JEAG Recommendation (Outbound Port 25 Blocking)

～第3回 迷惑メール対策カンファレンス～

赤桐 壮人

Japan Email Anti-Abuse Group

株式会社ぷららネットワークス

Copyright (c) 2006 JEAG. All rights reserved.

注意事項

1. **本プレゼンテーションは、**JEAG Recommendation**に目を通されていることを前提として進めさせて頂きます。**JEAG Recommendation**は、**http://jeag.jp/**より入手できます。**
2. **本資料は**JEAG Recommendation**の抜粋に補足のためのスライドを補充した構成となっております。著作権等に関しては、**JEAG Recommendation**およびJEAG**の規定に従います。**
3. **本プレゼンテーションもしくは、**JEAG Recommendation**の内容に関する疑問点は、**akagiri@jeag.jp**にて承ります。**(JEAG**の活動に対するお問い合わせはご遠慮ください。**)

Copyright (c) 2006 JEAG. All rights reserved.

- お詫び

  配布資料を基に、事前にプレゼンを行ったところ、
  かなりの数の補足資料が必要であったため、
  資料を大幅に更新しております。

- 今日の資料

  http://jeag.jpよりダウンロード可とする予定
  ユーザ名：spamconf　パスワード：antispam
  ※数日、お待ちください

Copyright (c) 2006 JEAG. All rights reserved.

今日の参加者について

1. ISP の関係者（メールサービス）
   - OP25Bを実施している
   - まだ実施していない
2. ホスティング事業者／ASP事業者
3. SIer
4. 企業の情報システム／NW管理者
5. 大学等、教育機関の関係者
6. その他

Copyright (c) 2006 JEAG. All rights reserved.

◆正しいメールの到達性を確保する（疎通をよくする）

- Outbound port 25 Blocking
- **送信ドメイン認証**
- Reputation
- **受信フィルタ**、RBL・・・

Copyright (c) 2006 JEAG. All rights reserved.

◆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

※ JEAG Recommendation 2章より

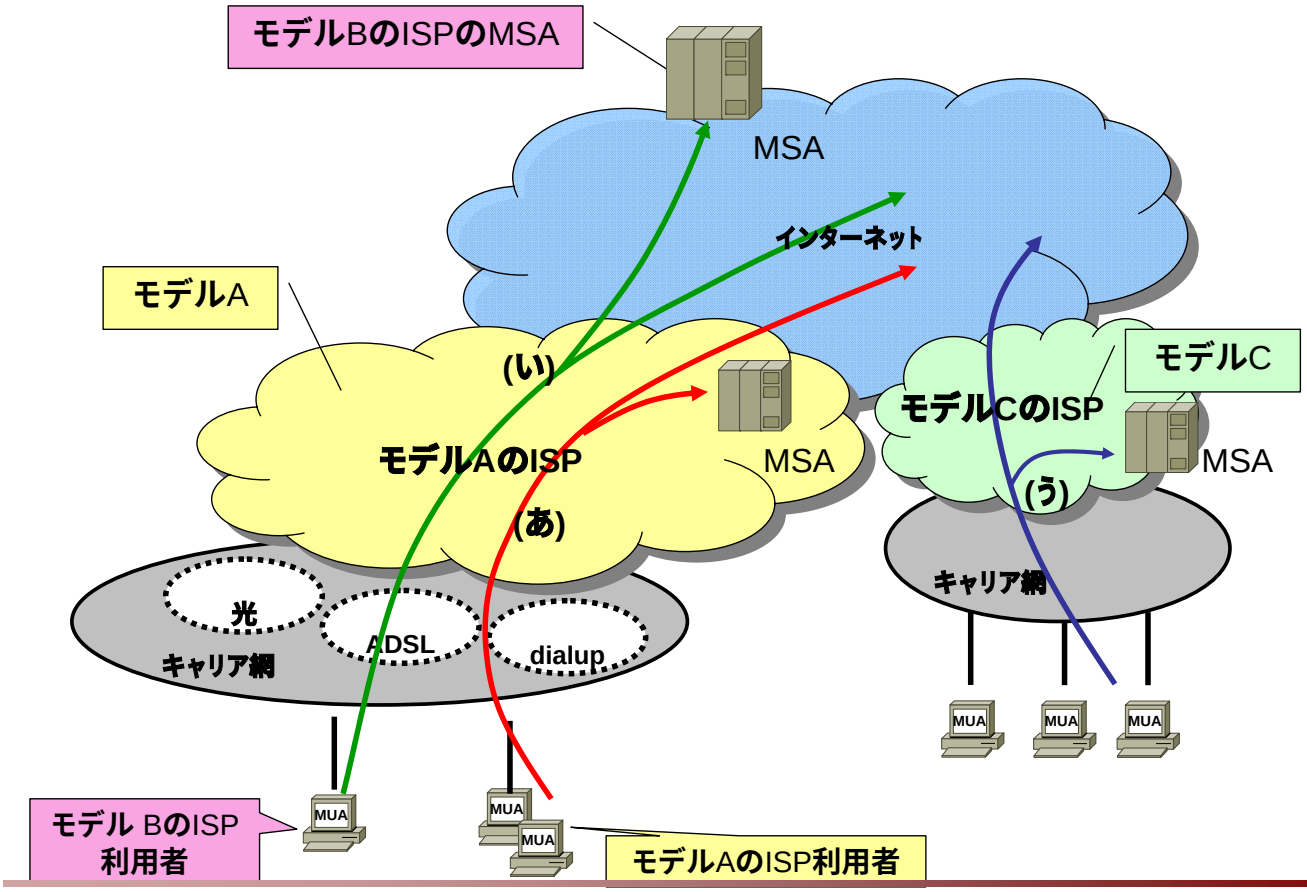
Copyright (c) 2006 JEAG. All rights reserved.

