JEAG
Japan Email Anti-Abuse Group

JEAG Recommendation
～携帯電話宛の迷惑メールに対する提言書～

Wireless サブワーキンググループ
(Wireless SWG)

JEAG
Japan Email Anti-Abuse Group

目　次

JEAG
Japan Email Anti-Abuse Group

１． はじめに

１．１． 背景

我が国における携帯電話の契約者数は、2006年1月末現在で9,043万を超え[1] 、人口普及率は実に7割に達する。その中で、携帯電話のインターネット対応率は約9割近くに及び、韓国を除く諸外国に比べ突出している[2] 。この携帯電話のインターネット機能は、メールやコンテンツなどにより、世界に先駆けて日本独特の新しいコミュニケーション文化を創造してきたといえる。

特にメール受信を通知する機能が具備された携帯電話のメールサービスは、携帯電話の所有者の約87%が1週間に1回以上利用しており[3]、音声と同等以上の重要なサービスとなっている。

一方で、利用者が増加した携帯電話は、いつも身近にある便利なコミュニケーションツールであるが故に、常に負の側面が問題となってきた。特に迷惑メールは、2001年春頃から、主に出会い系サイトの宣伝を中心としたメールが増加し、携帯電話事業者に多くの苦情相談が寄せられるようになったほか、出会い系サイトに起因した犯罪も多発するなど社会的に大きな問題となっていった [4]。

１．２． Wireless サブワーキンググループ(SWG)発足の趣旨

背景で述べた、携帯電話宛の迷惑メール問題に対し、ISP 事業者及び携帯電話事業者は、様々な対策を行ってきた。特に2003年頃から急激に増加した携帯電話発の迷惑メールに対しては、各携帯電話事業者が送信数制限などの事業者や利用者にとって痛みを伴う対策を講じた。それらの対策が功を奏し、現在では、携帯電話宛の利用者に届く迷惑メール[5]および、携帯電話から発信される迷惑メールは逓減傾向にある((参考1)および、2.3.対策の成果)。

しかしながら、インターネット発の迷惑メールは、高速なインターネットアクセス環境(FTTH、xDSL など)の普及に伴い、短時間に大量のメール送信が可能となり、携帯電話宛に送信される迷惑メールは増加している。更に、大半の迷惑メールは、自前のメールサーバを利用して直接受信側のサーバへ送信されていることから、送信側 ISP 事業者では迷惑メール送信行為の実態をつかみ難い状況にある。

一方、迷惑メールの受信側となっている携帯電話事業者は、迷惑メールに起因した大量メールから設備を保護するため、大量の存在しない宛先にメールを送信してくるサイトからのメールを受信規制するなどの対策を行っているが、受信側の対策だけでは、流通する迷惑メールを減らすことは出来ない。

このような環境下で迷惑メール問題を抜本的に解決するには、送信側と受信側の双方で協力して対応しないとその効果が得られないことを意味している。そこで、過去から現在に至る迷惑メール送信の実態を把握した上で、ISP 事業者各社と携帯電話事業者各社が連携して、インターネット発携帯電話宛の迷惑メールを根絶し、健全なメール流通環境を実現することを目的とした Wireless SWG を立ち上げ、ISP 事業者と携帯電話事業者で議論を重ねてきた。

１．３． 本提言書の趣旨

本書は、Wireless SWG での議論をまとめた提言書であり、後述する対策は、ISP 事業者や携帯電話事業者がすでに実行し、携帯電話宛迷惑メールの抑制に効果を上げている対策が中心であって、

---

[1] *社団法人電気通信事業者協会（TCA）ホームページより（H18 年 1 月末現在）*

[2] *情報通信白書平成 17 年版より*

[3] *(株）ビデオリサーチ『ケータイ 2005 edition』調査結果より*

[4] *総務省『迷惑メールへの対応の在り方に関する研究会』最終報告書より*

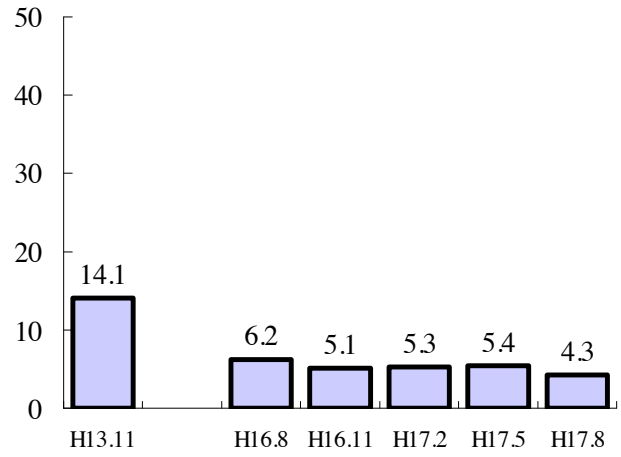
[5] *平成 13 年と平成 16 年を比較すると携帯電話宛の迷惑メールは 1／3 程度に減少しており、最近も減少傾向にある（通信販売の新たな課題に関する研究会『迷惑メール対策の今後の方向性』より*

