JEAG
Japan Email Anti-Abuse Group

Outbound Port25 Blocking

info@jeag.jp

Agenda　及び　講演者紹介

司会　若松　広司（Vodafone株式会社）

- **導入の是非**

  本間　輝彰（KDDI株式会社）

- **設定のノウハウ**

  赤桐　壮人（株式会社ぷららネットワークス）

- **運用経験の共有**

  池田　武（パナソニック ネットワークサービシズ株式会社）

JEAG紹介

JEAG Japan Email Anti-Abuse Group

- 迷惑メール対策を業界全体で取り組むべき問題と位置付け、技術的な見地を元にして対策を検討・実施するワーキンググループ
- 2005年3月15日設立
  - 国内ISP/ASP、携帯電話事業者、ソフトウェア、ハードウェアメーカー
  - 総務省、経済産業省、JPCERT/CC、(財)データ通信協会
- 活動内容
  - 統一的な方向性の模索・実施
    - 対策ポリシーの検討・作成を目指す
  - 対策技術導入についての共同作業実施
    - 対策技術の速やかな導入を目指す
  - 利用者・サービス提供者双方への啓蒙活動
    - 対策の重要性等につき理解を求める

JEAG OP25B SWG紹介

JEAG OP25B SWG

- 各ISPの動的IPに接続されたZombiePC(Bot)から発信される迷惑メールに対して有効な対抗手段であるOutboudPort25Blocking(OP25B)に関して、当該対策を広く普及させるために、以下の観点に着目して活動を行っている
  - 導入にあたっての問題点の整理
  - 問題点解決にあたっての対策案の検討
  - 対策案を実施するにあたってのアクションアイテムの整理
  - OP25B導入後の効果検証
- これらOP25B実施にあたっての各種情報に関しては、2006年の早い時期に、JEAG Recommendationとしてまとめ、展開する予定

導入の是非

本間輝彰（KDDI株式会社）

Outbound Port25 Blockingがなぜ必要か？

- FTTHやxDSL等の普及により、安価で短時間に大量メールを送信する事が可能になった。
- 現状の迷惑メールの大半は、ISPのメールサーバを経由せず、直接送信先のメールサーバに送られている為、送信元のISPでは、事実の特定が困難である。
- IPアドレスを（非常に短い周期で）頻繁に変えてくる為、受信側でも規制が困難である。

さらに．．．

- ウイルス等に感染し遠隔コントロール可能となったボット（ゾンビ）と呼ばれるPCから、メールを送信してくる方式も出てきた。
（誰もが、迷惑メール送信者になる可能性がある！）

