JEAG
Japan Email Anti-Abuse Group

# *JEAG Recommendation*
# *～Outbound Port25 Blocking について～*

*OP25B サブワーキンググループ*
*(OP25B SWG)*

JEAG
Japan Email Anti-Abuse Group

# 目　次

JEAG
Japan Email Anti-Abuse Group

## 1. はじめに

インターネットは、 1960 年代に産声を上げてから今も拡大を続けている。
もともとインターネットは学術目的で成長を続けていたため、商用プロバイダが出現するまでは利用者は限定され、特別な制限を設けなくても脅威にさらされることなく性善説に基づいて成り立っていた。
その後、商用プロバイダの出現、オペレーティングシステム（OS）の利便性向上、パーソナルコンピュータ（PC）の低価格化、xDSL や FTTH、CATV ネットワークに代表される高速インターネットアクセス環境(以後、ブロードバンド)などの低価格化により、利用者の裾野が広がった。その結果、インターネット環境はより便利になった一方で、迷惑メールやウィルスなどの脅威にさらされており、もはや性善説だけで成り立たなくなっている。
特に、2006年2月現在の迷惑メールは ISP の提供するブロードバンド環境から数多く送信されている。これは、帯域あたりの価格が下がったことによる送信コストの低下や、ウィルスなどによって、悪意ある第三者に乗っ取られた PC（ボット、またはゾンビという）が増加していることが原因と考える。

ブロードバンド環境では、IP アドレスを動的に割当てること[1]が一般的であり、迷惑メール送信者はこのような提供形態を悪用し、迷惑メールの送信行為を特定しづらくしている。
このような送信手法に対して有効的な対策として、プロバイダが提供する動的 IP からメールサーバへ直接配信される迷惑メールを制限する Outbound Port 25 Blocking(以下、「OP25B」）という技術が注目されている。Japan Email Anti-abuse Group（JEAG）では、OP25B サブワーキンググループ（OP25B SWG）を設け、この技術を検討してきた。その成果として OP25B の導入の目的、実現方法、問題点や効果について明確になり、動的 IP を視点とした迷惑メールを根絶するために、本 Recommendation を作成した。
OP25B の普及は、日本発の迷惑メール根絶への第一歩であり、多くのプロバイダで導入が促進される事を期待する。

## 2. 本 Recommendation の位置づけについて

本Recommendationは、これまで JEAG の OP25B SWG で議論、検討された内容である。また、OP25B を実施する方法や導入手順を説明しており、JEAG メンバーのみならず、ISP、ASP、ホスティング事業者、通信事業者、企業、各種学校などのメールサーバ管理者やネットワーク管理者、メールクライアントやメールサーバの開発者、および、これらに関わるシステムインテグレータなどを対象としている。
迷惑メール対策は、正当なメールを迷惑メールと判断してしまう危険性（False Positive）を常にはらんでいる。特に、 OP25B はメール送信自体の規制であることから、実行に伴う弊害を極力抑制した上での実現が必要となる。 日本における OP25B は、2005 年 1 月のぷららネットワークスとボーダフォン間の携帯向け限定のブロッキングを始まりとして、2006年2月現在では、多くの ISP が導入を進めている。その導入の過程で新たに確認された問題点、およびその解決策については、整理され次第公表していく予定である。
なお、本 Recommendation は OP25B を普及させる事を目的として、その導入において実施す

---

[1] *固定 IP 接続契約以外で、インターネットに接続する場合、IP アドレスがランダムに払い出される場合が多い。このようにして割り当てられた IP アドレスが「動的 IP Address」であり、本 Recommendation 中では、「動的 IP」と表記する。*

るべきことを提言しており、強制力はない。しかしながら、迷惑メールを根絶する事を目標に、必ず実施するべき事項を「しなければならない」、できる限り実施が必要な事項を「するべきである」、できれば実施したほうが望ましい事項を「するのが望ましい」と表現する。

## 3. 技術情報

本 Recommendation で前提となる技術情報を以下に示す。

### 3. 1. 配送と投稿[2]

OP25Bを説明するにあたり、重要となる用語を以下の通り定義する。

MUA　：MSA にメールを投稿するプログラム
MSA　：MUA からメールの投稿を受け付け、配送するプログラム
MTA　：MSA または MTA からメールの配送を受け、配送するプログラム
投稿　：MUA が MSA にメールを委ねること
配送　：MTA がメールを他の MTA へ委ねること[3]

これまでは、「投稿」と「配送」、「MSA」と「MTA」は明確に区別されていなかったが、本 Recommendationでは、これらを明確に区別する。

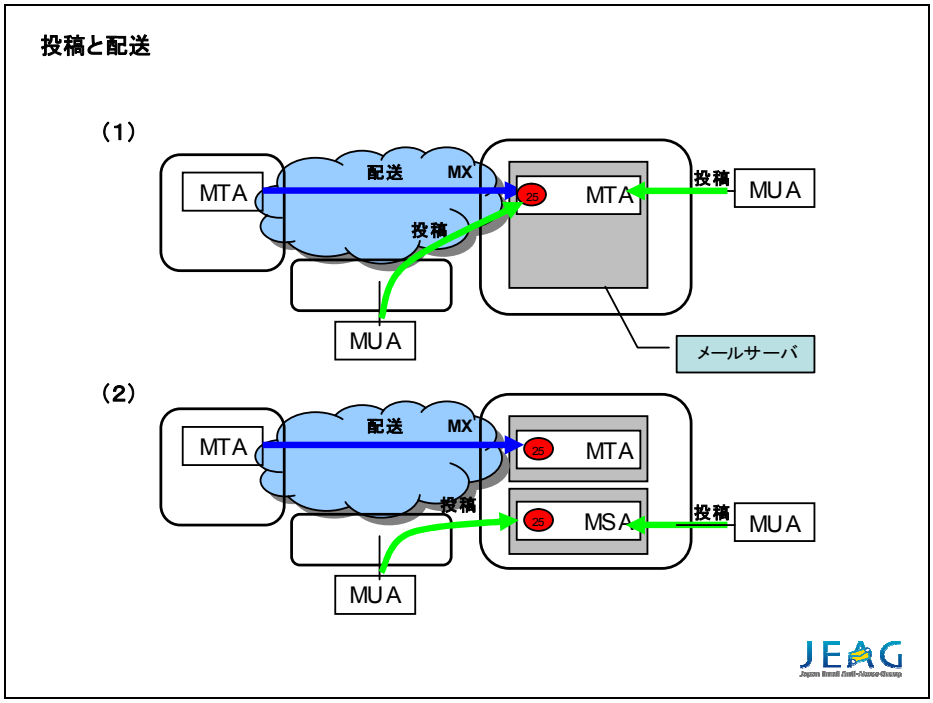


図 3-1

[2] イントラネットに閉じた環境での「投稿」「配送」は本 Recommendation では扱わない。

[3] 投稿とも配送とも表現できない場合は「送信」と表現する。

図 3-1 は、現在のメールサーバの代表的な構成を模式的に表している。

それぞれ、
(1) 一つの SMTP サーバが MSA と MTA を兼ねている構成
(2) MSA と MTA が分離されている構成
である。

(1) は、投稿用と配送用の 25 番ポートが同一の SMTP サーバで提供されているため、MSA と MTA の区別をすることができない。本 Recommendation では、この SMTP サーバへの投稿を「MTAへの投稿」と表現する。ただし、投稿に利用されていることを強調したい場合はMSAと表現するが、この時は、MTA の機能は考慮しなくてよい。
(2) は、投稿用と配送用の 25 番ポートが別々の SMTP サーバで提供されており、それぞれMSAとMTAに区別することができる。本 Recommendationでは、25 番ポートを利用した投稿用のSMTP サーバをMSA(25) と表現する。

## 3. 2. ISP モデルの整理

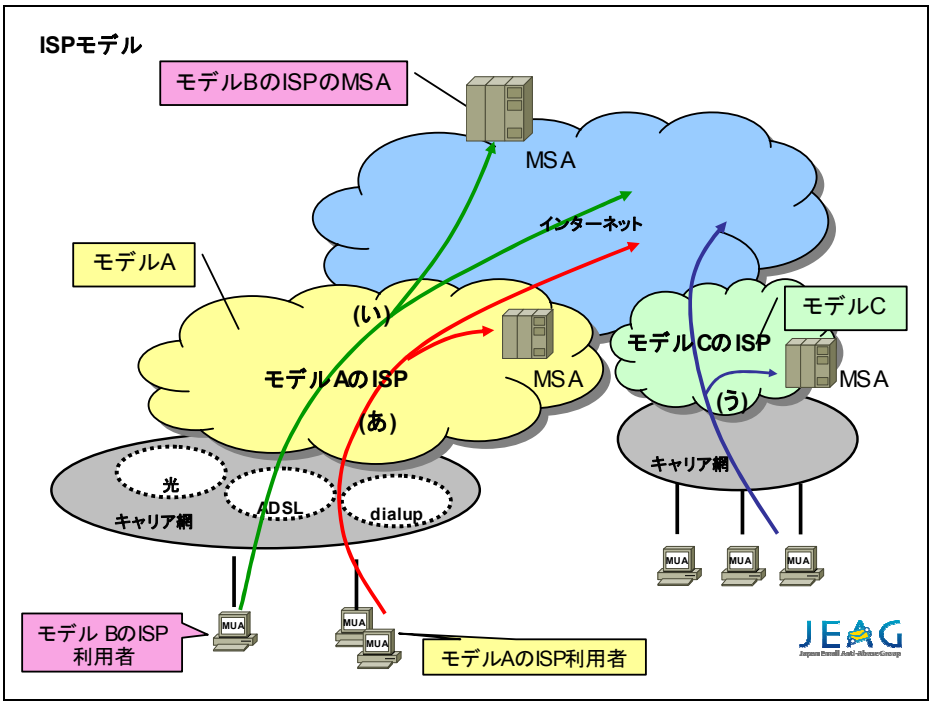


図 3-2

本 Recommendation では模式的に説明を行う[4]ので、ISP を以下のように 3 分類する。

モデル A ：インターネット接続を他の ISP(モデル B) に OEM 提供している
モデル B ：利用者のインターネット接続を他の ISP(モデル A) に依存している
モデル C ：自社のインターネット接続は自社のサービスでしか利用していない。