本提言書で示される対策は、少なくとも現時点においては限りなくベストプラクティスに近いと言える。迷惑メール対策を検討する事業者においては、本提言書を参考にその導入を検討して頂くことを期待している。中には実現のためのハードルが高いと感じるかもしれないが、迷惑メールの対策に万能薬となる方法は無く、より効果をあげるためには、本書に記載する対策を一つでも多くご検討いただき、実現されることを期待したい。掲載の対策については、各項の主旨をご理解いただき、実現の方法や運用に関しては、各事業者の事情に合わせて実施していただければ良いと考えている。

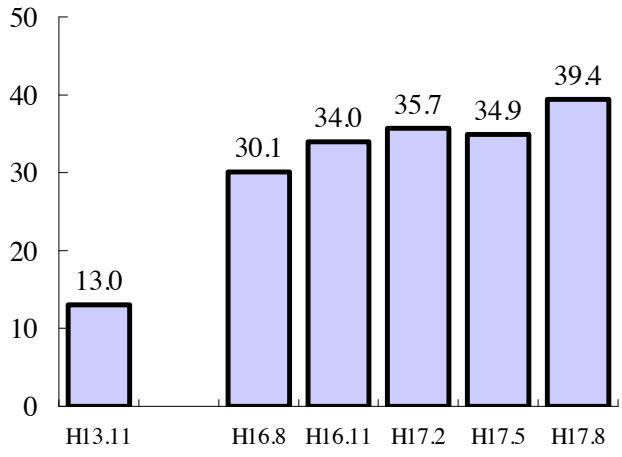
各事業者において迷惑メール対策の検討が行われている昨今において、迷惑メール送信者は規制が少なく、迷惑メール送信がしやすい事業者へ渡ってゆくこと[6]も考えられるため、このようなリスクに備え、より健全に事業に取り組む観点からも、本提言書を参考にしていただきたい。

なお、本提言書は携帯電話宛の迷惑メールの減少を目的としているが、ここで提言した対策の一部は、昨今増加傾向にあるパソコン宛の迷惑メール(参考2)の対策についても効果が期待できる。

(参考 1)携帯電話迷惑メール受信数(件/週)



(参考 2)パソコン迷惑メール受信数(件/週)



※出典：経済産業省調査

2． 携帯電話事業者の対策

迷惑メールが社会問題化する中で、各携帯電話事業者は様々な対策を行い、迷惑メールを減少させてきたことは先に述べたとおりである。そこで本章では、携帯電話事業者が実施してきた主な対策とその成果を紹介する。

2．1． 迷惑メールの被害者を減少させるための対策

2．1．1． メールアドレス変更機能など

初期の携帯電話のメールアドレスは、携帯電話事業者によっては、電話番号と同一だったこともあり、迷惑メール送信者が容易にアドレスを推測することが可能であった。携帯電話事業者は、アドレスの変更機能や初期アドレスに英数字を混在させるなどの対策を実施した。アドレスが短く単純な利用者に対しては、長く、英数字が混在したメールアドレスへの変更を啓発してきた。その

[6] *迷惑メールを送信し利用停止措置を受けた者が、新たに他の電気通信事業者と契約をして迷惑メール等送信行為を繰り返すことを「渡り」と言う*

結果、各携帯電話事業者の利用者の多くがメールアドレスを変更しており[7]、それ自体が有効な迷惑メール対策となっている。

その後、メールアドレス変更機能を悪用して、メールアドレスを開拓[8]する迷惑メール業者が顕在化した。携帯電話事業者は、アドレス変更可能回数を制限するなどして、その防止に取り組んだ。