- 配送／投稿
- MUA／MSA／MTA
- Outbound Port 25 Blocking
- SMTP AUTH
- Submission Port
- 第三者サーバ

Copyright (c) 2006 JEAG. All rights reserved.

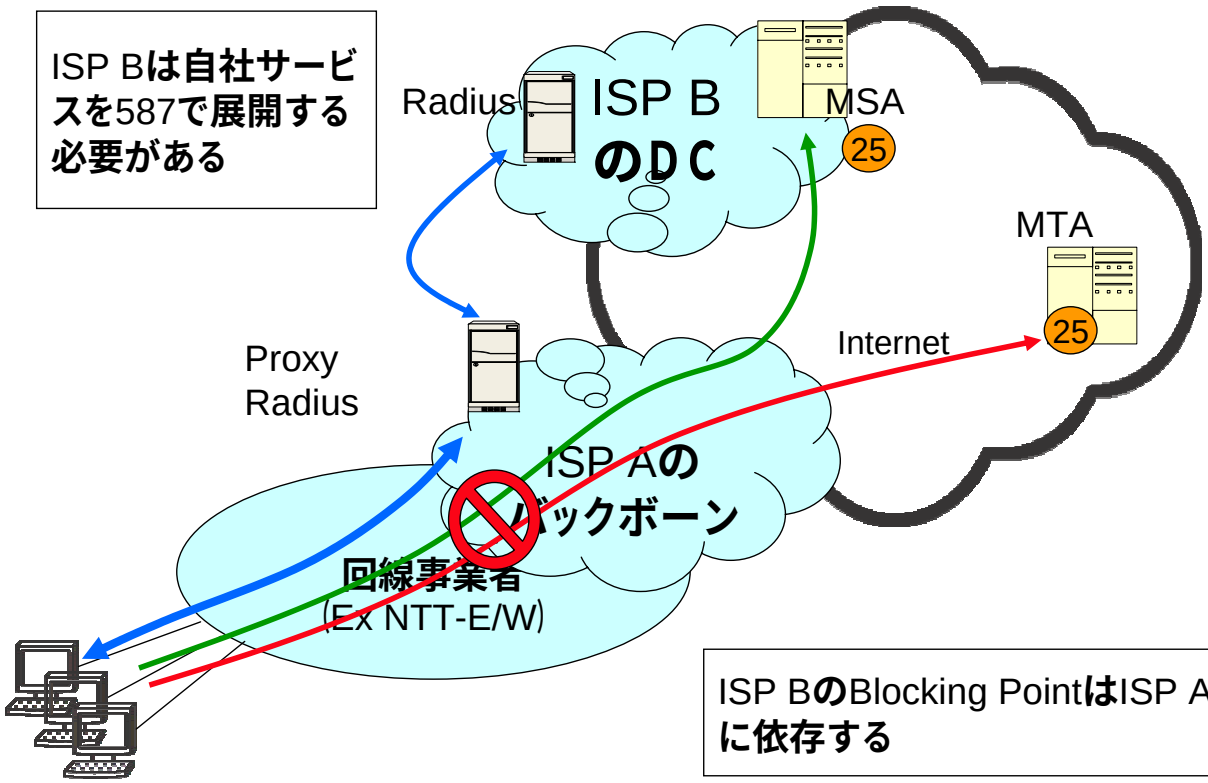
- モデル A
  - インターネット接続（バックボーン）を他の ISP(モデル B) に OEM 提供している ISP
- モデル B
  - インターネット接続（バックボーン）を他の ISP(モデル A) に依存している ISP
- モデル C
  - インターネット接続は自社のサービスでしか利用していない。
  - モデル B の ISP を抱えていないモデル A の ISP