図 3-2 はそれぞれのモデルの ISP の利用者がどのようにインターネットへ接続しているか表している。

(あ) : モデル A の ISP の利用者のインターネットへの接続
(い) : モデル B の ISP の利用者のインターネットへの接続
(う) : モデル C の ISP の利用者のインターネットへの接続

図 3-2 はそれぞれのモデルの ISP の利用者がどのようにインターネットへ接続しているか表している。(あ) や (う) の線のように、モデル A とモデル C の ISP の利用者は、契約している ISP を経由してインターネットへ接続する。模式的には MSA は契約している ISP の内部にある。これに対し、モデル B の ISP の利用者は (い) の線のように ISP A を介してインターネットへ接続している。模式的には、MSA はインターネット上のいずれかの場所に存在していることになる。

[4] *ISP のネットワークに詳しい方には模式的過ぎるかもしれない。MSA が、バックボーンを管理する ISP の管理下にあるか否かという程度の意味である。*

## 3. 3. メールの配送経路

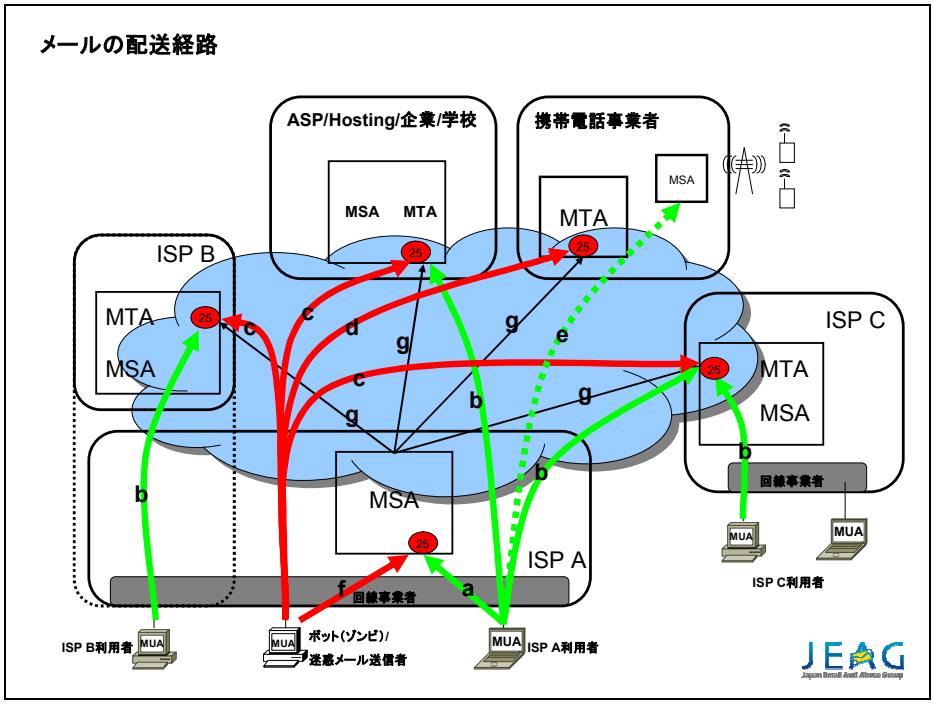


図 3-3

現在のメールの流れについて図 3-3 に模式的に示す。図 3-3 では「ISP A」がメールの送信側、「ISP B」「携帯電話事業者」「ISP C」「ASP/Hosting/企業/学校」を受信側としている。ここで、赤い線（c,d の線）が迷惑メールの配送経路でありOP25Bの対象である。緑の線（b の線）が通常のメールの配送経路である。

ISP A　：モデル A の ISP
ISP B　：モデル B の ISP
ISP C　：モデル C の ISP
PCの絵 ：動的IPを取得しているPC
- 利用者：ISP の契約者(迷惑メール送信者、ボットは含まない)
- 迷惑メール送信者
- ボット

a：利用者（MUA）の MSA(25) あるいは MTA への投稿
b：利用者（MUA）の「ISP Aの外部にある MSA」への投稿
- ISP B の利用者が ISP B の提供する MSA へ投稿する場合もこれにあた者

c：迷惑メール送信者やボットの「ISP A の外部にある MTA」への送信
d：迷惑メール送信者やボットの「携帯電話事業者の MTA」への送信

e：利用者（MUA）の携帯電話事業者への投稿（存在しない）
f：迷惑メール送信者やボットのMSAへの投稿
g：MTA 間（あるいは MSA→MTA）のメールの配送

### 3. 4. 迷惑メールの送信方法の分類とその対策

迷惑メールの送信方法には、大別して以下の２つのパターンがある。それぞれ、パターンI、パターンIIと呼称する。

パターンⅠ：MSAにメールを投稿して送信する方法
パターンII：動的 IP から、標的の MTA に対して、直接迷惑メールを送信する方法

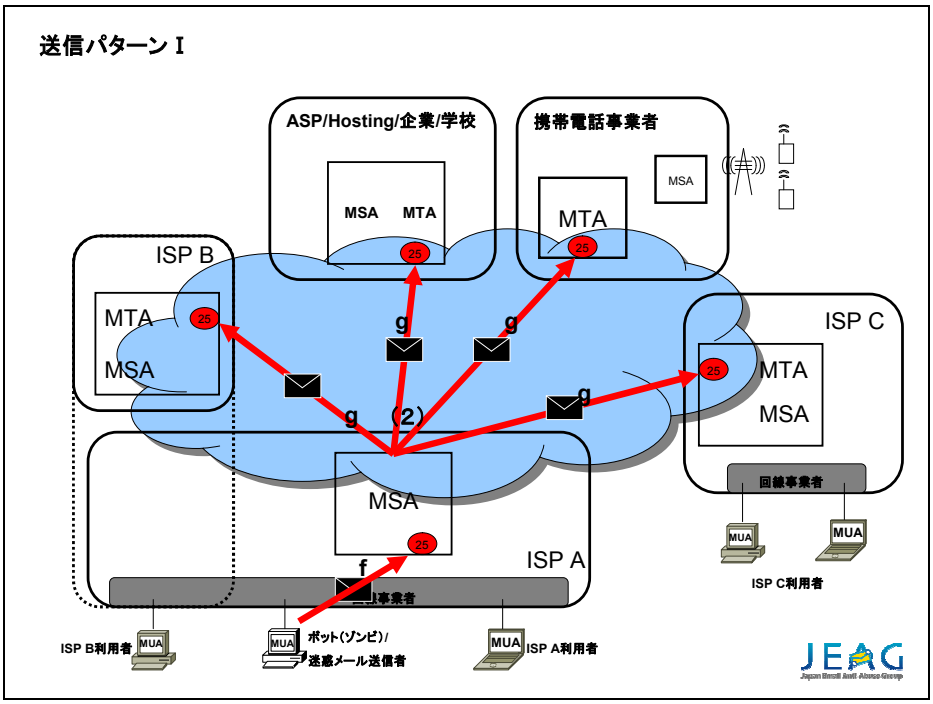


図 3-4

パターンⅠのメール送信経路について、図 3-4 に示す。
(1) 迷惑メール送信者が MSA へ迷惑メールを投稿する（f の線）
(2) 投稿された迷惑メールは MSA によって標的のドメインの MTA へ配送される（g の線）
この送信方法は、利用者の MUA を利用したメール送信方法と経路は同じである。
この送信方法への有効な対策は、 MSA においてユーザ認証に基づいた送信数制限であり、ユーザ認証を完全に実施している携帯電話発の迷惑メール対策ですでに効果が現れている。詳しくは、Wireless サブワーキング（Wireless SWG）からの「携帯電話宛迷惑メール対策に関する提言書」を参照のこと。