※各携帯電話事業者が提供しているアドレス変更機能など

事業者	概　　要
NTT ドコモ	・メールアドレス変更機能(1999.7) ・初期アドレスを電話番号から英数混在のアドレスに変更(2001.7) ・アドレス変更制限 3 回/日(2004.12)
KDDI	・初期アドレスは、英数混在で 20 桁のアドレスとなっており、利用者でメールアドレスが変更可能(EZ WIN・EZwebmulti コースのみ) ※EZwebmulti コースのサービス開始は、2001 年 12 月から。 ・アドレス変更制限 3 回/日
Vodafone	・メールアドレス変更機能(1999.12) ・初期アドレスを電話番号から 13～15 桁の英数字混在のアドレスに変更(2003.1) ・メールアドレス変更回数制限　3 回/日　最大 99 回(2004.6)
ウィルコム	・メールアドレス変更機能(2004.9) ・一度アドレス変更を実施すると 48 時間以内は変更不可(2004.9)

２．１．２．　受信機能の拡充

アドレス開拓された宛先に送信される迷惑メールを、携帯電話事業者側で一様に制限することは法制度の面からも困難なため、携帯電話事業者は利用者の意思で特定のドメインやアドレスから送信されるメールを受信または受信拒否する機能を提供した。

※各携帯電話事業者の受信(フィルタ)機能

事業者	概　　要
NTT ドコモ	・アドレス指定受信／指定拒否機能(2000.1) ・ドメイン指定受信機能(2002.1) ・未承諾広告※メール拒否機能(2002.10)
KDDI	・なりすましメール拒否機能 ・指定受信／指定拒否機能 ・未承諾広告※メール拒否機能
Vodafone	・受信可否アドレス設定(1999.12) ・未承諾広告メール受信設定(2002.8) ・なりすましメール受信設定(2005.3) ・URL リンク付きメール受信設定(2005.3)
ウィルコム	・指定拒否機能(1998.12) ・指定拒否アドレス登録件数拡張(2002.6) ・指定受信機能(2002.6) ・未承諾広告メール拒否機能(2002.6)

２．１．３．　利用者への啓発

上述の対策について、各携帯電話事業者は個々に、契約後の確認通知書や請求書同封物、店頭配布ツール、ホームページを通じ、長期間に渡り継続的な啓発を実施してきた。また、新聞、雑誌、TV、ラジオ、中吊り広告による啓発も実施した。

---

[7] *NTT ドコモの i モード契約者のメールアドレス変更率は 98%*

[8] *携帯電話のメールアドレス変更機能を用いて、入力したアドレスに変更できる／出来ないで、払出し済みのアドレスを確認し、実存するメールアドレスリストを作成する行為*

利用者への啓発は、確実にメッセージを届けるために継続することが重要であると考える。

２．２．　迷惑メールの加害者を根絶するための対策

２．２．１．　送信数制限

迷惑メールが社会問題化していく中で、2003年頃から携帯電話を発信元とする携帯電話宛の迷惑メールが顕著化してきた。各携帯電話事業者は、自社の利用者が迷惑メール送信者、すなわち加害者とならないよう送信数制限の導入を行った。

携帯電話は、独自の認証技術によりユーザ認証を行っているために、メール送信数を制限することができた。これにより、携帯電話から迷惑メールを大量送信することが困難となった。

※各携帯電話事業者のメール送信制限

事業者	概　　要
NTT ドコモ	i-mode メール ・1 日の送信通数を 1 回線あたり 1,000 通未満に制限(2003.10) ・i モードメールを 1 日に 200 通以上送信する相手からの受信拒否機能を提供(2004.1) SMS ・１日の送信通数を 200 通未満に制限(2005.8)
KDDI	E メール ・1 回の送信における同報宛先数を 5 件までに制限(2003.9) ・1 日の送信通数を 1 回線あたり 1,000 通未満に制限(2004.8) C メール(SMS) ・1 ヶ月の送信通数を 3,000～6,000 通に制限(2004.11)
Vodafone	Vodafone live!メール ・3 時間に 120 件以上の宛先に送信した場合、その後 21 時間規制 (2G スーパーメール/ロングメール/ロングＥメール　：2003.12) ・3 時間に 120 件以上の宛先に送信した場合、その後 21 時間規制(3G VGS メール：2004.3) ・24 時間以内に 1,000 件以上の宛先に送信した場合、その後 24 時間規制(3G MMS：2005.2) SMS ・１日に 500 件以上送信した場合、その後 20 日間規制(2G　スカイメール：2004.11) ・１日に 500 件以上送信した場合、その後 20 日間規制(3G SMS：2005.5)
ウィルコム	E メール ・1 日の送信通数を 1 回線あたり 1,000 通未満に制限(2004.8)

