資料６－３－１

改訂版

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～

（案）

２０１３年9月

迷惑メール対策推進協議会

目　次

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、1990 年代半ばの一般への商用利用開放の後、現在では世界中で幅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、多くの企業や個人に日々活用されており、様々な社会・経済・文化活動にとって必要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インターネット利用が現在のような形で幅広く行われる前の 1970 年代に作成された。インターネットや電子メールが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も顕在化している。

特に、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ないという問題点がある。近年、送信者情報を詐称してフィッシング[1]や不当・架空請求、迷惑メール、標的型攻撃メール等[2]が行われる事例が多くあり、送信者情報が詐称されていることにより受信側が的確に受信拒絶ができない中で、様々な問題が引き起こされている。

また、インターネット選挙運動が解禁される[3]中で、電子メールのなりすまし防止についてもその重要性は更に高まってきているといえる。

３　技術的な対応の可能性

電子メールのプロトコルは既に広く普及しており、それ自体への大きな修正は事実上困難である。一方、送信者情報が簡単に詐称できてしまい、それを受信側で簡単に判断できない現在のメールの仕組みにより様々な問題が生じて

---

1 実在する送信者（例：大手金融機関や大手運送事業者等）を詐称し、実際とは異なる偽のウェブサイトに誘導するフィッシングなどの事例が多くある。

2 この他、実在する送信者を詐称して不正プログラムを実施させたり、ボットにされるなどの行為が行われている。また、送信者を詐称した迷惑メールも多く、宛先不明のエラーメールが詐称されたメールアドレス宛に大量に送信されるバックスキャッタの問題もある。

3 公職選挙法の一部を改正する法律（平成 25 年法律第 10 号）。4 月 26 日公布、5 月 26 日施行。

いる。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として、送信ドメイン認証技術が開発されている。送信ドメイン認証技術の普及により、送信者情報詐称の問題点を防ぐことが可能となる。これにより、電子メールの送信者・受信者ともにトラブルに巻き込まれることが防止され、より安心安全に電子メールを送受信できる環境が実現することが期待される。

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、①ネットワーク方式[4]と②電子署名方式[5]の２つがあり、ネットワーク方式の送信ドメイン認証には、Sender Policy Framework(SPF)と Sender ID という２つのインターネット標準[6]がある。また、電子署名方式については、Domain Keys Identified Mail（DKIM）というインターネット標準がある[7]。

また、既存の送信ドメイン認証（SPF 及び DKIM）を利用して、送信側が受信側に期待する、認証に失敗したメールの扱い方の指針を表明する仕組みとして DMARC[8]が標準化に向けて検討されている。

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、当該企業ドメイン（メールアドレス）が悪用されることを防止し、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、

---

4 SMTP プロトコルにおいて送信元のメールサーバー（MTA）の IP アドレスを元にして認証。送信側で自分のドメインで利用している MTA の IP アドレスを公開

5送信側で公開鍵暗号方式を用いて、公開鍵と秘密鍵を用意し、あらかじめ公開鍵を公表した上で、秘密鍵を用いて送信するメールから電子署名を作成し、メールに付与した上で送信することで、受信側での電子署名の照会を可能とする。

6 IETF において標準規格化されている。SPF(RFC4408)、Sender ID (RFC4406,RFC4407)、DKIM（RFC6376）、DKIM-ADSP(RFC5617)

7 メール作成者の署名による DKM-ADSP（Domainkeys Identified Mail-Author Domain Signing Practices）も IETF において標準規格化されている（RFC5617）。

8 Domain-based Message Authentication, Reporting & Conformance（DMARC）：ドメイン認証できないメールの処理に関する標準企画案が 2012 年 3 月 30 日に公表。その後修正が加えられ、RFC ドラフトとして公開されている。

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。さらに、詐称されたメールによりトラブルに巻き込まれることを防止する効果などが期待されるなど、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。

送信ドメイン認証技術の活用により、なりすまされているかどうかが確認できる環境が整うと、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導入と活用には、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。

電子メール送受信に関わる関係者が各主体のメール環境において、送信ドメイン認証技術に対応し、電子メールのインフラ全体として、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ことにより、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強く期待される。

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組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　これまでの取組

１　迷惑メール対策推進協議会による取組の方向性

迷惑メール対策推進協議会[9]は、2009 年 10 月に「送信ドメイン認証技術ワーキンググループ」を設置し、2010 年 7 月に「なりすましメール撲滅プログラム」（本プログラム）を作成・公表した。また、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組を実施してきている。