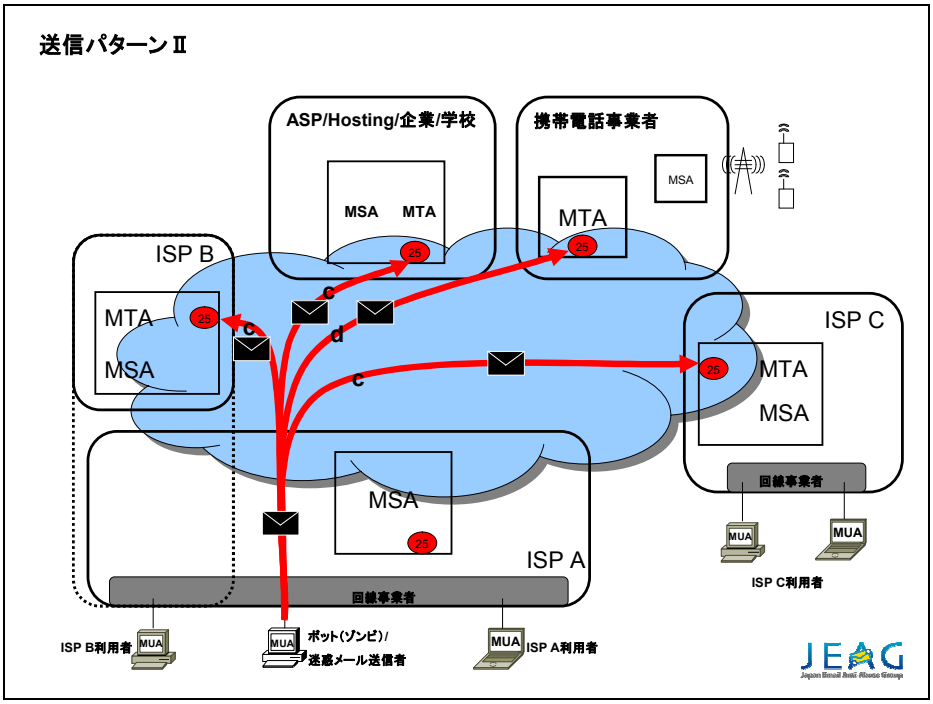


図 3-5

パターンⅡのメール送信経路について、図 3-5 に示す。

(1) 迷惑メール送信者は動的 IP を取得する

(2) その動的 IP から、標的のドメインの MTA へ直接迷惑メールを送信する

この送信方法に対する有効な対策が「OP25B」である。

# 4. Outbound Port 25 Blocking

## 4. 1. 前提条件

本 Recommendation では、OP25B を「Source IP Address が動的 IP、かつ、Destination Port が 25 である TCP トラフィックを遮断すること」と定義する。

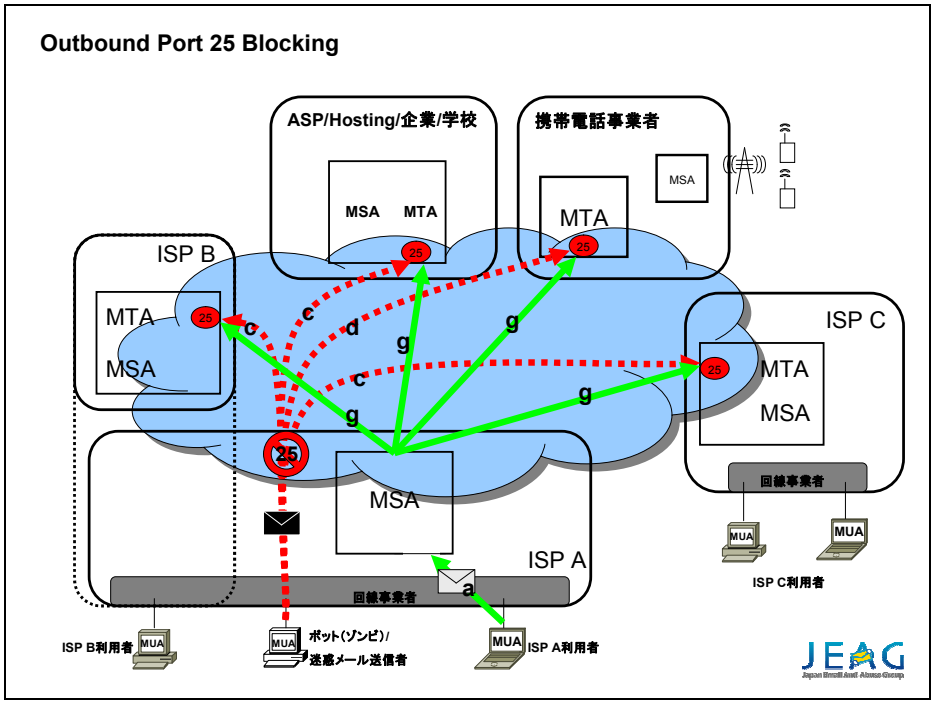


図 4-1

図 4-1 は、OP25B を模式的に示している。ISP A が OP25B を実施すると、メール送信者は、ISP A の指定する MSA を経由してメールの送信はできる（a→g）が、それ以外の経路（c、d）でメールの送信はできない。利用者のメール送信は MSA への投稿によって確保されているので、利用者は困らない。よって、パターンⅡの送信方法を用いた迷惑メールを根絶することが可能である。

d の線のみに対する OP25B を「携帯電話宛限定の OP25B」と表現する。また、c および d の線を対象とした OP25B を「完全な OP25B」と表現する。

OP25B は、バックボーンのいずれかのネットワーク機器に ACL などを用いたフィルタリングを設定することで実現される。本 Recommendation では、このネットワーク機器の場所を Blocking Point と呼ぶ。動的 IP からの迷惑メール送信を制限するフィルタリングポリシーの一例として以下を提示する。

1. 動的 IP からは決められた MSA(25) との通信のみを許可する。
2. これ以外の MSA(25) との通信は全て制限する
3. 固定 IPからの通信は特に規制しない

これは単純な例のひとつであり、このルールを適用する装置やサービスポリシーにより許可したり制限したりする対象は変わってくる。

ACL の行数は、

（ACL の行数）＝（動的 IP のアドレスブロックの数）×（MSA のアドレスブロック数 ＋1）

で、算出される。例えば、「動的 IP のアドレスブロックの数」が 100、「MSA のアドレスブロックの数」が 10 であるとしても 1,100 行になる。ACL の行数は、ネットワーク機器の性能やフィルタリング条件の管理などコストに直接影響する。この例では、1,100 行の ACL によるフィルタリングを実施できる性能のネットワーク機器が必要となる。モデル A の ISP では、傘下のモデル B の ISP の数により、Permit の設定が必要な「MSA のアドレスブロックの数」が多くなり、ACL の行数が問題となる場合がある。

これに対して、モデル C の ISP は自社の MSA への投稿だけを考えればよいので、ACL の行数は少なくなる。

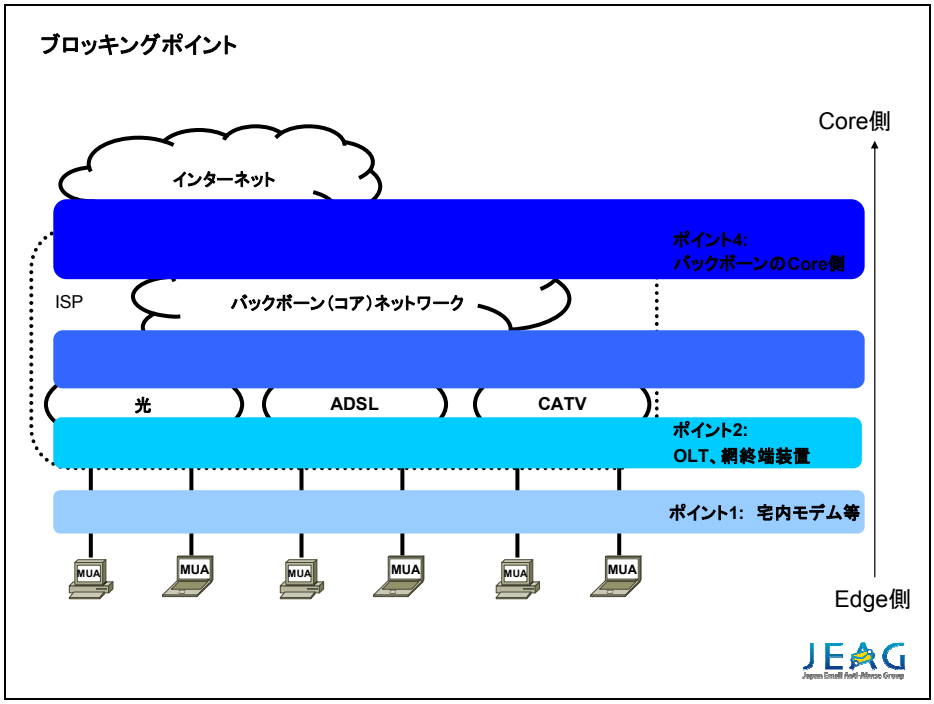


図 4-2

図 4-2は、バックボーンネットワークの構成による Blocking Point を模式的に表している。これを利用し、各ポイントの特徴を示す。なお、Blocking Point はネットワーク構成や各プロバイダの事情によって異なる。

Blocking Point は、Core 側に近づくほど、ネットワーク機器に性能が要求されるが、設定対象機器の数は少なくなる。一方、Edge 側に近づくほど、ネットワーク機器の性能は必要とされなくなるが、設定対象機器の数が増え、かつ広範囲になる。

ポイント 1 は、利用者側に最も近い場所に設置されている「モデム」を Blocking Point とする方法である。「Access Control List （以下、ACL）が少なくて済む」、「バックボーンに不要なトラフィックが流れない」、「バックボーンに手を加える必要がない」、などのメリットがある。この方法が利用できるのは、センターからモデムを制御できる事業者である。