２．２．２．　利用停止措置

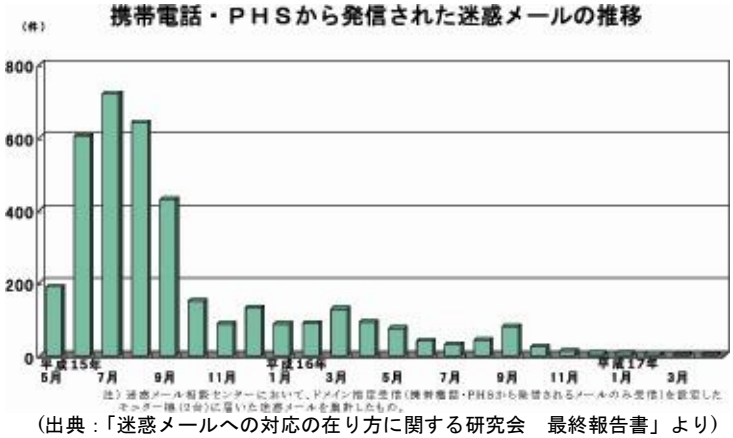
携帯電話は、ユーザ認証ができており、また、契約時の本人性確認を厳格に行っていることから、法令違反となる迷惑メールの大量送信行為が発生した場合、送信元の特定が比較的容易である。所在なども把握しているため、各携帯電話事業者は利用停止などの措置に努めた。

携帯電話事業者における利用停止回線数
６５，０００回線以上(2005.6)

（出典：「迷惑メールへの対応の在り方に関する研究会　最終報告書」より）

２．３．　対策の成果

上述の2. 1. および、2. 2. にあげられる対策の実施により、自社発の迷惑メールを『送信させない、受信させない、法令に違反して大量に迷惑メールを送信する者に対しては利用停止措置を実施する』ことで携帯電話発および携帯電話着の迷惑メールの根絶に尽力した。これらの成果とし、携帯電話事業者に寄せられる苦情数などは激減し[9]、携帯電話から送信される迷惑メールも大幅に減少した。



（出典：「迷惑メールへの対応の在り方に関する研究会　最終報告書」より）

３．　ISP 事業者経由の迷惑メール送信パターン

３．１．　パターンⅠ

ISP 事業者が提供している MTA[10] を利用して迷惑メールを送信する形態。ここでは、クライアント PC に IP アドレスが固定的に払出されているか、動的に払出されているかは問わない。

パターンⅠでは、ISP 事業者のログから利用者の特定や迷惑メールの送信事実が確認できるため、送信制限や利用停止などの対策が比較的容易に実施することができる。

３．２．　パターンⅡ

IP アドレスが動的に払出され、且つ、自営 MTA 経由または、インターネットに直接、迷惑メールを送信する形態。現時点では、迷惑メールの大半はパターンⅡの形態で送信されている。

IP アドレスが動的に変わるため受信側での規制がしづらく、また、送信元の特定に時間を要することが多いため、送信元を特定できた時には、すでに大量の迷惑メールを送信した後で、しかも姿を消していることが多い。また、送信されたメールのログは ISP 事業者側には残らないため、利用停止などの措置を実施する際には、各社でポリシーを整理しなければならない。

３．３．　パターンⅢ

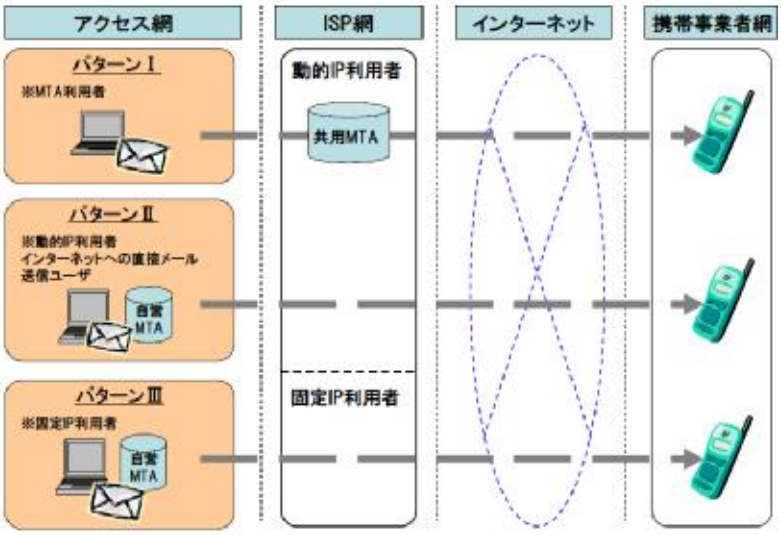
パターンⅡと、IP アドレスが固定化されている部分のみが異なる形態。IPアドレスが固定されているので比較的容易に迷惑メール送信者を特定できる。