Copyright (c) 2006 JEAG. All rights reserved.



Copyright (c) 2006 JEAG. All rights reserved.

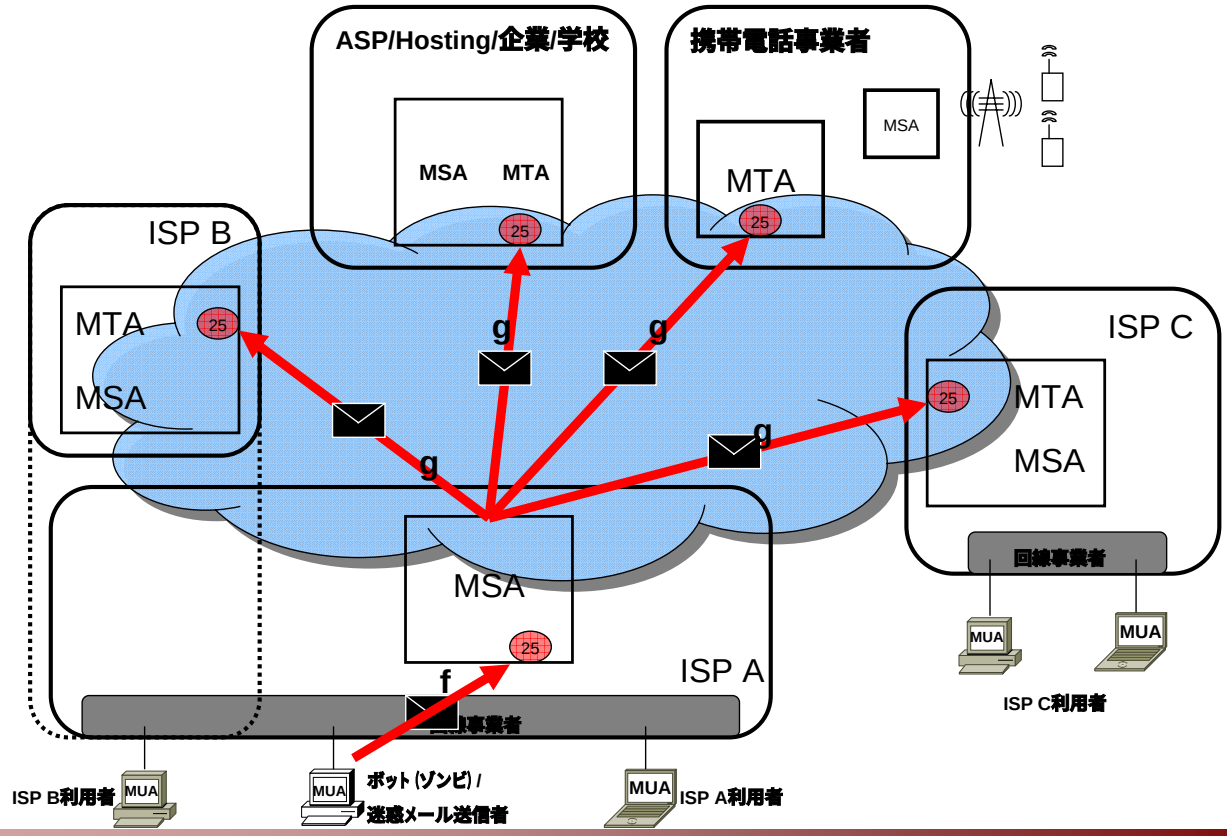