ポイント 2 は、キャリア網の終端装置を Blocking Point とする方法である。設定は、Radius

の Attribute を利用することになる。日本と制度の違うアメリカでは主流である。

ポイント 3 は、バックボーンの Edge 側を Blocking Point とする方法である。この方法を利用する ISP が最も多いと予想される。このようなISPは二次 ISP を抱えていることが多い。

ポイント 4 は、Core に近い場所を Blocking Point とする方法である。 ACL が集中することになるため、大量の ACL を設定した場合の負荷に耐えられる機器が必要となる。

## 4. 2. 完全な OP25B を実施するにあたっての問題

3.1 章で述べたように、現在、メールの投稿には 25 番ポートが利用されている。このため完全な OP25B を実施すると、以下の例のように、利用者がメールを投稿できなくなる場合がある。

(1) 利用者が接続している ISP とは別の ISP の提供する MSA を利用する場合(利用者が複数の ISP を契約していることが前提)
(2) 利用者がホスティングや ASP サービスの MSA を利用している場合
(3) 利用者が契約している ISP が、モデル B の ISP である場合[5]

(1) ～ (3) ではいずれも、投稿に利用される MSA が、利用者が接続している ISP の管理するネットワークの外に存在している。このような MSA への投稿を、本 Recommendation では「第三者サーバへの投稿」と表現する。したがって、「第三者サーバへの投稿ができなくなる」ことが、完全な OP25B を実施するにあたっての課題である。図 4-3 はこれらの例を模式的に表している。

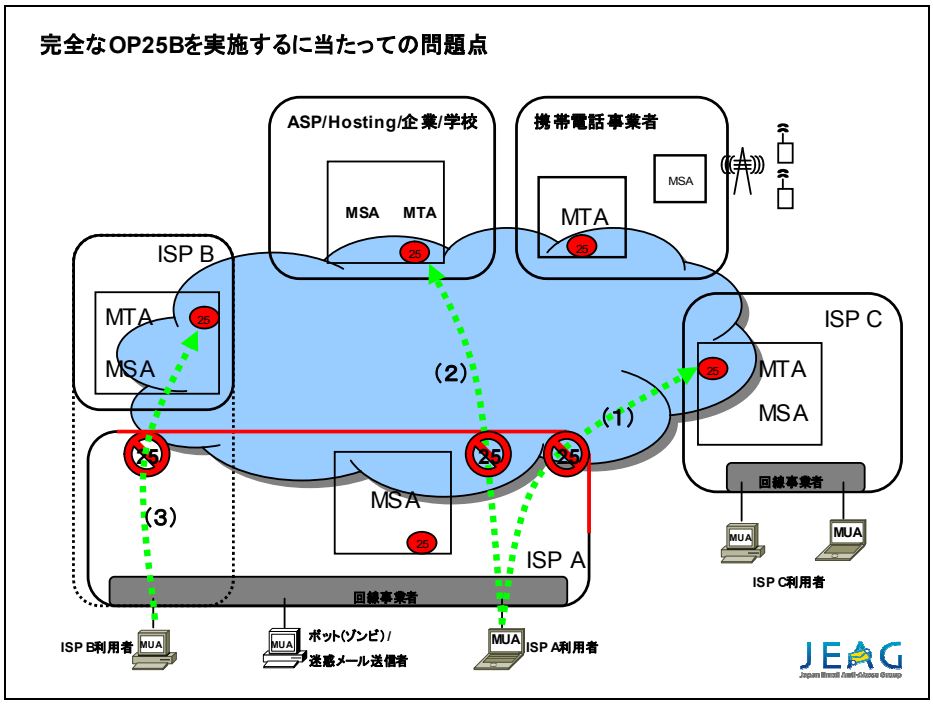


図 4-3

ISP A はモデル A の ISP, ISP B はモデル B の ISP である。前述したように、ISP B の利用者がメールを送信する際には ISP A のバックボーンネットワークを介して、ISP B の MSA へ接続する。もし、ISP A が回避手段を提供せずに OP25B を実施した場合、(3) の経路は遮断されるので、ISP B のユーザは MSA への投稿ができなくなる。

[5] *本 Recommendation では (3) を「第三者サーバへの投稿」に含めて扱うので注意すること。*

## 4. 3. 解決方法

4.2 章で提示した課題を解決するためには、メールの投稿に 25 番ポート以外のポートを利用する方法がある。具体的には、Submission Port(587 番ポート）をメールの投稿に用いる[6]。この方法は、RFC2476 でインターネット標準として提示されている。これに準拠し、メールの投稿には 587 番ポートを利用すればよい[7]。

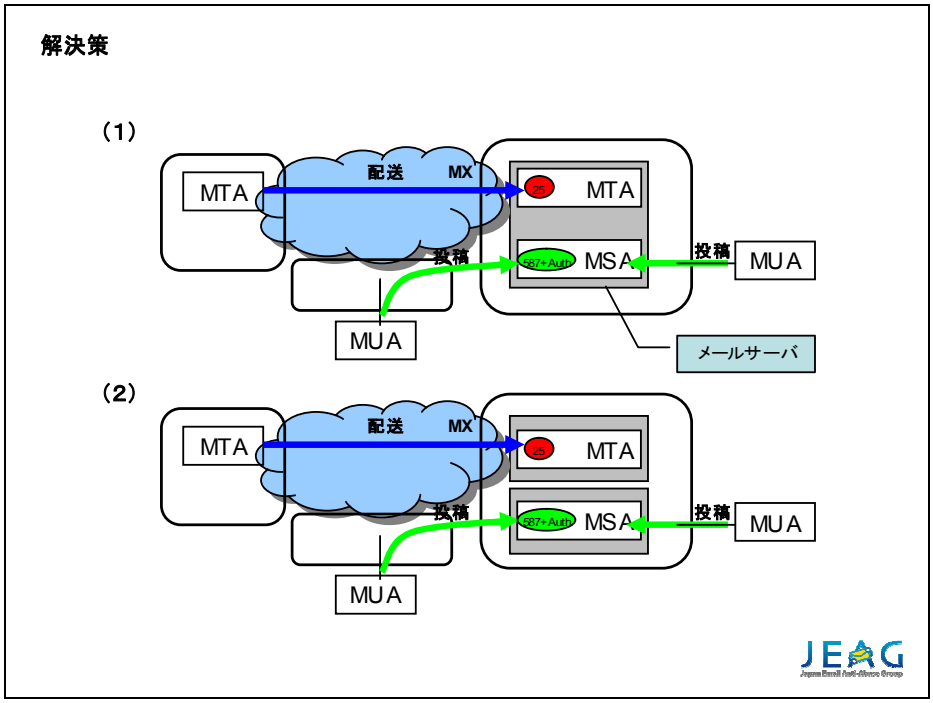


図 4-4

図 4-4 は、本 Recommendation にて推奨する SMTP サーバの代表的な構成を模式的に表している。

(1) 25 番ポートを利用した MTA と 587 番ポートを利用した MSA を同じサーバ上で動作させている構成
(2) 25 番ポートを利用した MTA と 587 番ポートを利用した MSA を別々のサーバで動作させている構成

いずれの場合も、MTA は配送に利用され、MSA は投稿に利用されている。完全な OP25B を実施した場合でも、25 番ポート以外は遮断対象にならない。したがって、587 番ポートへの投稿を可能にすることで、第三者サーバへの投稿を救済することができる。また、587 番ポートには SMTP 認証（以後、SMTP AUTH）を実装しなければならないため、図中では「587+Auth」と表現している。詳細については後述する。

---

*6 25 番以外のポートを利用する方法として、他に SMTP over SSL(465) がある。*

*7 配送にはこれまで通り 25 番ポートを利用する。*

## 5. 実現方法

以下、順を追って OP25B の実現方法を解説する。

### 5. 1. 携帯電話宛限定の OP25B

**Recommend 1. 携帯電話宛限定の OP25B**

- 完全な OP25B の実現に時間のかかる ISP は、携帯電話宛限定の OP25B を実施するべきである。

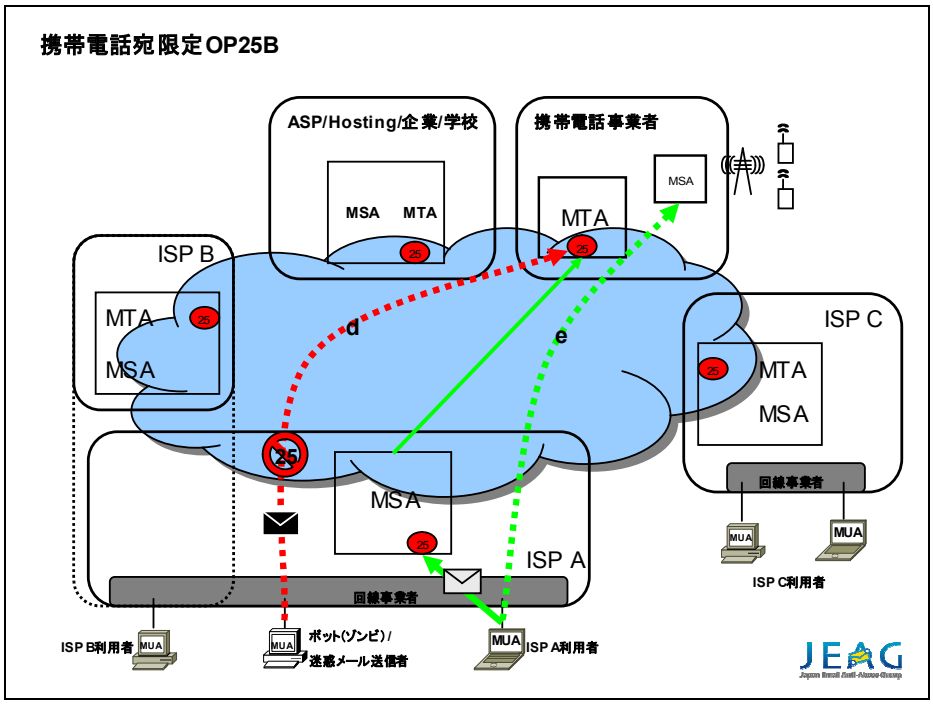


図 5-1

図 5-1 は、図 4-2 から携帯事業者宛のメールの配送経路を抜き出した図である。 d の線は「ISP の動的 IP 発、携帯電話宛」の迷惑メールの送信経路である。