---

[9] *NTT ドコモでは苦情件数の最も多い時期と比較して98%減少*

[10] *MSA (メーラーからメールの投稿を受け付け、配送するプログラム)または、MTA からメール配送を受け、配送するプログラム*

※各送信パターンの構成イメージ



４． パターンＩの迷惑メール対策

４．１． 送信数制限について

パターンＩの送信方法については、現在では ISP 事業者の多くがいわゆる Rate Control（Rate Limiting）[11]を行っていると思われる。これは、明らかな不正送信、例えば大量送信などに対する制限を目的としているが、メールサーバの運用が煩雑となってしまう側面がある。

パターンＩの規制に関しては、善良な利用者のメール送信に影響を与えることなく、迷惑メール送信者に対してのみ制限が機能するようにする必要があるのは言うまでもない。仮に、もし正確に同一の利用者を判断することができれば、送信数制限が有効な手段であることは容易に想像がつくと思う。例えば、メール送信について、善良な利用者が同一アカウントから 100通／日以上の送信をする可能性が低いことを合理的に判断できれば、送信 100通／日の上限値を設けたとしても、善良な利用者には影響を与えず、迷惑メール送信者にのみダメージを与えることが可能となるであろう。もちろん ISP 事業者によって、この規制値が、100通／日であるか、1000通／日であるか、あるいは 100通／時間であるかなどの適正値があるはずである。それぞれの ISP 事業者の利用者の使用状況に合わせてチューニングをしていただきたい。

実際、携帯電話発の送信に関しては、送信時に独自のユーザ認証を利用した宛先数制限が功を奏していることが見て取れる(参照：2.3.対策の成果)。携帯電話発とインターネット発では多少、事情の違いはあるが、総じてこの方法が有効であると思われる。

したがって、Wireless SWG では、ユーザ認証として一般的とされる MSA[12] での SMTP認証（以下、SMTP AUTH ）を必須として、この ID をベースとした送信数制限をかけることを推奨事項として提言したい。一般的な POP before SMTP[13] に関しては「動的な IP フィルタ」に過ぎないため、利用者を正確に特定することはできない。そのため、認証方式として POP before SMTP を利

---

11 ここではメール送信量に関する制限を指し、実現の方法は様々な方法がある

12 メーラーからメールの投稿を受け付け、配送するプログラム

13 電子メールの送信を行なう際のユーザ認証方法の一つ。送信前に指定した POP3 サーバにあらかじめアクセスさせることによって、SMTP サーバの使用許可を与える方式

用することは推奨しない。

導入については、既存の利用者に設定変更を求めることになるため、利用者へのインパクトが大きくなることが予想される。その際は、最初のフェーズとして、Submission Port (587番ポート)を利用して SMTP AUTH を実装した MSA を準備し、新規利用者やメーラーの設定変更を必要とする利用者から対応していき、徐々に既存の利用者に拡大するなど段階的な移行を実施することが現実的だと思われる。また、同時に、SMTP AUTH を実施していないサーバでは厳しい Rate Control を実施するなど、大量送信を許容しない対策を施すことが望ましい。

本件については、Outbound Port 25 Blocking SWG(OP25B SWG)のRecommendation[14] に詳細の記述があるのでご覧いただきたい。

※ ISP 事業者の事例

	概　　要
A 社の例	以下の対策を MSA へ適用 ・連続メール送信制限(2004.6) ・同一 IP アドレスからの SMTP 接続数制限(2004.9) ・Message Submission 対応 MSA の提供開始(2005.7)
B 社の例	以下の対策を MSA へ適用 ・同一 IP アドレスからのメッセージ数制限(2002.1) ・同一 IP アドレスからの SMTP 接続数制限(2002.1) ・Submission 対応(2005.10) ・SMTP AUTH 対応(2005.12)

注意) Outbound Port 25 Blocking による制限は除く

５．　パターンⅡの迷惑メール対策

パターンⅡの場合、セッションを切断する毎に IP アドレスが変わり、しかも自営メールサーバであるため、メール送信行為自体を特定することが困難である。そのような理由から、迷惑メールの多くが、パターンⅡの形態で送信されている[15]。したがって、迷惑メールを減少させるには、本項で示される対策を実行することが非常に重要である。