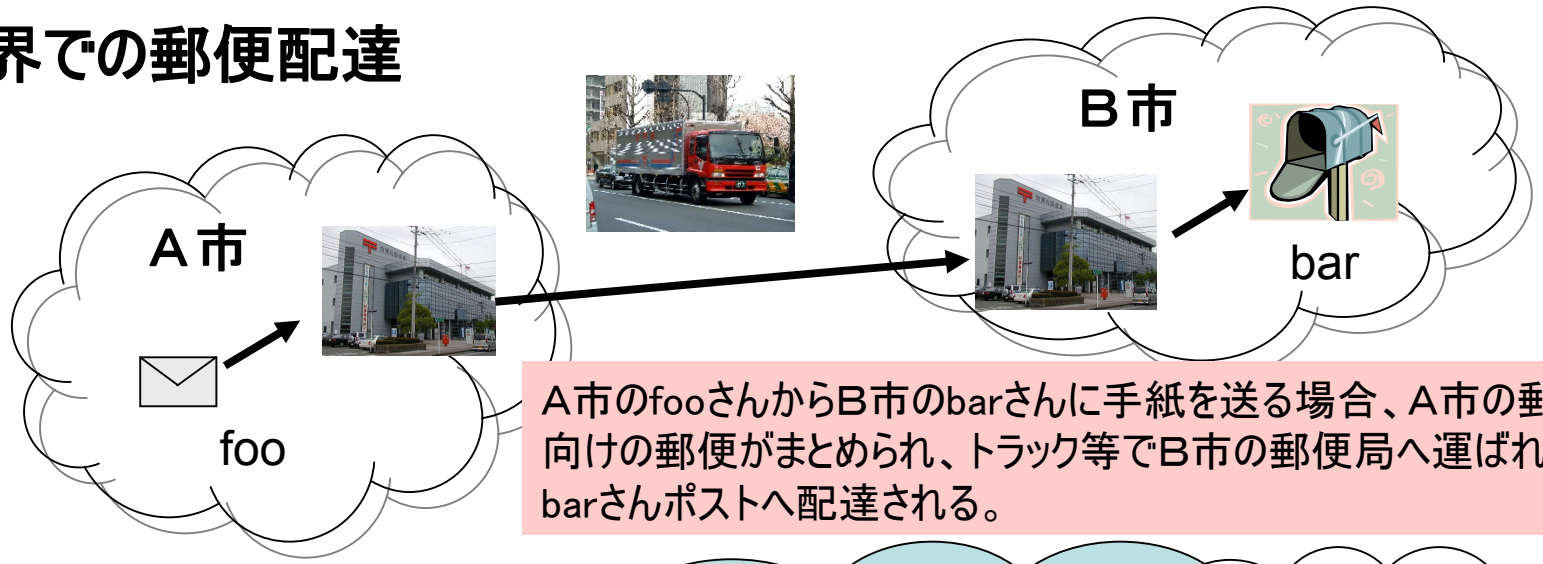
Outbound Port25 Blockingがなぜ必要か？

結果として、送信側だけではなく、**受信側でもリアルタイムな迷惑メールの検知が困難**となりつつある。
また、運用対処するにしても、かなりの量の迷惑メールを受信後の対応となり、その間は**ユーザが被害を受ける**事となる。

これらに対処するには、迷惑メールそのものを送信出来なくする仕組みが必要となり、その為には、
“***Outbound Port25 Blocking (OP25B)***”
が必要となる。