[9] 「迷惑メール対策推進協議会(Anti-Spam mail Promotion Council(ASPC))」（座長：新美育文 明治大学法学部教授）は、電気通信事業者、送信事業者、広告事業者、配信ＡＳＰ事業者、セキュリティベンダー、各関係団体、消費者、学識経験者、関係省庁 など迷惑メール対策に関わる関係者が幅広く集まり、関係者間の緊密な連絡を確保し、最新の情報共有、対応方策の検討、対外的な情報提供などを行うことなどにより、関係者による効果的な迷惑メール対策の推進に資することを目的に平成 20 年 11 月 27 日に設立された。

2　関連組織でのこれまでの取組

(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組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「サイバーセキュリティ 2013」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、なりすまし防止対策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。

3　なりすましメール撲滅プログラム第1段階（2010年7月～2013年3月）

(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)　プログラムを踏まえた迷惑メール対策推進協議会による取組

迷惑メール対策推進協議会では、なりすましメール撲滅プログラム第一段階（2010 年 7 月～2013 年 3 月）において、送信ドメイン認証技術の普及により、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して取組を進めた。

具体的には、平成 22 年（2010 年）9 月以降、電気通信事業者や広告関係者など、本協議会の主要な構成員の会員等に対する説明会を精力的に開催し、送信ドメイン認証技術の導入方法や課題への対応方法等について周知を図った。

さらに、高いドメインの信頼性が求められると考えられる自治体、金融機関等の業界団体の協力を得て、説明会やリーフレットの活動等を行うことにより、送信ドメイン認証技術の必要性について認知度を高めるとともに、その導入率の向上に努めた（参考資料→「送信ドメイン認証技術の企業・団体向け説明会の実施」）。

また、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方法について議論を開始した。

「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）抜粋

第3章　具体的な工程表

1　第1段階

(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。

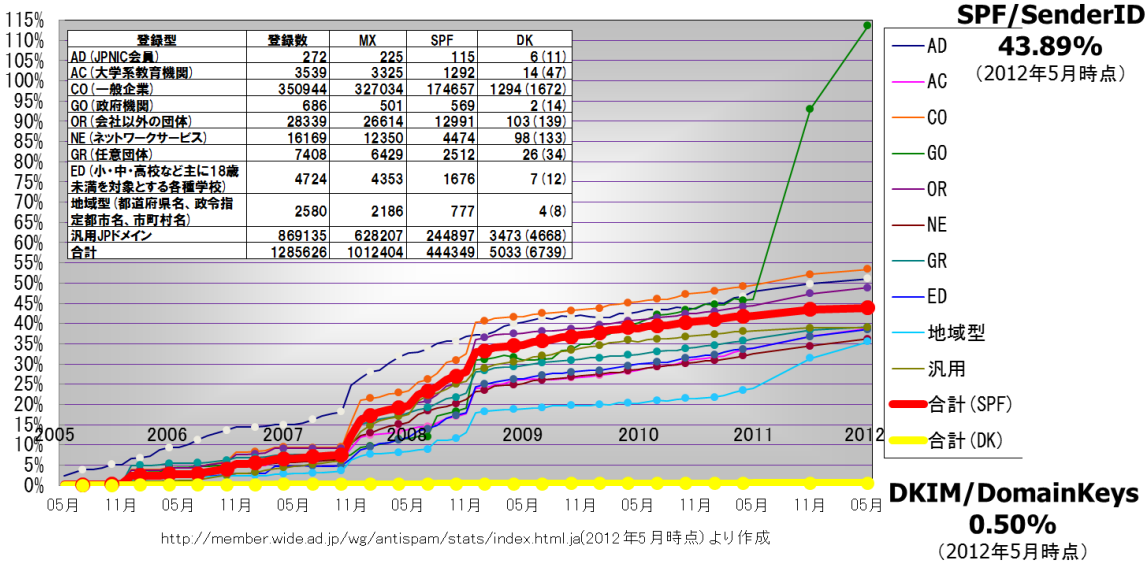
(3)　送信ドメイン認証技術の普及の状況について

【送信側】

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 44%が SPF/SenderID に対応している。

プログラムを開始した 2010 年 7 月以降の送信ドメイン認証技術の導入状況を見ると、ドメイン数としては SPF/SenderID については、2010 年 3 月現在の 38.7%から 2012 年 5 月現在の約 43.9%に 5.2%増加し、co.jp では 50%以上のドメインで導入、go.jp においても全てのドメインで導入されるなど一定の普及が進んでいることがわかる。また、電子署名方式の送信ドメイン認証技術である DKIM については、2010 年 3 月現在の 0.4%から 2012 年 5 月現在の約 0.5%に 0.1%増加している。