e の線は「ISP 利用者による携帯電話事業者の MSA への第三者サーバへの投稿」を表している。しかし、携帯電話事業者の MSA は携帯電話機以外からの投稿を認めていないため、実際には e の線は存在しない。さらに、携帯電話事業者の MTA はインターネットからの投稿を受け付けていない[8]。したがって、e の線は遮断対象にしても問題にならず[9]ここを遮断することで動的 IP から携帯電話宛の迷惑メール（d の線）を根絶できる。

現在でも、この経路を利用した迷惑メールが多く、完全な OP25B の実施に時間を要する ISP は、この対策を実施するべきである。携帯電話宛限定の OP25B を実施する場合の情報は Wireless SWG からの「携帯電話宛迷惑メール対策に関する提言書」に記載があるので参照のこと。

---

[8] *当然、MTA からの配送は許容されている。*

[9] *動的 IP に MTA を立ち上げている場合などは、配送が問題になる場合がある。*

## 5. 2. Submission Port(587 番ポート) の利用者への提供

### Recommend 2. Submission Port(587 番ポート) の利用者への提供

- メールシステム管理者は Submission Port (587 番ポート)に対応した MSA[10] を提供しなければならない。
- MSA には SMTP AUTH を実装しなければならない[11] (SMTP AUTH を実装していない MSA(587)[12] は提供してはならない)
  - ローカルドメインへの配送であっても、SMTP AUTH を実施するのが望ましい。
  - POP ID/Password は AUTH ID/Password と同一にするのが望ましい。
- MSA では POP before SMTP を提供してはならない。

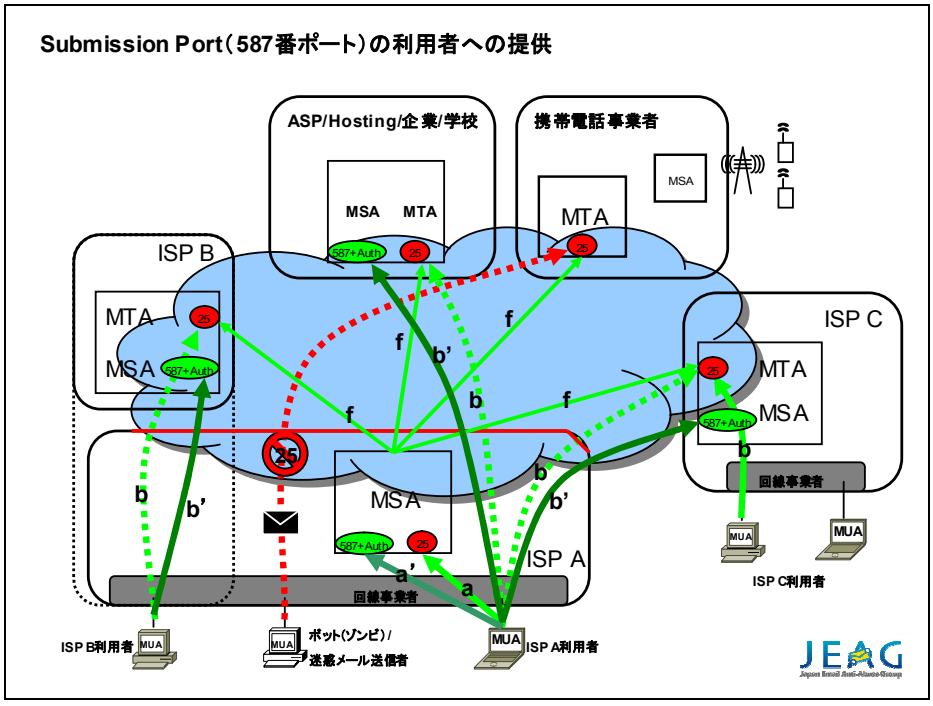


図 5-2

図 5-2 の場合、ISP A が OP25B を実施すると、 b の線は遮断対象になる。すると利用者がそれまで利用できていた機能が損なわれてしまうため、ISP は第三者サーバへの投稿のための代替手段、すなわち Submission Port(587 番ポート) を提供しなければならない ( b' の線)。利用者が MUA の設定を変更すれば、第三者サーバへの投稿ができるようにすることが、この Recommend 2 の目的である。したがって第三者サーバとして利用されるMSAの管理者は、速やかに Submission Port(587 番ポート) を提供しなくてはならない。

---

*10 MSA は物理的に新たなサーバが必要なわけではない。また、この章で扱う MSA は第三者サーバとして利用される MSA をさす。*

*11 ユーザ認証が担保されれば SMTP AUTH でなくても構わない*

*12 本 Recommendation では、587 番ポートを対応している MSA を MSA(587) と表記する。*

MSA の管理者は、Submission Port を提供する場合、SMTP AUTH を実装しなければならない。この場合、MSA を経由した、ローカルドメイン宛の迷惑メールを防ぐために、ローカルドメインへの配送であっても、SMTP AUTH を実施することが望ましい。また、「AUTH ID/Password」は「POP ID/Password」と同一にすることが望ましい。これは、一部 MUA では、AUTH ID/Password が POP ID/Password と同一の設定しか出来ない場合があるためである。

もし、投稿時に SMTP AUTH が実施されなかったら、迷惑メール送信者は、投稿ポートを 25 番から 587 番に移行し、迷惑メール送信手段のパターンⅠを用いて迷惑メールを送信し続けるであろう。SMTP AUTHを実装しておけば、同一IDからの送信数を制限することでこの対策が可能である。したがって、SMTP AUTHを実装していないMSA(587)は提供してはならない。

(参考情報)POP before SMTP の扱い

ホスティング事業者や ASP では投稿時に「認証」が必要である。この場合、POP before SMTP が利用されることが多い。しかし、POP before SMTP には、仕組み上の欠点が指摘されている。そのため、MSA の Submission Port(587番ポート）では、SMTP AUTH の代用として POP before SMTP を提供してはならない。これは、POP before SMTP[13] で用いられる認証が「ユーザ認証」ではなく「IP Address 認証」であることに起因している。

欠点の例

インターネットへ接続している LAN の場合、ルータやファイアウォールなどのゲートウェイにおいて、アドレス変換（NAT など）を利用して、複数の PC が同一の Global IP Address を利用する。さらに、LAN 内の複数の PC が、インターネット上の同一の MSA を利用しているとする。このような状況下で、LAN 内の PC がボットに感染したとする。ボットに感染していない正常な PC が POP をした場合、ボットは MSA を利用して、メールの送信が可能になってしまう。LAN 内からの POP が定期的に実施されていれば、認証は実施されていないのと変わらない。

*13 一般的な POP before SMTP は、POP アクセスが正常に完了した IP アドレスのからの、SMTP アクセスを一定時間許可するという動的な IP フィルタである。*

## 5. 3. メールの投稿の Submission Port (587) への完全移行

### Recommend 3. MSA(587+Auth) と MTA の分離

- メールの投稿には必ず MSA(587+Auth) を利用しなければならない
  - MSA(25) は廃止しなくてはならない[14]
  - MTA への投稿を廃止しなければならない