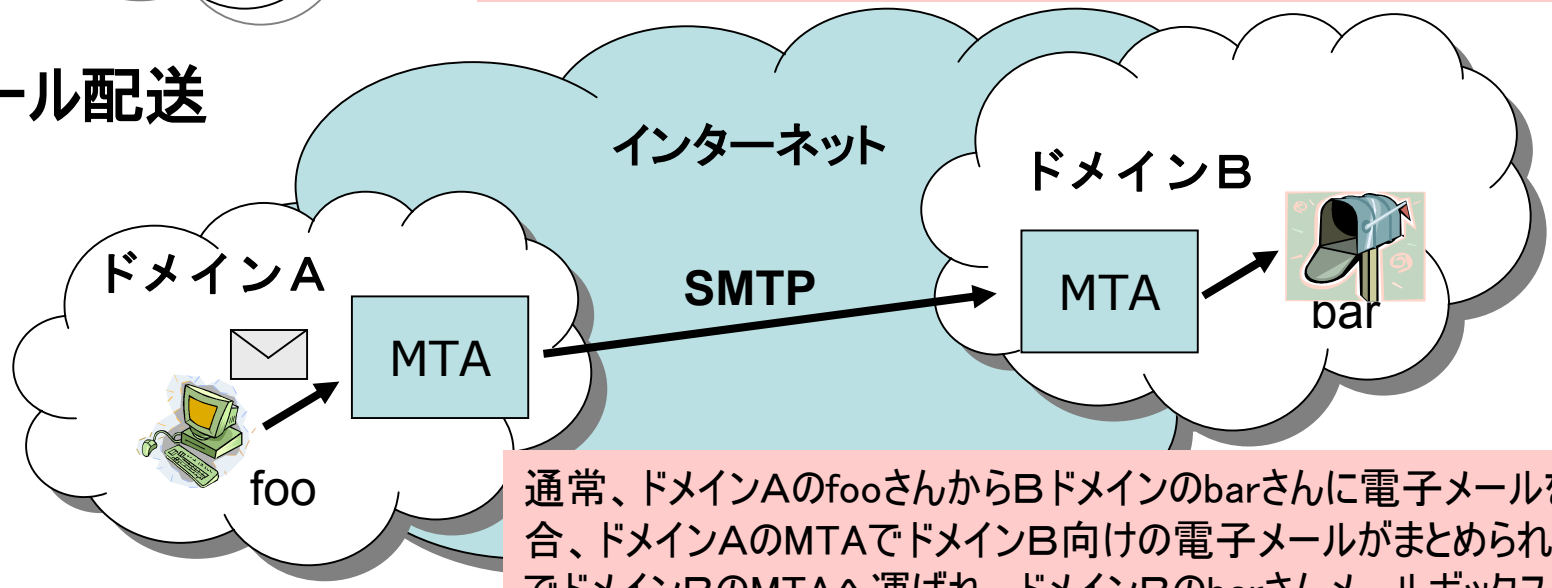
Outbound Port25 Blocking（OP25B）とは？

実世界での郵便配達



A市のfooさんからB市のbarさんに手紙を送る場合、A市の郵便局でB市向けの郵便がまとめられ、トラック等でB市の郵便局へ運ばれ、B市内のbarさんポストへ配達される。