送信ドメイン認証技術の導入状況

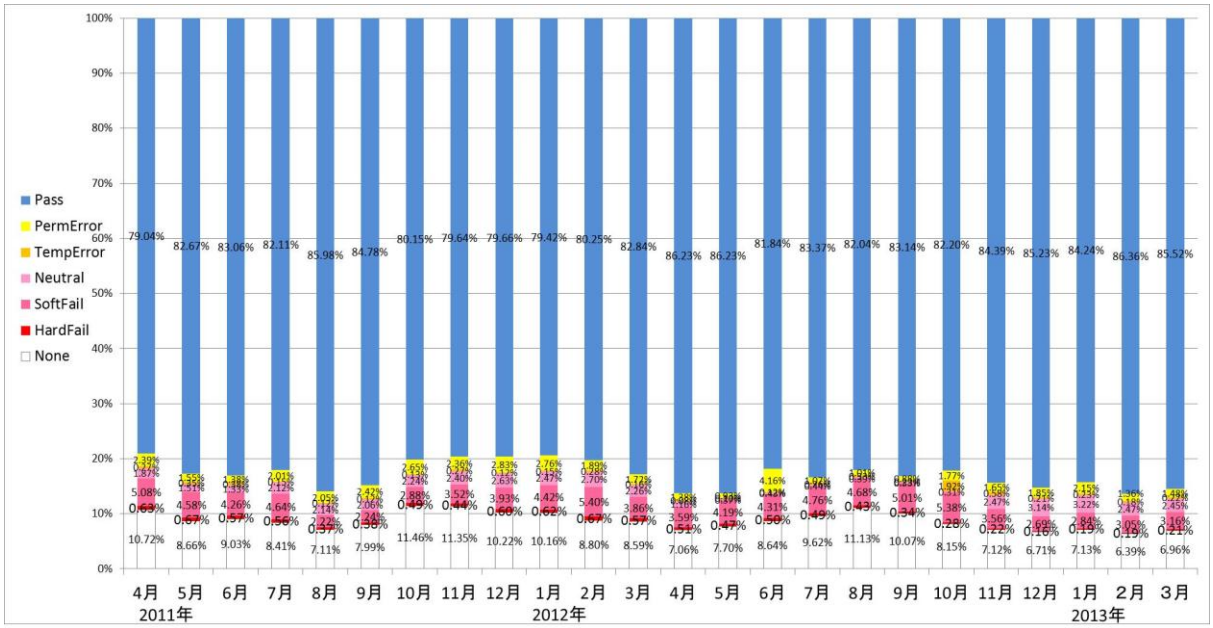


登録型	登録数	MX	SPF	DK
AD（JPNIC会員）	272	225	115	6（11）
AC（大学系教育機関）	3539	3325	1292	14（47）
CO（一般企業）	350944	327034	174657	1294（1672）
GO（政府機関）	686	501	569	2（14）
OR（会社以外の団体）	28339	26614	12991	103（139）
NE（ネットワークサービス）	16169	12350	4474	98（133）
GR（任意団体）	7408	6429	2512	26（34）
ED（小・中・高校など主に18歳未満を対象とする各種学校）	4724	4353	1676	7（12）
地域型（都道府県名、政令指定都市名、市町村名）	2580	2186	777	4（8）
汎用JPドメイン	869135	628207	244897	3473（4668）
合計	1285626	1012404	444349	5033（6739）