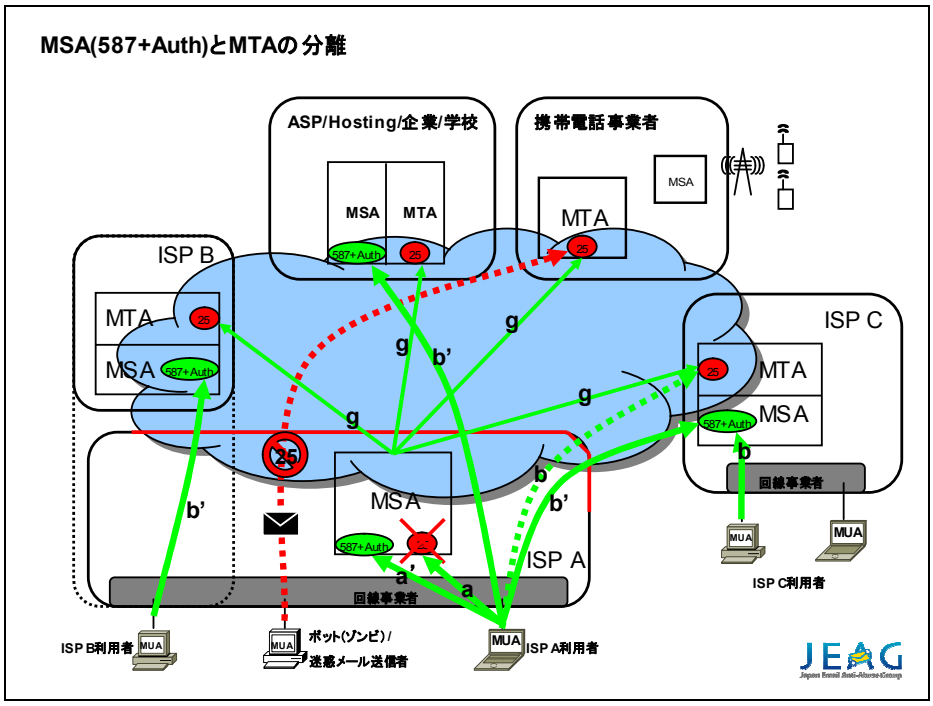


図 5-3

3.4 章で説明したように、パターンⅠの迷惑メール対策には SMTP AUTH を利用した送信数制限が有効である。このためには、すべてのメール投稿に SMTP AUTH が実施されていることが必要条件となる[15]。したがって、将来的な利用者の分かり易さを考慮して、モデル C の ISP であっても、これから SMTP AUTH を提供するのであれば、同時に 25 番ポートを 587 番ポートへ移行するべきである。したがって、すべてのメールの投稿には必ず Submission Port(587) を利用し、なおかつ、すべてのメールの投稿時には SMTP AUTH を実施[16]しなければならない。図 5-3 は、Recommend 3 を模式的に表しており、a の線は a' へ移行し、b の線は b' へ移行する。

Recommend 3 を実現するためには、利用者が MUA の設定変更を実施しなければならない。したがって、ISP は変更を促す必要がある。ここでは、そのひとつの方法を提案する。

---

*14 イントラネットにおけるメールの投稿は、25 番ポートを用いても構わない。しかし、可能であれば 587 番ポートを用いるのが望ましい*

*15 モデル C の ISP であり、なおかつ、既にすべての投稿に SMTP AUTH が実施されている場合は Recommend 3 は不要である。*

*16 すべてのメールの投稿には MSA(587+Auth) が利用される*

1. MTA/MSA(25) の他に MSA(587+Auth) を準備する。
2. 新規利用者へは MSA(587+Auth) を案内する[17]。
3. メールアドレスを変更するなど、MUA の設定をする必要のある利用者に MSA(587+Auth) を案内する。結果、MSA(25) の利用者は増加しなくなる。
4. 既存利用者に対して、MUA における SMTP サーバの設定を MSA(587+Auth) に変更するように促す[18]。

Recommend 3 は各々の事業者の事業形態やネットワーク構成により、移行完了のための、問題点や着目すべき点が異なる。以下の３つのモデルを想定し、事項以降、各々のモデルにおける問題点等を解説する

1. モデル C の ISP
2. モデル A およびモデル B の ISP
3. MSA に接続してくるネットワークが特定できない事業者（ASP 事業者など）

モデル A やモデル B、モデル C といった分類は、ISP 事業者を分類するモデルではなく、ISP 事業者が利用者に対して提供するサービスの形態を分類するモデルである。しかし、便宜上、事業者の分類に利用しているので注意すること（あるISP事業者が、モデル A に分類されるサービスと、モデル B に分類されるサービスをそれぞれ利用者に提供する場合がある)。

---

[17] *SMTP サーバとして、MSA(587+Auth) を設定するように、オンラインマニュアルや、利用者へ送付する冊子などの記載を変更して対応する。*

[18] *また、PC 以外でメールを送る機能を保持している機器については、ファームウェアの改良や新たなプログラムの提供などを通じ、利用者がメールの投稿に困らないようにしていく必要がある。*

### 5. 3. 1. モデル C の ISP

モデル C の ISP は、自らの利用者に対して MSA(25) あるいは MTA(25) への投稿を提供したままで、OP25B の実施が可能である。すなわち、この ISP にとって、Recommend 3 は OP25B を実施するにあたっての必要条件にはならない。

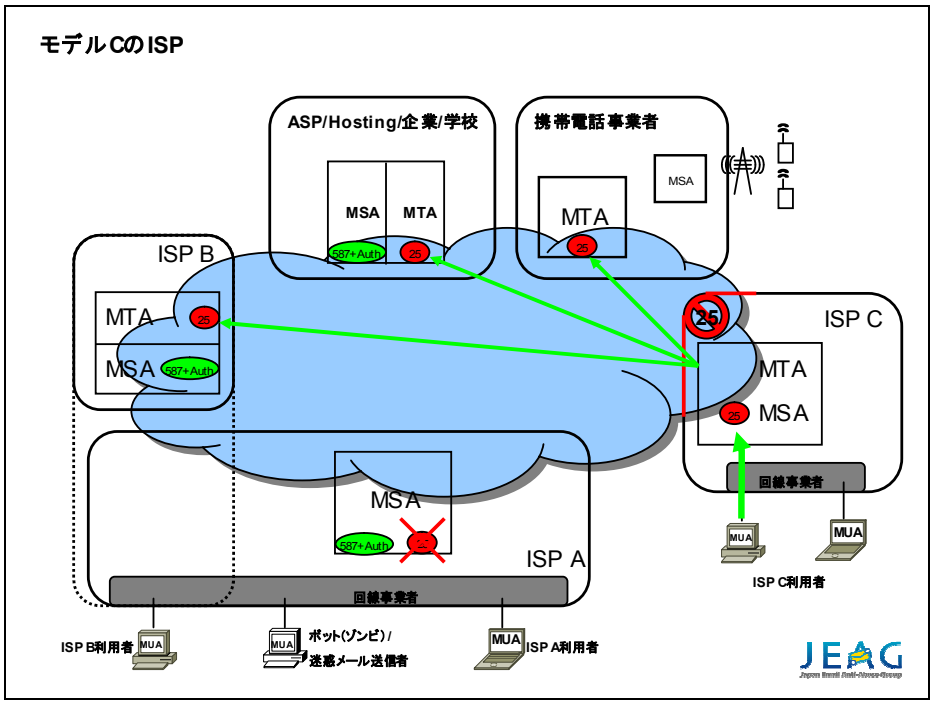


図 5-4

### 5. 3. 2. モデル B の ISP

**Recommend 3． 1．**

- モデル B の ISP は、モデル A の ISP と協調して OP25B を実施するべきである（協力の依頼には、積極的に応えるべきである）
- モデル A の ISP は、モデル B の ISP のすべての利用者が MSA(587+Auth) へ移行するまで、MSA(25)(あるいは MTA) への投稿経路を確保するべきである。

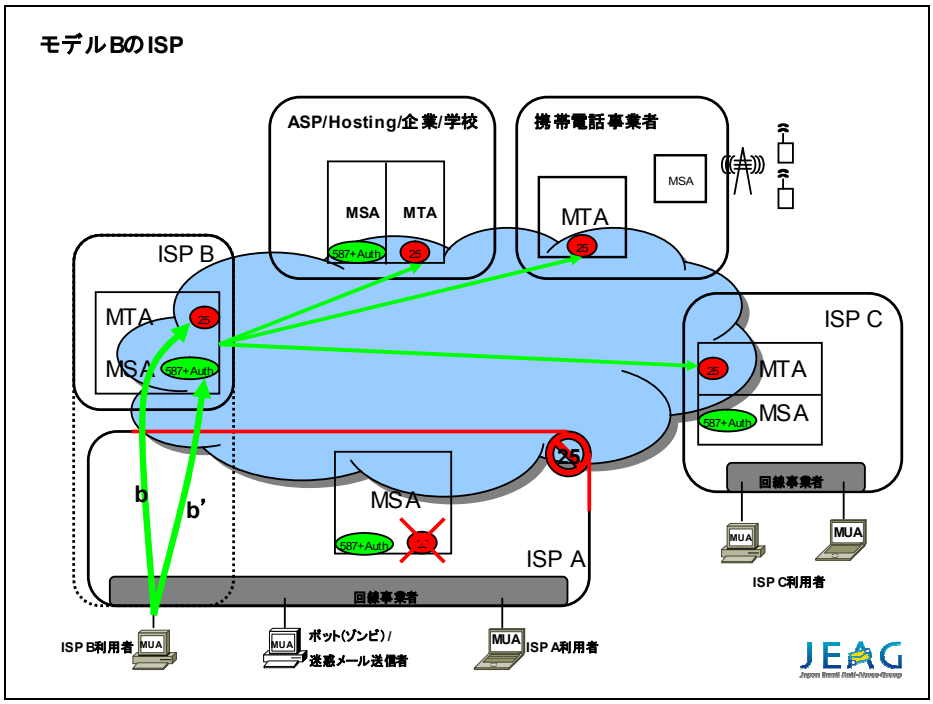


図 5-5

図 5-5 のように、ISP A [19] が OP25B を実施すると、ISP B の利用者は MSA(25)（あるいは MTA）への投稿（b の線）ができなくなる[20]。また、ISP B は自社でバックボーンネットワークや利用者へ払い出すIPアドレスを持たないため、OP25B の実施にあたっては ISP A に依存しなければならない。したがって、ISP A と ISP B はお互いに協調した上で OP25B を実施するべきである。