電子メール配送

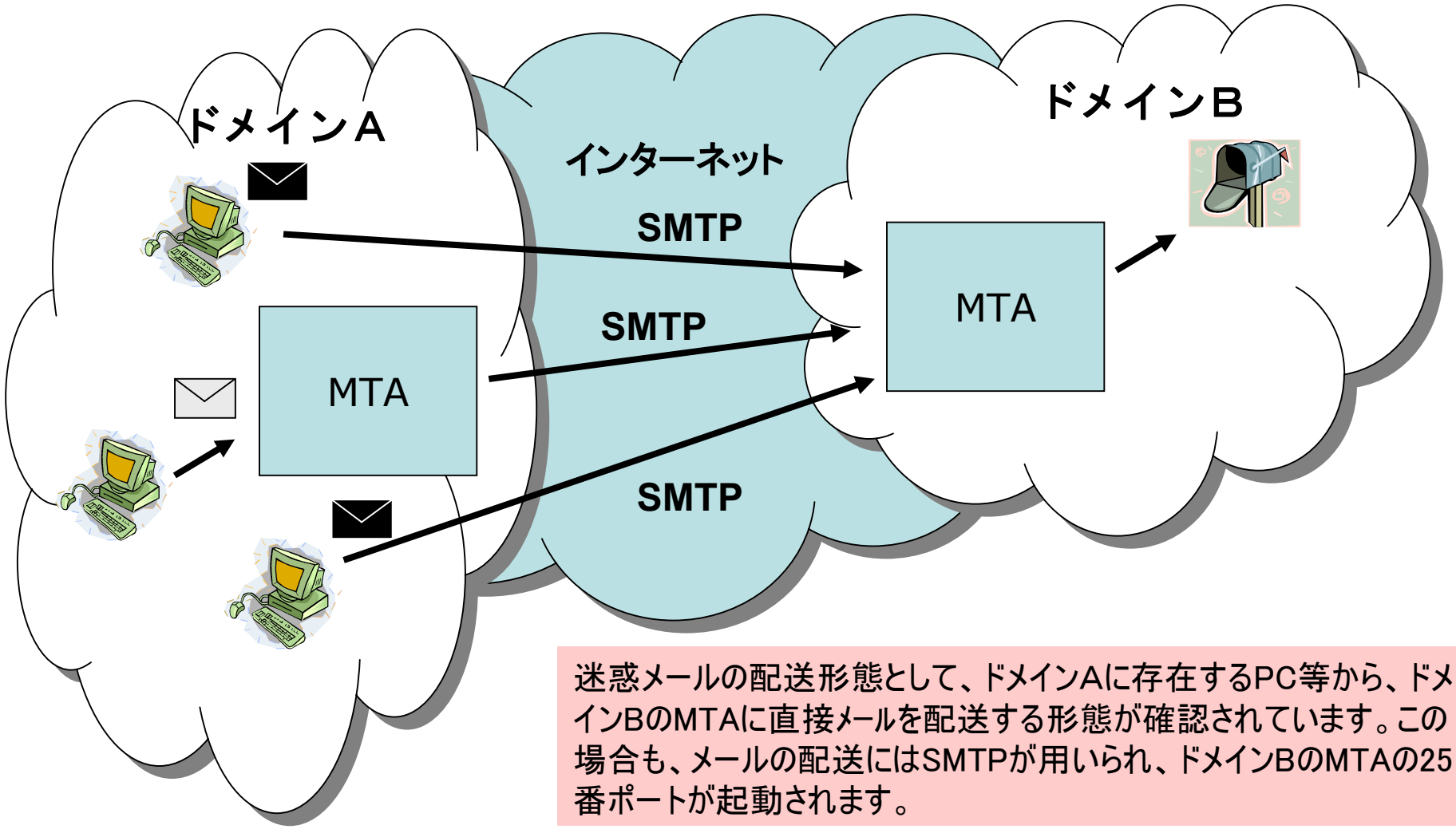


通常、ドメインAのfooさんからBドメインのbarさんに電子メールを送る場合、ドメインAのMTAでドメインB向けの電子メールがまとめられ、SMTPでドメインBのMTAへ運ばれ、ドメインBのbarさんメールボックスへ配信される

