを前提とした効率的な迷惑メール対策の実施が可能となる。

(2)　送信側・受信側の取り組み

我が国での取り組みの状況を踏まえ、諸外国における普及促進のための働きかけを実施する。

(3)　さらなる取り組み

引き続き、送信ドメイン認証技術の利活用方法についての周知を行う。

第4章　２０１２年度に取り組むべき課題

スマートフォンが急速に普及していく中で、迷惑メールの動向に注意を払いながら、以下の事項に精力的に取り組んでいくこととする。

1　企業・団体向けの説明会等の実施

① 2011 年から作成・公表しているパンフレット「電子メールのなりすまし対策」、技術担当者向けの「送信ドメイン認証技術導入マニュアル」について、必要な改訂を行い、公表する。　【随時更新】

② 電気通信事業者や広告関係者など、主要な協議会の構成員の会員等に対する説明会の実施や協議会以外の主要企業等に対する周知や導入の働きかけを引き続き実施具体的には、個別企業や業界団体等に対する説明会等を通じて周知を行う。　【随時説明会を開催】

2　利用者での活用のための受信側の対応の促進

① ISP 等で、送信ドメイン認証技術による認証及びその結果に基づくラベリングやフィルタリングの在り方に関する検討を実施するよう、関係団体に対する働きかけを実施する。　【随時働きかけ】

② ISP 等における送信ドメイン認証技術の導入状況（送信側、受信側）について、（財）日本データ通信協会で、年２回調査し、継続的に公表していく。　【継続的に実施】

③ セキュリティソフトのベンダーにおいて、送信ドメイン認証技術による認証結果も活用するよう取り組む。　【継続的に実施】

3　利用者への周知

① 一般利用者に向けた電子メールのなりすまし対策に関する理解を促進するための資料を作成し、（財）日本データ通信協会のウェブページで公表する。　【初版を６月に作成、随時更新】

② ISP 等や（財）日本データ通信協会のウェブページなどを通じて、一般利用者に対する周知活動を実施する。 【継続的に実施】

4 その他の取り組み

① 実際に流通する電子メールにおける認証結果の状況について、総務省において、関係事業者の協力を得つつ、継続的に調査を行う。 【継続的に実施】

② 送信側における送信ドメイン認証技術の導入に際して、正しい記述が行われるよう促す取り組みを実施する。 【継続的に実施】

③ 政府機関や地方自治体、大学等における導入を促進するため、関係組織等と協力して取り組みを行う。 【継続的に実施】

（参考１）海外での取組状況

１　ＩＥＴＦでの標準規格化

送信ドメイン認証技術は、IETF で標準規格が提案されている。すなわち、SPF は RFC4408、SenderID は RFC4406、DKIM は RFC6376 が提案されている。

また、認証結果のメールヘッダーへの記録形式（ラベリングの形式）に関する RFC5451 など、いくつかの RFC が提案されている。

２　国際機関での取組

OECD では、2006 年にスパム対策のツールキットを作成しており、その中で、スパムへの技術的対策の一つとして、送信ドメイン認証技術を取り上げて解説している。

３　各国での取組

(1)　米国

米国では、連邦取引委員会（FTC）が、2005 年 6 月に送信ドメイン認証技術関係のカンファレンスを開催し、また、同年 12 月の迷惑メール対策法（CAN-SPAM Act）の執行状況に関する議会報告で同技術の広範な導入の必要性に言及するなど、関連の取り組みを実施している。

また、米国を中心とした通信関連企業が集まり設立した団体である M^3AAWG では、送信ドメイン認証技術の導入に関するホワイトペーパーを作成するなどの取り組みを実施している。

さらに、米国の金融機関からなる非営利団体である BITS では、セキュリティ関係のツールキットでの導入推奨や、ベストプラクティス集作成の取り組みなどを実施している。

また、2012 年 1 月に、メール送信事業者等 15 社からなる迷惑メール対策やフィッシング対策等を目的とする「DMARC.org」が設立され、SPF、DKIM 等の技術を活用し、送信者認証を行うための仕組みを策定している。

(2)　カナダ

カナダでは、2005 年 5 月に、官民の関係者からなるタスクフォースが取

りまとめたレポートの中で、ISP 等のベストプラクティスの一つとして、送信ドメイン認証技術の導入をあげて、その導入を推奨している。

(3) オーストラリア

オーストラリアでは、2005 年 12 月に、インターネット協会（Internet Industry Association）が取りまとめた迷惑メール対策の規約の中で、サービスプロバイダに推奨されるベストプラクティスの一つとして、送信ドメイン認証技術を定めている。