具体的には、ISP A と ISP B は、OP25B を実施する際、以下のいずれかの調整が必要となる。

1. ISP A が ISP B の MSA(25)（あるいは MTA）への投稿を許可する
2. ISP B が利用者の MUA における SMTP サーバの設定を MSA(587+Auth) へ「完全に」移行する

まず、1については、ISP A では ACL 問題[21]が発生してしまう。 2 については、完了を待って

---

*19 この章では読みやすくするために、図 5-5 にしたがって、モデル A の ISP を ISP A、モデル B の ISP を ISP B として記載する。*

*20 ISP B の利用者にとって、メールの送信は第三者サーバへの投稿にあたる（4.2 章参照）*

*21 ACL 問題については、4.1 章にて説明する。ここでは ACL の行数が多くなりすぎて、設定することができないと解釈してほしい。*

いると、OP25B の実施が遅れてしまう。そこでモデル A の ISP とモデル B の ISP が協力して、OP25Bを実施するための、現実的な方法として、以下を提案する。

1. ISP B は MSA のアドレスブロックをできるだけ少なくまとめる
2. ISP A は ISP B の利用者の MSA(25)（あるいは MTA）への投稿を許可する
3. ISP A は OP25B を実施する
4. ISP B は利用者の MUA における SMTP サーバの設定を MSA(587+Auth）へ移行する
5. ISP B は ISP B の利用者の MSA(25)（あるいは MTA）への投稿許可を解除する。

この移行に要する期間は短ければ短いほど望ましい。

### 5. 3. 3. MSA に接続してくるネットワークが特定できない事業者

**Recommend 3. 2. MSA に接続してくるネットワークが特定できない事業者**

- MSA(587+Auth) へ直ちに移行しなくてはならない

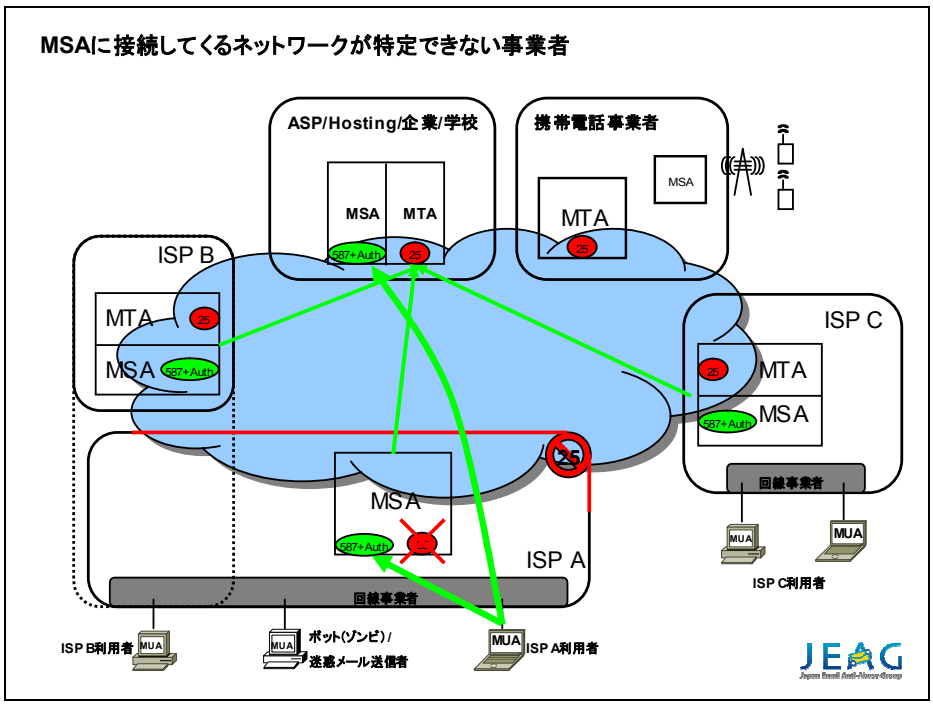


**図 5-6**

ASP サービスやホスティングサービスを提供する事業者は、利用者がどの ISP から MSA に接続してくるかを特定できない。インターネットからの投稿を許可している企業や学校などでも事情は同じである。このような事業者は、ISP が OP25B を実施した瞬間から、MSA(25)（もしくは MTA）は投稿を受けられなくなるため、早急に MSA(587+Auth) を準備し、利用者に MUA の設定変更を促す必要がある。

ISP の OP25B が進んでいる現状を鑑みれば、Recommend 3 の早期実現が必要となる。しかしながら SMTP AUTH の提供に時間を要する等の理由から、やむを得ず Submission Port(587 番ポート）で、POP before SMTP を提供せざるを得ない場合があると予想される。このような場合でも、5.2 章で述べたように、POP before SMTP は推奨されないので、一時的な利用と明確に定めた上、できる限り早く SMTP AUTH へ移行するべきである。

## 5. 4. OP25B の 実施

### Recommend 4． OP25B の実施

- Source IP Address が動的 IP であり、かつ、Destination Port が 25 である TCP トラフィックを遮断しなければならない
- Asymmetric Routing Attack[22] 対策を実施するべきである
- 第三者サーバの代替 MSA を提供するべきである

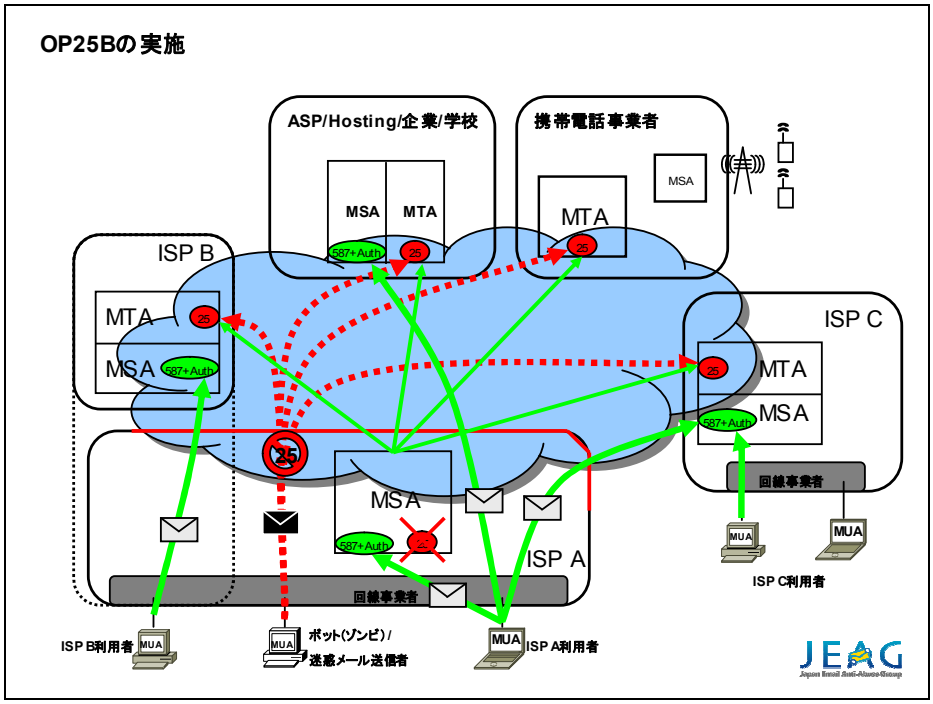


図 5-7

図 5-7 は OP25B について模式的に表した図である。図のように、MSA を経由しない MTA へのメール送信を遮断するため、迷惑メール送信者は標的へ直接メールを送ることができなくなる。メールの投稿に Submission Port(587 番ポート）を利用することにより、利用者は問題なくメールを投稿することができる。OP25B の実施の方法については、4.1 章で述べている通りである。この章では、OP25B を実施する際の細かな注意事項を説明する。

[22] *Asymmetric Routing Attack については、実際に ACL を書く方が理解していればよい。*

### 5. 4. 1. 関連事項

**Recommend 4. 1. 関連事項**

- 通信する必要のある MSA が LAN 外に存在する場合、ファイアフォールやルータからインターネットへの TCP587 の通信を Permit（許可）しなくてはならない
- 動的 IP を利用した MTA は、固定 IP を取得するべきである

本章では、OP25B に付随して発生する「第三者サーバへの投稿」以外の問題点について説明する。

ISP が OP25B を実施した場合に、ファイアウォールやルータなどのネットワーク機器のフィルタリングの設定が問題になることがある。例えば、企業や教育機関などが、「動的 IP のサービスを利用していて、なおかつ、MSA を ASP やホスティングサービスに依存している」場合には、MUA はメールを投稿する際、ファイアウォールやルータを介して MSA と通信する。この時、Submission Port(587番ポート）がフィルタされていると、メールを投稿できない。したがって、このような環境の場合、企業や教育機関のシステム管理者やネットワーク管理者は、Submission Port(587番ポート）への通信を Permit に設定しなければならない。これはプロキシにおいても同様であり、Submission Port(587番ポート）への通信を中継しなければならない。