資料提供：JEAG

Outbound Port25 Blocking（OP25B）とは？

迷惑メールの配送形態

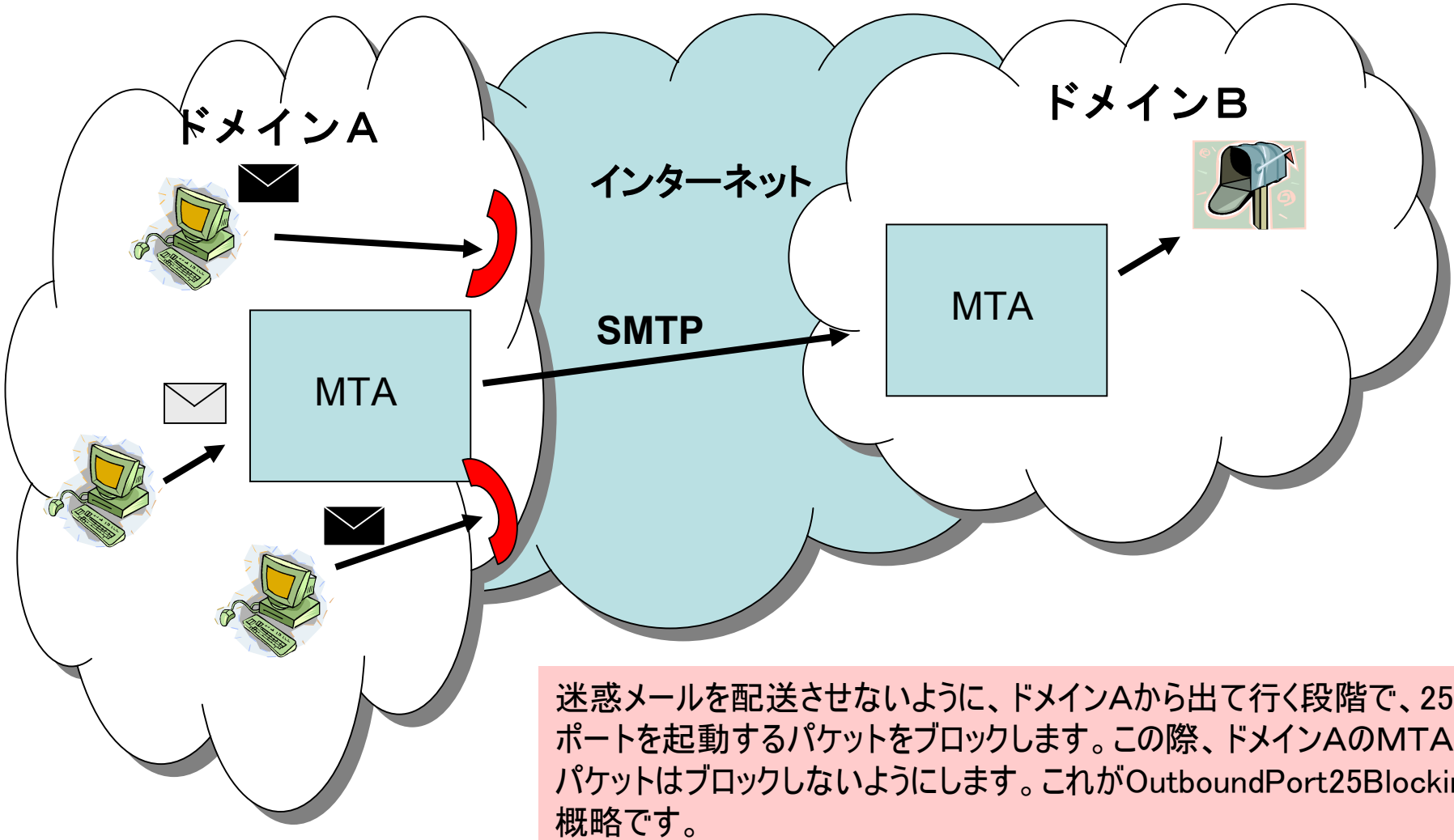


迷惑メールの配送形態として、ドメインAに存在するPC等から、ドメインBのMTAに直接メールを配送する形態が確認されています。この場合も、メールの配送にはSMTPが用いられ、ドメインBのMTAの25番ポートが起動されます。

資料提供：JEAG

Outbound Port25 Blocking（OP25B）とは？

Outbound Port25 Blocking



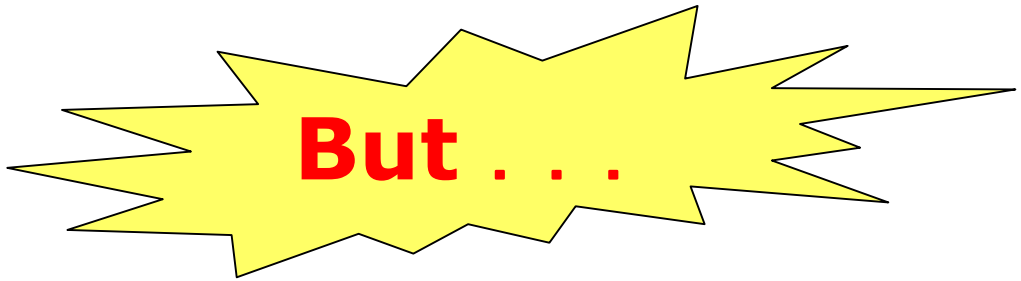
迷惑メールを配送させないように、ドメインAから出て行く段階で、25番ポートを起動するパケットをブロックします。この際、ドメインAのMTAからのパケットはブロックしないようにします。これがOutboundPort25Blockingの概略です。

資料提供：JEAG

OP25Bの問題点

- 他ISPで契約しているアドレスを該当のISPのメールサーバ経由でメールが送信出来なくなる。
- ダイナミックDNSを使って、自前でメールサーバを構築している場合、メールの送信が不可となる。