http://member.wide.ad.jp/wg/antispam/stats/index.html.ja(2012年5月時点)より作成

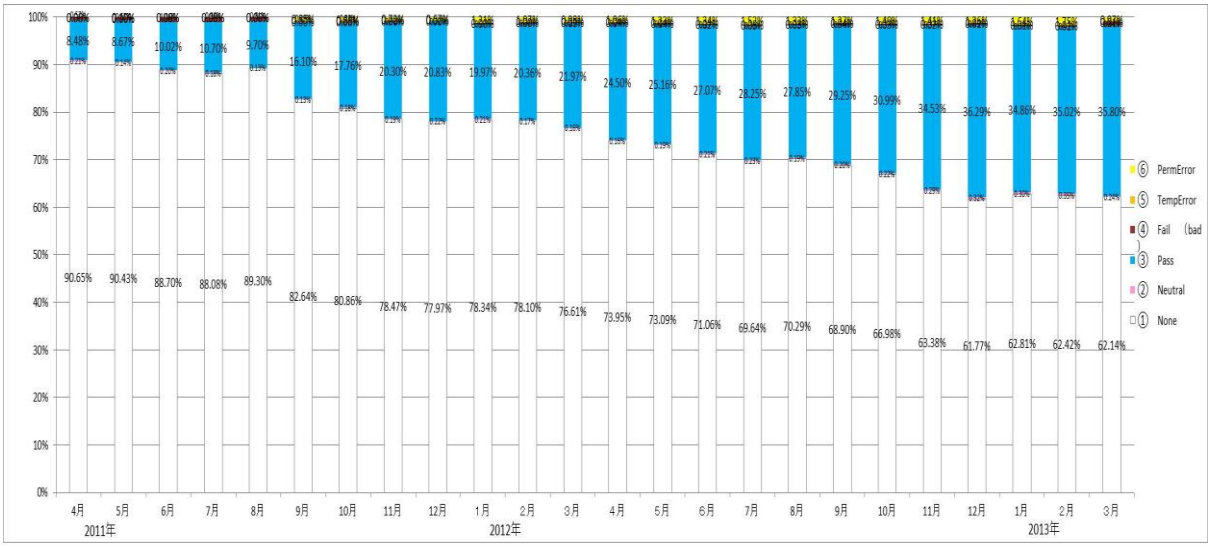
また、我が国で実際に流通しているメールの送信ドメイン認証技術への対応状況については、総務省が電気通信事業者の協力により行っている調査結果によると、SPF/SenderID については 2010 年 7 月の時点では約５割のメールが対応していたものが、2013 年 3 月時点では約 9 割のメールがこれに対応したドメインから送信され、そのうち 8 割以上が正規の送信元から送信されたメールとなるなど、プログラム期間中に顕著な増加がみられた。また、DKIM については、2010 年 7 月の時点では約 3%のみのメールがこれに対応していたが、2013 年 3 月時点では約 3 割が対応するなど、プログラム期間中に約 8 倍の普及率の増加がみられた。

送信ドメイン認証技術流量調査結果（ＳＰＦ／Ｓｅｎｄｅｒ ＩＤ）



※出典：電気通信事業者７社（KDDI(株)、NEC ビッグローブ(株)、(株)インターネットイニシアティブ、NTT コミュニケーションズ(株)、(株)テクノロジーネットワークス、ニフティ(株)、ヤフー(株)）の協力により総務省がとりまとめ

送信ドメイン認証技術流量調査結果（ＤＫＩＭ）



※出典：電気通信事業者４社（NEC ビッグローブ(株)、ヤフー(株)、(株)インターネットイニシアティブ、ニフティ(株)）の協力により総務省がとりまとめ

このように、本プログラムの第一段階の期間中において送信側については顕著な導入促進の実績が達成されたと評価できる。

【受信側】

総務省が毎年公表している「特定電子メール等による電子メールの送受信上の支障の防止に資する技術の研究開発及び電子メールに係る役務を提供する電気通信事業者によるその導入の状況」[10]によれば、送信側の対策については、調査対象の移動系電気通信事業者５社中５社すべて（100%）、固定系電気通信事業者 16 社中 16 社すべて（100%）が導入しているのに対し、受信側の対策については、調査対象の移動系電気通信事業者５社中２社（40%）、固定系電気通信事業者 16 社中８社（50%）が導入するにとどまっている。

また、日本データ通信協会の調査[11]によれば、送信側については、調査対象の電気通信事業者の全社が SPF/SenderID、DKIM のいずれかの方式で対応（SPF/SenderID：100%、DKIM：13%）している一方、受信側については、調査対象の電気通信事業者 168 社の 174 サービスのうち、ラベリング、フィルタリングのいずれかを実施しているのは 59 社（34%）（ラベリング：SPF/SenderID で 33%、DKIM で 18%、フィルタリング：SPF/SenderID で 10%、DKIM で５%）にとどまっている。

このように、送信側の対応は進展しているが、受信側については、主要な移動系電気通信事業者や固定系電気通信事業者においても未だ対応していないところもあり、まだ十分普及が進んでいるとはいえない状況であり、第二段階における課題として残されている。