動的 IP 上に「MX レコードをひいて、直接相手先 MTA へメールを配送する」SMTPサーバが存在すると、この「配送」は OP25B により遮断の対象となる。例えば、以下の場合などが該当する。

1. ダイナミック DNS などを利用し、動的 IP を用いて MTA を立ち上げている場合
2. 送信専用 SMTP サーバに、動的 IP を用いる場合

このような場合は、利用者に 遮断対象にならない固定 IP を取得してもらうのが望ましい。

(参考情報) 移行期の対策（Inbound Port 25 Blocking)

- ISP は動的 IP の逆引きを公開するべきである
  - 逆引きは一種類の正規表現で記述できることが望ましい

移行期の対策についての上記参考情報は、JEAG 内において、議論が不十分であるため、今回は参考情報として紹介する。

各社、あるいはサービスによって、OP25B は実施時期が異なる。ここでは、OP25B が十分に普及するまでの時期を「移行期」と呼称する。我々は移行期の対策として、他ISP事業者の提供する動的 IP から MTA の 25 番ポートへの接続をメール受信側ISPがinboundでフィルタするという方法も検討している。動的IPを提供するISP が「受信（25番ポートへの接続）を拒否してよいアドレスを宣言する」という方法でこれを実現できる。このアドレスの宣言にDNS逆引きレコードを利用する。動的 IP の逆引きレコードに、一定のルールを与えることで受信側において動的 IP の判別が可能となる。

動的 IP の逆引きレコードの記述ルールとして、例えば、「動的 IP の逆引きレコードは単純な正規表現を用いて動的IPが判別できるように記述する」「動的 IP の逆引きレコードには、各社で共通の特定文字列を挿入する」などがあがっている。また、「DNS以外での公開方法をどうするか」という課題も指摘されている。

移行期には、迷惑メール送信者は OP25B を実施していない ISP へ移動すると予想される。この ISP の提供する動的 IP からの 25 番への接続を受信側でフィルタすることで、OP25B と同様の効果が得られる。迷惑メール送信者が特定の ISP に偏った場合、この方法は効果的であると考える。

(参考情報) 自社動的 IP 発　自ドメイン宛の迷惑メール対策

- 自社の動的 IP[23] から、自ドメインの MTA の 25 番ポートへの通信は遮断してしまうのが望ましい

OP25B の導入が進んだ場合、迷惑メール送信者は標的とする受信者（ドメイン）のいる ISP と契約して、そのドメインの MTA へメールを送信することが考えられる。この対策として、ISP は Source IP Address が自社のネットワークの動的 IP で Destination が MTA の 25 番ポートである通信を 遮断 することが望ましい[24]。これは、MSA と MTA でポート番号かもしくは IP Address の少なくともどちらか一方の分離が完了していれば実現可能である。設定しなくても、困るのは自社だけなので、参考情報として記載する

*[23] モデル B の ISP はモデル A の ISP が払い出す動的 IP 群*

*[24] これはネットワーク機器でなくて、MTA で実施することも可能である。*

## 5. 5. 送信通数制限の実施

**Recommend 5.　送信通数制限の実施**

- MSA においては、「SMTP AUTH」を利用した送信数制限を実施するべきである。
- 通数は「RCPT TO」でカウントするべきである。

Recommend 3 と Recommend 4 が完了すれば、動的 IP を Source とする場合、メール送信者は投稿に MSA(587+Auth) を利用するしかない。これは利用者にとって問題とならない。

迷惑メール送信者が MSA(587+Auth) を利用して迷惑メールの送信を試みると、これは 3.2 章で説明した迷惑メール送信手段のパターン I に類似する。MSA(587+Auth) では、SMTP AUTH により、「誰が何通送ったか」の正確なカウントが可能である。これを利用して、迷惑メールの大量送信の制限が可能であり、「同一 ID からは単位時間で何通まで送信を認める」という送信通数制限を実施するべきである。ただし、迷惑メール送信者にはダメージを与えるが、利用者は困らないように、制限値をチューニングする必要がある。

また、送信通数は、「RCPT TO」でカウントするべきである。RFC2821 によれば、RCPT TO は 100 個まで受け付けないといけないと規定されている。仮に MAIL FROM を 100 個までと制限すると、「MAIL FROM」×「RCPT TO」、つまり 100×100＝10,000 通の迷惑メールの送信が可能になってしまうからである。

## 5. 6. スケジュール

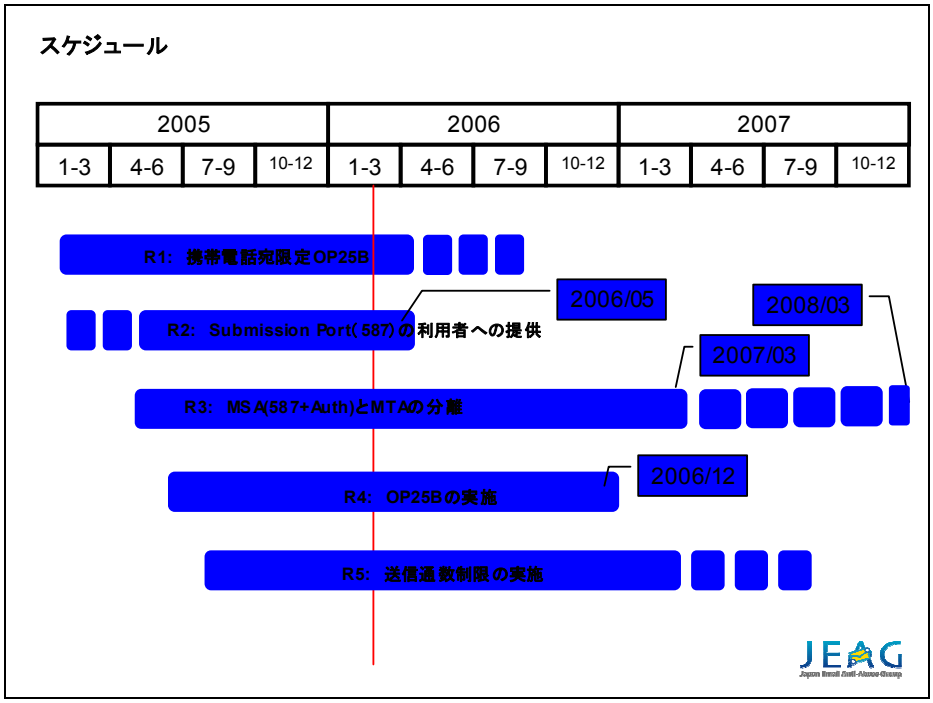


図 5-8

本 Recommendation では、事業者間で協力して進める必要のある Recommend について、完了目標日を設定する。事業者間で協力が必要なのは、以下の３項目である。

- 【Recommend 2】MSA(587+Auth) の利用者への提供
- 【Recommend 3】メールの投稿の Submission Port(587) への完全移行
- 【Recommend 4】OP25B の完全実施

**Recommend 6. Recommend 2 の実施時期に関して**

- 2006 年 5 月末までに、MSA(587+Auth) の提供を開始するべきである

OP25B が既に普及し始めている状況を鑑みると、Recommend 2 に関しては利用者の利便性の観点から、早急に実施するべきである。本機能は、利用者へのサービス影響はない事から、導入のハードルも低いと考える。

**Recommend 7. Recommend 3 の実施時期に関して**

- ISP は、2007 年 3 月 までに完了するべきであり、2008 年 3 月までに完了しなければならない
- ASP やホスティング事業者は、OP25B の完了までに提供することを推奨する

Recommendation 3については、各々の事業者により、実施時期が異なる。
ISP は移行に時間をかけることが可能であるが、OP25B SWGとしては、移行を 1 年後の 2007 年 3 月までに完了するべき、 2 年後の 2008 年 3 月までに完了しなければならないと目標を設定する。

移行期間を確保することができないASP やホスティング事業者は、早急に対応しなければならない。既に OP25B を実施した事業者が存在するので、この対応は始まっていると予想される。OP25B の完了がそのまま対応完了の目標日になる。

**Recommend ８． Recommend 4 の実施時期に関して**

- OP25B を 2006 年 12 月 までに実施するべきである

迷惑メール送信者は、OP25B が実施されていない ISP へ移動する。したがって、OP25B の実施が遅れた ISP へ、迷惑メール送信者が流入することを意味する。どの ISP も自社で迷惑メール送信者を抱えるのは本意ではない。携帯電話宛限定の OP25B が、2005 年夏から秋にかけて一気に広まったことや、完全な OP25B の普及が開始し始めている状況から、完全な OP25B は加速度的に普及すると考える。このような背景を考慮し、完了目標日を 2006 年 12 月に設定する。

最後に、ここで提言した完了目標日はあくまでも目安であり、必ず実施が必要なわけではない。しかし、実施が遅れた ISP は、迷惑メール送信者の温床になる可能性が高い。逆に、すでに実施している ISP がいる現在、早期に実施が可能であれば、完了目標日まで待つ必要はない。
すなわち、Recommend の実施は早ければ早いほど望ましい。

JEAG Recommendation (Outbound Port 25 Blocking Sub Working Group)

2006 年 2 月 23 日　　初版発行

**JEAG Recommendation 利用に際しての条件**



改変・翻案等に関する問合せは、以下にお願い致します。

連絡先：contact@jeag.jp