OP25Bを実施した場合、一部ユーザに対してサービスのデグレが発生する事は否めない。



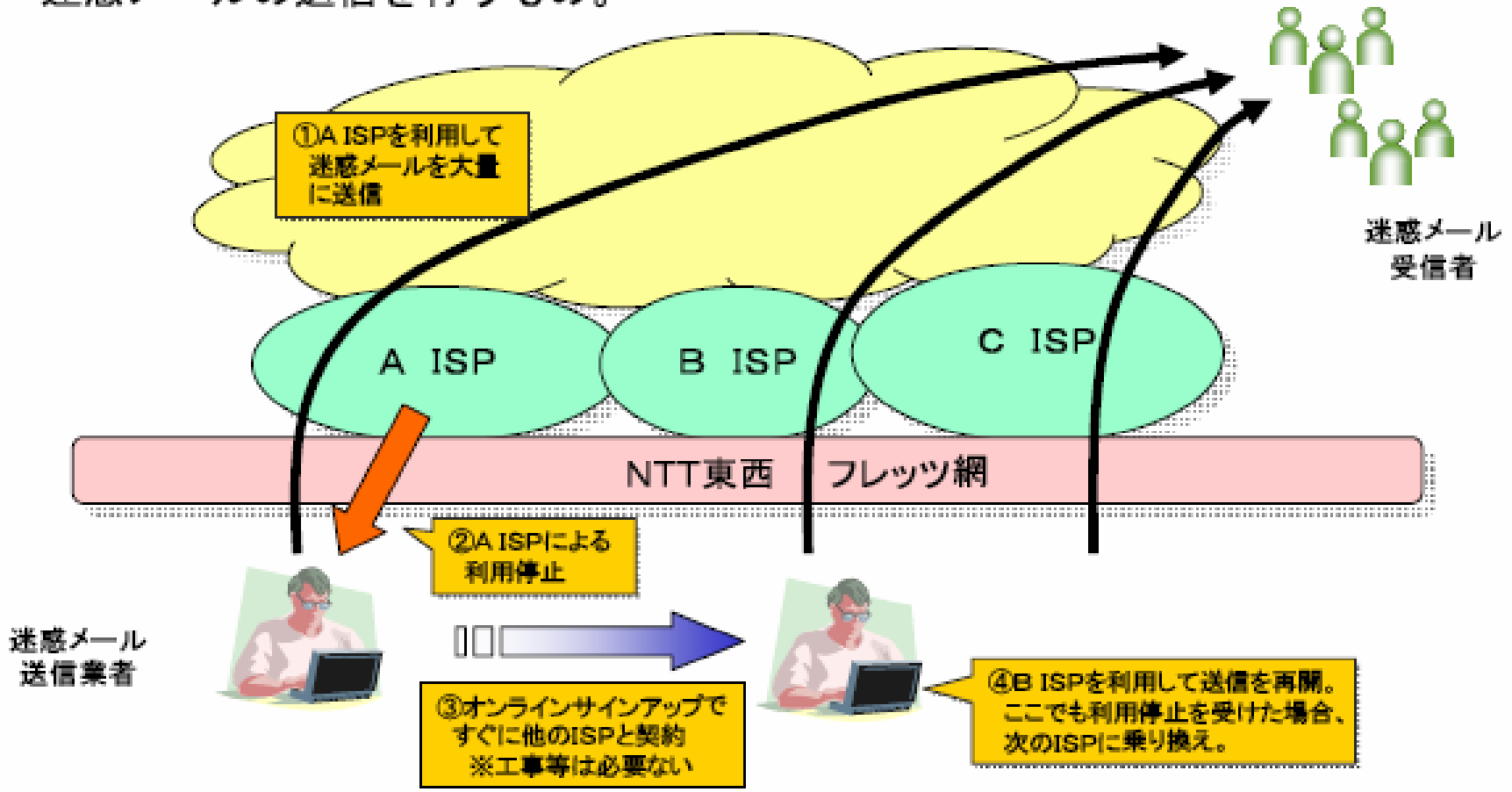
動的IPからの迷惑メールの特徴

日本での迷惑メールは、海外からのものもあるが、多くはFTTHやxDSL等の動的IPから送信されている。また、送信方法においても、下記のような工夫がされている。

- 高速な回線を用いて、1契約で大量な迷惑メールを送信してきている。
- 特定のISPで利用停止になると、送信ISPを乗り換えて送信してくる。（***「渡り」送信***）
- 受信側の規制をかいくぐる為、IPアドレスを非常に短いスパンで変更して送信する。（***「IP循環」送信***）
- 特定の地域で利用停止が進むと、拠点を変えて送信をしてくる。（***「拠点移動」送信***）

渡り送信

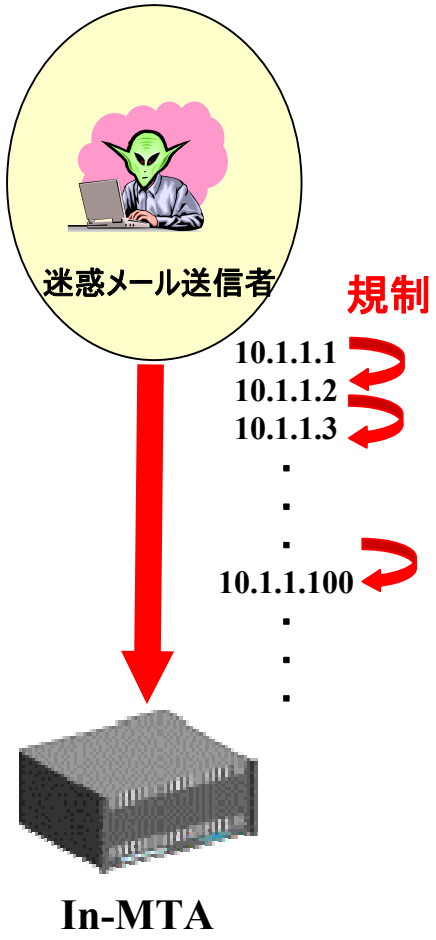
ＮＴＴ東西のフレッツ網を利用している場合に、あるＩＳＰが利用できなくなると、即座に他のＩＳＰと契約することにより、間を空けずに継続して迷惑メールの送信を行うもの。



出典：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（平成17年7月）

IP循環送信

規制される都度（または周期的に）送信IPアドレスを変更して、メール送信を規制されないように送信してくる。なお、IPアドレスの変更周期は1分より短いものも多い。