プロバイダ、ケーブルテレビ、ケータイ／PHS 事業者における送信ドメイン認証実施状況

	送信側		受信側			
	SPF/ Sender ID	DKIM/	SPF/Sender ID		DKIM	
			ラベリング	ﾌｨﾙﾀﾘﾝｸﾞ	ラベリング	ﾌｨﾙﾀﾘﾝｸﾞ
プロバイダ	47/47 (100%)	6/47 (13%)	16/47 (34%)	5/47 (11%)	9/47 (19%)	4/47 (9%)
ケーブルテレビ	116/116 (100%)	13/116 (11%)	34/116 (29%)	8/116 (7%)	18/116 (16%)	3/116 (3%)
ケータイ／PHS	6/6 (100%)	0/6 (0%)	3/6 (50%)	4/6 (67%)	0/6 (0%)	0/6 (0%)
フリーメール	5/5 (100%)	3/5 (60%)	5/5 (100%)	1/5 (20%)	4/5 (80%)	1/5 (20%)
計	174/174 (100%)	22/174 (13%)	58/174 (33%)	18/174 (10%)	31/174 (18%)	8/174 (5%)

【利用者への周知】

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冊子「電子メールのなりすまし対策」を 2011 年１月から作成、公表し、（一財）日本データ通信協会のウェブページで公表してきている。

---

10 平成 25 年 3 月 29 日公表
（http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000102.html）

11 平成 25 年 4 月 10 日時点調査（http://www.dekyo.or.jp/soudan/auth/index.html）

第３章　今後の具体的な工程表

1　なりすましメール撲滅プログラム第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を活用して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、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、なりすましのない電子メールの信頼性が確保できる環境整備の実現を目指すこととする。[12]

また、送信側はもとより受信側の対策導入も一体として検討していく。

受信側が送信ドメイン認証技術を活用して送信者情報の認証や署名者の認証等により、受信者がなりすましメールを見分けたり、受信者が希望する場合にはなりすましメールを受け取らないなどの対応を行えるように、主要なインターネットサービスプロバイダー等とも協力しつつ取組を推進することとする。

これにより、他者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)　送信側の取組

本プログラムの第一段階の期間中において送信側については顕著な導入促進の実績が達成されたと評価できるものの、まだドメイン単位あるいは流量比で送信ドメイン認証技術を何ら導入していない事例も見られるため、受信側の導入を促進し、送信ドメイン認証が確認されないメールを確実に見分けたり受信しないなどの対応を行えるよう、SPF 又は DKIM のどちらかで必ず認証できる環境を目指すことが望ましい。このため、SPF[13]、DKIM[14]と

12　本プログラムは、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組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が、送信ドメイン認証技術が普及した段階では、紛らわしいドメイン名の利用や display name の悪用といった課題への対策をとっていくことが望ましい。

13　ドメイン単位で 43.9%（2012 年 5 月現在）、流量比で約 90%（2013 年 3 月現在）が導入されている。

14　ドメイン単位で 0.5%（2012 年 5 月現在）、流量比で約 30%（2013 年 3 月現在）が導入されている。

も更なる普及率向上を目指す。

また、DMARC のような新たな仕組みについても、国際的な動向を踏まえつつ対応する。

なお、第一段階に引き続き、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。

(3) 受信側の取組

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電子メールをブロックする取組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（確認された迷惑メール送信ドメイン等に対する対応をフィルタリング等を通じて行う等）。

(4) 利用者への周知の取組

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。

2 なりすましメール撲滅プログラムが最終的に目指すべき目標

(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・受信側の取組

我が国での取組の状況を踏まえ、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) 更なる取組

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　２０１３年度に取り組むべき施策

1　企業・団体向けの説明会等の実施

① 主要企業等に対する周知や導入の働きかけを継続的に実施。比較的導入率が低いがなりすましメールが送信された場合に一般利用者にもたらされる被害が重大となりうる金融機関、地方自治体、大学等の教育機関における導入を促進するため、関係組織等と協力して取組を行う。

【随時説明会を開催】

② 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】

③ 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組を継続する。【継続的に実施】

④ 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。【継続的に実施】

⑤ 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。【継続的に実施】

2　送信ドメイン認証技術を活用した送受信環境の改善

① 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、（一財）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】

② 金融機関等の業界団体・関係団体等に対して働きかけを行い、当該業界団体・関係団体等に関係する企業や法人等が一般利用者に対して電子メールを送信する際に実際に使用しているドメインを調査・集約した信頼のおけるドメインリストの策定と当該リストの電気通信事業者（携帯電話事業者及び ISP 等）への提供の依頼を検討する。

信頼のおけるドメインリストが策定された場合、電気通信事業者はこれを試行的に活用し、自社のフィルタリングサービスと連動させること等により、リストに登録されたドメインを利用する企業や法人等になりすましたメールの受信を防止する。

③ 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】

3 利用者での活用のための受信側の対応の促進

① 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、（一財）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。

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。 【継続的に実施】

② 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をどのように活用することを希望するか把握する。上記２②において信頼のおけるドメインリストが策定された場合、これを必要に応じ試行的に活用する。 【継続的に実施】