５．１．　Outbound Port 25 Blocking (OP25B)

JEAGのOP25B SWG で導入に向けた検討が進められているが、Wireless SWG としても、OP25B の積極的な導入を強く推奨したい[14]。すべての宛先に対してブロックすることが懸念される場合は、携帯電話事業者宛のメールに限りブロックするなどの段階的な導入を検討していただきたい。

これが実現できれば、迷惑メールの送信パターンはⅠかⅢとなるため、受信事業者側での受信ブロックや送信経路となった ISP 事業者側で迷惑メール送信者への利用停止措置などを効果的に実施することが可能となる。結果的に OP25B を導入した ISP 事業者からは迷惑メール業者がいなくなり、迷惑メールに係わるオペレーションコストが低減するとともに、レピュテーションリスクから開放されることとなるはずである。すでに、一部の ISP 事業者[16]が携帯電話事業者向けの OP25B を導入しており、パターンⅡの形態から送信される迷惑メールを根絶している[17]。

---

14 OP25B SWG の Recommendation については、JEAG のホームページ（http://www.jeag.jp）を参照してください

15 携帯電話事業者に寄せられた利用者からの申告に基づく想定

16 携帯電話メール宛に限定した対応も含めて、JEAG 参加企業の中で 13 社が導入済み（2006.2.21 現在）

17 パターンⅡに関する OP25B 以外の対策例（A 社）：A 社のメールサーバを経由しないで他社のメールサーバに直接メールを送信する"直接送信"において、同一 IP アドレスから一定時間内に大量に送信されるメールの流量を制御（2005.7）

なお、OP25B を導入する際に必要となる携帯電話事業者各社の接続先 MTA アドレスは下記のとおりであり、各社のホームページなどを通じ公開する予定である。また、アドレスの追加や変更が生じる場合は、概ね3ヶ月前に告知する。

※携帯電話事業者の受信 MTA の IP アドレスまたは帯域

	ドメイン	IP アドレス	帯　域
NTT ドコモ	@docomo.ne.jp	203.138.180.112 203.138.180.240 203.138.181.112 203.138.181.240	203.138.180.0/24 203.138.181.0/24 または、 203.138.180.0/23
KDDI	@ezweb.ne.jp	222.1.136.5 (2006 年 4 月頃にアドレスを 222.15.69.195 に変更予定)	－
Vodafone	@x.vodafone.ne.jp	－	210.169.176.0/24 210.169.171.0/24 202.179.204.0/24
ウィルコム	@xx.pdx.ne.jp	210.168.199.33	－

６． 各パターン共通の迷惑メール対策

６．１． 迷惑メールの情報収集と利用停止措置の実施

携帯電話事業者は、利用者が受信した迷惑メールを申告してもらい、特電法(特定電子メールの送信の適正化等に関する法律)に違反して大量の迷惑メールを送信した自社契約者に対し、予め定めた契約約款に基づき利用停止などの措置を行ってきた。この対策が大きな効果をあげたことは前述のとおりである。また、電子メール通信役務を提供する事業者にとって、利用停止措置を実行するための関係法令も整ってきている。

よって、ISP 事業者各社においても迷惑メールを送信した自社契約者に対して利用停止措置などを実施していない場合は、これを具現化する検討をなるべく早く開始することを推奨する。上記を実施するにあたり、利用者が受け取った迷惑メールを ISP 事業者側で収集することは、少なくともその情勢を知るにあたっては必要であることに異論はないと考える。情報収集の窓口は、一般の利用者から見て情報提供の方法が容易に調べられることが望ましい。

申告されたメールの全てに対して返信などアクションを取ることは大小さまざまな規模が存在する ISP 事業者の現状を考えると困難な場合も考えられる。そのため、収集した情報をどのように扱い対応するかのルールを事前に決めておき、利用者に伝えておくことが重要である。

※ ISP 事業者の迷惑メール情報収集の手段

	概　　要
A 社、C 社	Web サイト内でお問合せフォームを用意し、迷惑メールに関する対応を行っている
D 社	Web サイトで迷惑メール・不正行為のお問合せ窓口を紹介し、メール(abuse のメールアドレス)にて受付を行っている

※携帯電話事業者はメール窓口を開設し、利用者から情報を収集している

	NTT ドコモ	KDDI	Vodafone
申告先アドレス	imode-meiwaku@nttdocomo.co.jp	au-meiwaku@kddi.com	stop@meiwaku.vodafone.jp