（ADSLモデムをリセットなどする事でIPアドレスを都度変更していると想定される。）



拠点移動送信

渡り送信を繰り返す内に、その地域のISPで利用停止措置が進むと、送信拠点を変えて送信して来る方法。

運用対処の効果とその限界

フレッツ網からのサインアップ時に即時払い出しを中止し、運用体制を強化し利用停止を促進した結果、一時的な効果はあったが、完全に撲滅には至らず、ある程度は送信されてしまう状況である。

OP25Bの実施時の効果

実際に、某ISPが携帯宛OP25Bを実施した際に、（当然の結果だが）動的IPからのメールはなくなった。

携帯宛OP25B

今年の秋頃から、続々と携帯宛OP25Bを実施しているが、その対策が浸透した事により、日々のメールのトラフィックが大きく変動する事がなくなり、その効果が確認出来ている。

まとめ

- 動的IPからのメールは、送信側のみならず、受信側での対応も困難としており、また、短時間に相当数の送信が可能である。この背景から、OP25Bは現時点で、最善の手と考えられる。
- OP25Bを実施した場合、一部ユーザにはサービスのデグレが発生する事があるが、それ以上に安定したメール流通の確保がし易くなり、サービス全体の安定度は向上する可能性が高い。

- OP25Bを実施にあたってのノウハウや手順については、以下の章で説明を行います。