4 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周知啓発資料を作成し、（一財）日本データ通信協会のウェブページで公表するとともに、パンフレット等として印刷し必要に応じ配布する。

【随時更新】

② 一般利用者に向けた迷惑メール対策の一環として、迷惑メール対策に関する周知啓発資料等の中に電子メールのなりすまし対策に関する記述を追記し、（一財）日本データ通信協会のウェブページで公表するとともに、パンフレット等として印刷し必要に応じ配布する。 【随時更新】

③ ISP 等やその他迷惑メール対策推進協議会の会員各社のウェブページ等を通じて、一般利用者に対する周知活動を実施する。 【継続的に実施】

（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、DKIMーADSP は RFC5617 が提案され標準規格化されている。SPF については、2013 年 5 月、実験的カテゴリからスタンダードに格上げするインターネット・ドラフトが IETF に提案されている。

また、SPF 及び DKIM を利用して送信側が受信側に期待する、認証に失敗したメールの扱い方の指針を表明する仕組みとして DMARC（Domain-based Message Authentication, Reporting & Conformance）が標準化に向けて検討されている。標準企画案が 2012 年 3 月 30 日に公表され、その後の修正を経て RFC ドラフトとして公開されている。

さらに、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、関連の取組を実施している。

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組を実施している。

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組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。
サイバーセキュリティ 2013	政府としての情報セキュリティに関する年度計画。2013 年度及び 2014 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」、その後 2012 年度までは「情報セキュリティ」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、RFC5322.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, RFC4407。
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 Subject: ヘッダなどでメッセージの改変を行う場合、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。また、再署名した場合でも、作成者署名を認証対象にする DKIM-ADSP や DMARC による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	DMARC (Domain-based Message Authentication, Reporting & Conformance)技術を推進する団体。
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 Comments）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。

（参考３）

迷惑メール追放宣言

我が国では、携帯電話やインターネットの発展・普及に伴い、新たなコミュニケーション文化としての電子メールが広く国民に定着してきている。その一方で、いわゆる迷惑メールにより、望まない情報の着信による受信者への支障、大量のあて先不明の電子メールの処理に伴う電気通信ネットワークへの支障、正当なメールマーケティングを行う事業者への支障などがあり、さらにフィッシングやワンクリック詐欺等に結びつくこともあるなど、様々な支障が生じている。

この迷惑メールに対しては、平成１４年（２００２年）の「特定電子メールの送信の適正化等に関する法律」の制定及び「特定商取引に関する法律」の改正などによる制度的な対応が行われており、また、本年には、両法の一部改正により、いわゆるオプトイン規制が導入されるなど、実効性の効果に向けた規制の強化が図られてきているところである。

また、迷惑メール対策については、このような制度的な方策のみならず、技術的な対策、電気通信事業者による自主的な措置、利用者への周知啓発・相談体制の充実、国際連携の推進など、関係者による総合的対策が必要とされるものである。

このような中で、迷惑メール対策に関わる関係者が広く集まり、本日、「迷惑メー

ル対策推進協議会」を設置することとした。ここに集まった関係者は、それぞれの立場から自ら必要な措置を精力的に講じていくとともに、積極的に関係者への周知・広報活動を行うなど、継続的な取組を行うことにより、我が国からの迷惑メールの追放を図っていくことを宣言する。