(4) 韓国

韓国では、2009 年 10 月に、放送通信委員会（KCC）が取りまとめた「スパム防止総合対策」の中で、送信ドメイン認証技術を推進することを定めている。

2009 年 11 月に SPF 利用方法マニュアルを発表。また、2009 年の韓国情報保護振興院（KISA）の調査では約 45%のドメインで SPF を導入している。

（参考２）用語集

用語	説明
コンテンツフィルタ	電子メールの内容の特徴を元に機械的に判断して、専用フォルダに格納したり削除したりする機能。
情報セキュリティ2011	政府としての情報セキュリティに関する年度計画。2011年度及び2012年度に実施する情報セキュリティに関する具体的な取組について示している。なお、情報セキュリティに関する年度計画は、2009年度以前は、「セキュアジャパン」という名称であった。
送信者情報	電子メールの送信者を表す情報。例えば、from欄に表示される情報がこれにあたる（技術的には、header-fromと言われる）。そのほかにも、メールサーバー間での通信でやりとりされる際の送信者に関する情報などもある（技術的には、reverse pathと言われる。）。
送信ドメイン認証技術	メール送信元のドメインのDNSに問い合わせることにより、そのメールが確かにメール送信元として記されたメールサーバーから送信されたものであるか確認する技術。
SPF	Sender Policy Framework。送信ドメイン認証技術の１つ。送信側のメールサーバーのIPアドレスをDNSで宣言することにより、ネットワーク的に認証を実施する技術。メールサーバー間の通信でやりとりされる送信者情報（reverse-path）を用いる。RFC4408。
SenderID	送信ドメイン認証技術の１つ。SPFと同様に、送信側のメールサーバーのIPアドレスをDNSで宣言することにより、ネットワーク的に認証を実施する技術。SPFとの違いは、用いることができる送信者情報が多様になっている点である（SPFと同様の確認に加え、他の送信者情報を順次確認する（Resent-sender:→Resent-from:→Sender:→From:という順序）ことも可能。RFC4406。
DKIM	送信ドメイン認証技術の１つ。電子署名の技術を用いる。送信側のメールサーバーで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ざんの有無を確認することができる。RFC6376。
エラーメール誤配送の問題	送信者情報が偽装されていることにより、宛先不明等のエラーメールを、本来関係のない偽装された送信元に対して送付してしまう問題。
メール転送に係る問題	電子メールを転送している際に、転送するメールサーバで送信者情報を元のまま転送しているときに、送信者情報が偽装されていない場合でも、SPFでの認証が失敗する問題。
メーリングリスト関連の問題	メーリングリストへの投稿に関して、メーリングリストを取り扱うサーバーで再署名しないと、送信者情報が偽装されていない場

	合でも、DKIM での認証が失敗する問題。
電子メールのプロトコル	現在インターネットの電子メールの送受信に広く用いられているのは、SMTP(Simple Mail Transfer Protocol)である。その標準規格は、RFC5321 で定められている。
ドメイン	インターネット上に存在するコンピューターやネットワークを識別する名称。重複しないように ICANN という国際組織により一元管理されている。電子メールアドレスでは、@より右の部分にあたる。
メールクライアントソフト	クライアントで用いる電子メールのソフトウェア。ウェブメールの場合には、用いない。
メールサーバー	インターネット上で電子メールのやりとりをするためのコンピューター。
迷惑メール対策推進協議会	本協議会。迷惑メール対策に関する関係者が幅広く集まり、2008 年 11 月に発足。座長は、新美育文明治大学法学部教授。
ラベリング	電子メールの件名やヘッダーなどに、何らかの情報を記述すること。例えば、迷惑メールである可能性が高い電子メールの件名に[meiwaku]という記述をする場合などがある。
BITS	Banking Industry Technology Secretariat。
DMARC.org	Domain-based Message Authentication, Reporting & Conformance。
DNS	Domain Name System。ドメイン名と IP アドレス（インターネット上で個別の端末を判別するための番号）を対応づけるデータベースシステム。インターネット上のコンピューターにアクセスするためには IP アドレスを知らなければならないが、直接 IP アドレスを入力するのは実用的ではないので、名前（ドメイン名）を用いてアクセスする方法が考案されたもの。
IETF	Internet Engineering Task Force。インターネット上で利用される技術の標準化を行う組織。策定された標準仕様は、RFC（Request For Comment）として発行される。
JEAG	Japan Email Anti-abuse Group。日本の通信関連企業が集まった迷惑メール対策の技術検討を行うグループ。
M³AAWG	Messaging,Malware and Mobile Anti-Abuse Working Group。迷惑メールを含めたインターネット上のウィルスによる Dos 攻撃などに対処するために通信関係企業が集まったグループ。
OECD	Organization for Economic Co-operation and Development。経済協力開発機構。