利用停止が必要と判断してから実際に停止措置を実施する際に、契約者へ事前通知を行い、利用者の応答に対応していると、その間に迷惑メール送信者は、送れる限りの迷惑メールを送り、他の ISP 事業者へ渡り、当該の ISP 事業者からは姿を消してしまうケースが多くなってしまう[18]。したがって、通知書の発送から措置実施までは、あまり期間を空けないことを推奨する。

パターンⅡとパターンⅢに関しては、メールサーバが自営であるなどの理由により、利用者の特定や送信事実の確認が困難であることが多い。前述したように情報収集窓口を設け、送信元を認定するに足りる申告を多く受け付ける努力が必要となる。より信頼度の高い情報として、経済産業省および総務省が実施している迷惑メール追放支援プロジェクトなどによる申告メールもあるが、その数にも限りがあろう。そのため、携帯電話事業者側は、2005年11月に施行された改正特電法[19]により特定電子メールの範囲が企業などの事業用メールアドレス宛の送信にも拡大されたことで、携帯電話事業者の業務用電話に受信した迷惑メールを、法令に違反して大量に送信された迷惑メールとして各 ISP 事業者 に申告するという、独自の迷惑メール追放支援を検討している。 ISP 事業者各社においては、この情報を自社の迷惑メール対策に活かしてもらい、迷惑メール根絶への有効な手段として使用してもらえればと考える。

６．２．　本人性確認の重要性(強化の推奨)

６．２．１．　メール利用の制限

迷惑メールの送信方法に、オンラインサインアップを悪用し、ID / パスワード情報などの入手直後に大量の迷惑メールを送信するケースがある。

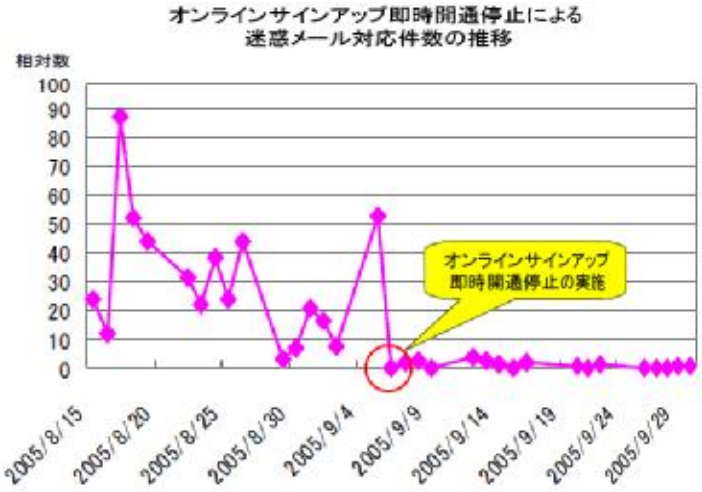
ISP 事業者側でも、確認書などを郵送し、不達となった場合に以後の利用を許容しないよう措置するなどの対策がとられているが、それまでの間に、大量の迷惑メールが送信されてしまう。

このことを回避するための方法の一つとして、まず、SMTP AUTH を導入し、次に、オンラインサインアップ直後のメール送信を大幅に制限し、最後に、確認書の郵送などにより契約時の情報や本人性の確認を行い、問題がなければ制限を開放する、などの対策が考えられる。(参照：4.1. 送信数制限について)

事業者 (効果対象)	ISP 事業者の取組み事例
A 社の例 (パターンⅠ)	入会直後に大量のメールを送信するケースに対応するため、入会直後の仮パスワード利用期間は送信できる最大通数を制限している。(2004.6)
C 社の例 (パターンⅡ)	これまで、オンラインサインアップ後に、利用に必要な情報(ネットワーク ID やメールアドレスなど)を画面上に表示することにより、オンラインサインアップ直後の即時利用を提供してきたが、オンラインアップ後すぐにサービスを利用できないよう、これらの情報を画面に表示しないこととした。 サービス加入者に対しては、従来通り郵送にてこれらの情報を案内し、この郵送物にある情報により、サービスの利用が可能とした。
E 社の例 (パターンⅠ、およびパターンⅡ)	一部のコースにおいてオンラインサインアップ直後の即時利用可能機能を停止し、利用に必要な情報(接続ＩＤやパスワードなど)を郵送で通知することとし、当該情報を受けとらなければインターネット接続ができない仕組みに変更するなどの対策を採っている。 また、即時利用可能機能を維持しながら、利用に必要な情報が通知されるまでの間は、メール送信に一定の制限を加え、大量メールを送信できない状態にする対策を採っている。