２００８年１１月２７日

迷惑メール対策推進協議会

（別紙）

関係者が講ずるべき取組の例

（電気通信事業者）

○ ＯＰ２５Ｂなど、迷惑メールを送信させないための技術の開発･導入、外国の電気通信事業者への普及促進

○ 迷惑メールフィルタなど、受信者側で利用可能な迷惑メール対策のためのサービスの提供

○ 迷惑メールに関する関係者への周知

（広告関係者）

○ 適正な同意の取得など、健全性を確保したメールマーケティングの実施

○ 迷惑メールに関する関係者への周知

（配信事業者）

○ 広告･宣伝メールの適切な配信

○ 迷惑メールに関する関係者への周知

（セキュリティベンダー等）

○ 効果的なフィルタリングソフト等の提供

○ 迷惑メールに関する関係者への周知

（消費者団体等）

○ 利用者側で行える迷惑メールへの対応策についての消費者に対する周知

（行政機関等）

○ 法の迅速かつ適正な執行

○ 迷惑メールに関する関係者への周知

○ 迷惑メールに関する情報収集、受信者からの相談受付の適切な実施

○ 迷惑メール対策に係る外国執行当局との連携の推進

（その他関係者）

○ 送信ドメイン認証の活用など

○ 迷惑メールに関する関係者への周知

（参考４）

送信ドメイン認証技術に係る説明等の状況

1　協議会関係

主催者等	期日	対応者	概要
社団法人日本広告業協会	2010/9/17	・櫻庭主査、本間副主査（事務局、総務省陪席）	・インターネット広告小委員会で説明（先方約 10 名） ・会合後、事務局に、同協会会員社への周知を依頼
社団法人日本インターネットプロバイダー協会	2010/10/18	・櫻庭主査、本間副主査、末政、竹内（事務局、総務省陪席）	・地域 ISP 部会で説明(約 20 名） ・導入によるユーザークレーム回避策準備が導入条件、との意見強
一般社団法人モバイル・コンテンツ・フォーラム	2010/12/21	・櫻庭主査、本間副主査（事務局陪席）	・会員向けセミナーで説明(約 50 名）
財団法人インターネット協会	2011/3/8	・櫻庭主査	・電子メールセキュリティーセミナー in 熊本で紹介
社団法人日本広告業協会	2011/4/20	・櫻庭主査、本間副主査（事務局、総務省陪席）	・EDI 小委員会で説明（13 名）
違法・有害情報相談センター、通信４団体	2011/4/25 2011/4/26 2011/4/28	・櫻庭主査、本間副主査、末政、竹内（事務局陪席）	・事業者向けセミナーで説明 25 日：東京 26 日：名古屋 28 日：大阪
財団法人インターネット協会	2011/11/25	・櫻庭主査	・迷惑メール対策セミナー[新潟]で説明（30 名）

リーフレット配布

主催者等	期日	概要
全国消費者団体連絡会	2011/3/3	団体会合で会員に配布(50 部)
財団法人インターネット協会	2011/5/27	迷惑メール対策カンファレンスで配布(100 部)

2　協議会以外

主催者等	期日	対応者	概要
全国銀行業協会	2010/11/8	・櫻庭主査、本間主査（事務局、総務省陪席）	・E コマース部会で説明（約 20 名）
社団法人全国地方銀行協会	2010/11/22	・櫻庭主査、本間副主査、末政、（事務局、総務省陪席）	・ＥＢ関連業務部会で説明(約 20 名）

特別区情報システム勉強会	2011/2/25	・本間副主査（事務局席）	・特別区情報システム勉強会で説明（約 20 名）
社団法人生命保険協会	2011/3/4	・櫻庭主査、本間副主査、末政、竹内（事務局、総務省陪席）	・情報システム部会で説明（約 50 名）
日本証券業協会	2011/4/5	・櫻庭主査、本間副主査（事務局、総務省陪席）	・証券会社最高情報責任者（CIO）会議にて説明（約 20 名）
社団法人日本クレジット協会	2011/7/21	・櫻庭主査、本間副主査（事務局、総務省陪席）	・カード取引対応研究部会にて説明（約 30 名）
大阪府大阪電子自治体推進協議会	2011/8/24	・櫻庭主査（事務局陪席）	・第三次ＬGWAN整備等説明会において、大阪府及び大阪府下市町村に説明（約 60 名）
都道府県 CIO フォーラム	2011/9/2	総務省、事務局	・都道府県の CIO 等に説明（約 50 名）
財団法人地方自治情報センター	2011/10/12 2011/10/17 2011/10/18 2011/10/19 2011/10/21	・櫻庭主査	・都道府県・市町村の情報セキュリティ担当者を対象とした情報セキュリティ研修会で説明（合計約 500 名） 12 日：東京 17 日：大阪 18 日：福岡 19 日：名古屋 21 日：札幌
一般社団法人日本マーケティングリサーチ協会	2012/1/30	・櫻庭主査（事務局陪席）	・会員対象の説明会にて説明（約 20 名）
内閣官房情報セキュリティセンター（NISC）	2012/2/16	・櫻庭主査	・府省庁等の情報セキュリティ担当職員「標的型メール攻撃対策等についての車座集会」で説明
社団法人金融先物取引業協会	2012/2/24	・本間副主査（総務省、事務局陪席）	・会員セミナーにて説明（約 110 名）
社団法人日本通信販売協会	2012/3/2	・櫻庭主査（総務省、事務局陪席）	・会員対象のセミナーにて説明（約 20 名）
社団法人全国学習塾協会	2012/6/10	・総務省	・協会通常総会にて説明（約 40 名）
財団法人地方自治情報センター	2012/10/22 2012/10/24 2012/10/26 2012/10/30 2012/10/31 2012/11/2	・櫻庭主査 ・本間副主査 ・総務省 ・事務局	・都道府県・市町村の情報セキュリティ担当者を対象とした情報セキュリティ研修会で説明（合計約 785 名） 22 日：東京 24 日：東京 26 日：仙台 30 日：大阪 31 日：名古屋 2 日：福岡

会員誌への周知記事の掲載等

主催者等	期日	概要
社団法人日本クレジット協会	2011/6	・会員に周知文をメールで送付
社団法人日本フランチャイズチェーン協会	2011/7	・会員専用サイトに周知文を掲載。
株式会社東京証券取引所	2011/11	・広報誌「Exchange Square　vol.35」(11 月発行)に周知記事を掲載。
社団法人日本冷凍食品協会	2011/12	・会員向け機関誌「冷凍食品情報」に周知記事を掲載
社団法人投資信託協会	2012/2	・会員向けＨＰに掲載
社団法人信用金庫協会	2012/3	・会員向け機関誌「信用金庫」(3 月号)に周知記事を掲載
社団法人日本パブリックリレーションズ協会	2012/3	・協会ニュース（3 月号）に周知記事を掲載

リーフレット配布

主催者等	期日	概要
(財)地方自治情報センター（LASDEC）	2011/1/26 ～ 2011/2/28	・期間に開催される自治体向けセミナーにおいて、配布（330 部）
社団法人投資信託協会、社団法人日本証券投資顧問業協会	2012/3/5	・研修会において配布（300 部）

（参考５）

サイバーセキュリティ2013（2013.6.27 情報セキュリティ政策会議）（抜粋）

① 政府機関等における対策

１）情報及び情報システムに係る情報セキュリティ水準の一層の向上

【電子メールに係るなりすまし防止等の対応強化】

(ﾈ) 政府機関から発信する電子メールに係るなりすましの防止（内閣官房、総務省及び全府省庁）

a) 内閣官房及び全府省庁は、悪意の第三者が政府機関又は政府機関の職員になりすまし、一般国民や民間企業等に害を及ぼすことが無いよう、送信者側及び受信側における送信ドメイン認証技術の採用を推進するとともに、受信側対策の一層の推進を図る。また、DKIM や S/MIME のように暗号技術を利用した対策の導入を推進する。

b) 総務省において、迷惑メール対策に関わる関係者が幅広く参加し設立された「迷惑メール対策推進協議会」や、国内の主要インターネット接続サービス事業者や携帯電話事業者が中心となって設立された民間団体である「JEAG」等と連携して、送信側及び受信側における送信ドメイン認証技術（SPF、DKIM 等）等の導入を促進する。

【独立行政法人、地方公共団体等における対策の強化】

(ﾌ) 独立行政法人等における情報セキュリティ対策の推進（内閣官房、独立行政法人等所管府省庁及び関係府省庁）

c) 関係府省庁において、独立行政法人から発信する電子メールについて、悪意の第三者が独立行政法人又は独立行政法人の職員になりすまし、一般国民や民間企業等に害を及ぼすことが無いよう送信側及び受信側における SPF、DKIM 等の送信ドメイン認証技術の採用等を推進する。

(ﾍ) 地方公共団体の情報セキュリティ対策水準向上のための普及・啓発（総務省）

e) 総務省において、地方公共団体における SPF 等の送信ドメイン認証技術の採用を推進するため、地方公共団体における送信ドメイン認証技術の導入状況を調査するとともに導入の効果・有用性についてセミナーで解説するなど、普及・啓発を推進する。

④ サイバー空間の衛生

【その他】

(ヤ) スパムメール対策の強化（内閣官房、総務省及び消費者庁）

a) 総務省及び消費者庁において、巧妙化・悪質化が進展し全体として増加が続くスパムメールに対応するため、特定電子メール法及び特定商取引法の着実な執行等所要の措置を講じる。

b) 総務省において、国内の主要なインターネット接続サービス事業者や携帯電話事業者が中心となり設立された民間団体である「JEAG」等の業界団体と連携して、スパムメール送信の防止に効果のある技術である 25 番ポートブロックや送信ドメイン認証技術（SPF、DKIM 等）等の導入を促進する。

c) 総務省において、我が国に着信するスパムメールの大部分を占める海外から発信されるスパムメールに対応するため、スパムメール対策を行う外国執行当局との連携を強化するとともに、民間における国際的なスパムメール対策の連携を推進する。

d) 総務省において、その他、違法なスパムメールに関する情報を当該スパムメールの送信等に利用されたインターネット接続サービス事業者に通知し利用停止等の措置を促進する「迷惑メール追放支援プロジェクト」を実施する。