18 「渡り」は迷惑メール送信方法の巧妙化・悪質化した方法の一つとして、総務省『迷惑メールへの対応の在り方に関する研究会』最終報告書においても紹介されている

19 近年における送信の悪質化および巧妙化の現状に鑑み、特定電子メールの拡大や架空アドレスあての送信禁止等について規定を整備するとともに、罰則規定を整備するため、特定電子メールの送信の適正化等に関する法律の一部を改正する法律が施行された



C 社の取組みに関する効果(C 社提供データより)

６．２．２． 違反行為者の再契約の抑止

一度、利用停止措置などを受けた行為者に対し、契約約款などに基づき合理的な期間において再契約を拒むことは、迷惑メールを送信する行為を根絶する上で有効な手段である。

現在、ISP 事業者の多くがオンラインサインアップを導入しており、クレジットカードの与信チェックが通ればインターネットサービスを利用できるようになっている。

その際、与信に使われたクレジットカードが不正カードの場合、使用者は名前や住所、連絡先を容易に偽ることができ、結果的に虚偽契約となるケースも発生している。メールの利用制限や利用停止措置などが行われる中、迷惑メールの送信行為を根絶するためにも、虚偽契約ができる環境を改善するための検討が必要である。

迷惑メール送信者にとっても相応のリスクを負わせることができるので抑止力の観点からも効果は大きいと思われる。

６．２．３． その他

このオンラインサインアップによる虚偽契約は、迷惑メールをはじめとする犯罪の温床になる可能性が非常に高い。したがって、ISP 事業者には、できるだけ虚偽契約されない契約条件などの整備や仕組みを整えることが望ましい。

また、2006年3月に予定される携帯電話・PHS 事業者間での迷惑メール等送信行為に係る加入者情報交換は、事業者間をまたがった、いわゆる「渡り行為」をできなくする制度である。これが実現した大きな要因は、携帯電話事業者が適正な本人性確認を行い、利用停止措置を確実に行なってきたためだといえる。今後、ISP 事業者においても同様の制度の導入を検討する際には、行為者を特定するための、本人性の確認の適正化が前提となろう。

７． メーリングリスト、メールマガジンのアドレス管理と利用者への啓発など

７．１． メーリングリストとメールマガジンのアドレス管理の徹底

迷惑メールを送っていなくても、アドレスクリーニングを十分行っていないメーリングリスト(以下、ML)やメールマガジン(以下、メルマガ)が、結果的に宛先不明メール(不達メール)を送りつづけ、電子メール通信役務提供事業者の設備に多大な負荷を与え、安定したサービスの提供の妨げになるこ

とは、広く知られていない。

大量の宛先不明となるメールを送りつづけている場合、善意のメール送信であっても、設備保護の観点から受信規制などの影響を受けることがある。そのため、ML やメルマガのサービス管理者(事業者)は、存在しないメールアドレスへは、メール送信しないよう、会員などのメールアドレスの管理を徹底していただくようお願いしたい。

このような送信行為はメールのエチケットに反することを理解している利用者はまだ少ないので、ML やメルマガを配信する事業者やメールサービスを提供する事業者は、自社の利用者に対し、メールアドレスを変更する場合は、各自が登録しているML やメルマガのアドレスも変更するようホームページなどを通じ啓発をお願いしたい。

７．２．　ウィルススキャンの励行

ADSL などの普及で PC を常時インターネットに接続する環境が広がるなか、セキュリティへの関心が低い初心者などがウィルスに感染するリスクが高まっている。メール受信時やインターネットからファイルなどをダウンロードした際にウィルスに感染したり、不正侵入者に遠隔操作ソフトを仕掛けられたりすることで、持ち主である利用者がそのことに気付かずに自分の PC が迷惑メールを送信しつづけることがある。これらはボットなど(ゾンビ PC とも言う)と呼ばれ、迷惑メールを送信するだけではなく、他のコンピュータにウィルス感染させたり、他のコンピュータやネットワークへの不正侵入のための踏み台にされたりしてしまうこともある。

ISP 事業者は自社サービスを利用する利用者にウィルススキャンの励行などの啓発を行ったり、スキャンサービスなどを提供したりすることでこれらのリスクを軽減する取り組みを継続するようお願いしたい。

JEAG Recommendation（Wireless 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