ISP Bは自社サービスを587で展開する必要がある



ISP BのBlocking PointはISP Aに依存する

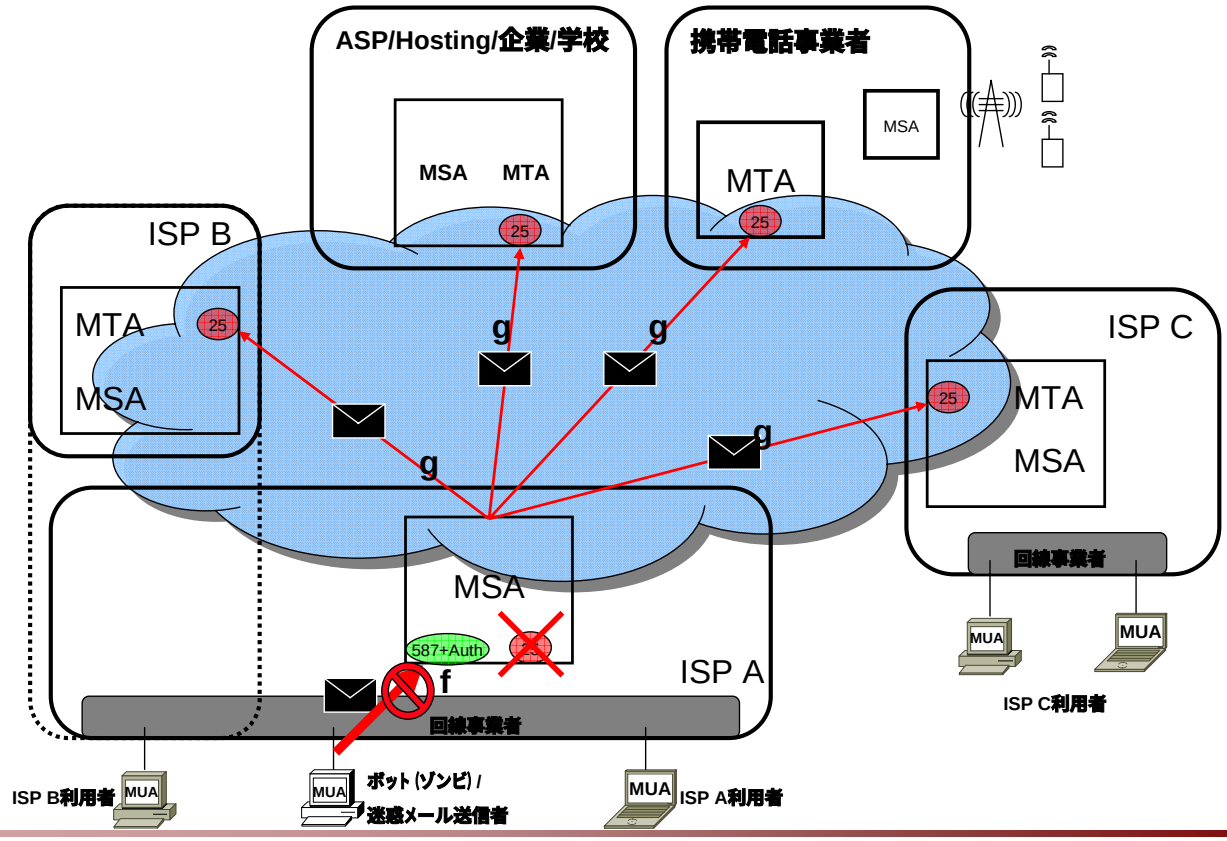
Copyright (c) 2006 JEAG. All rights reserved.

送信パターンⅠ



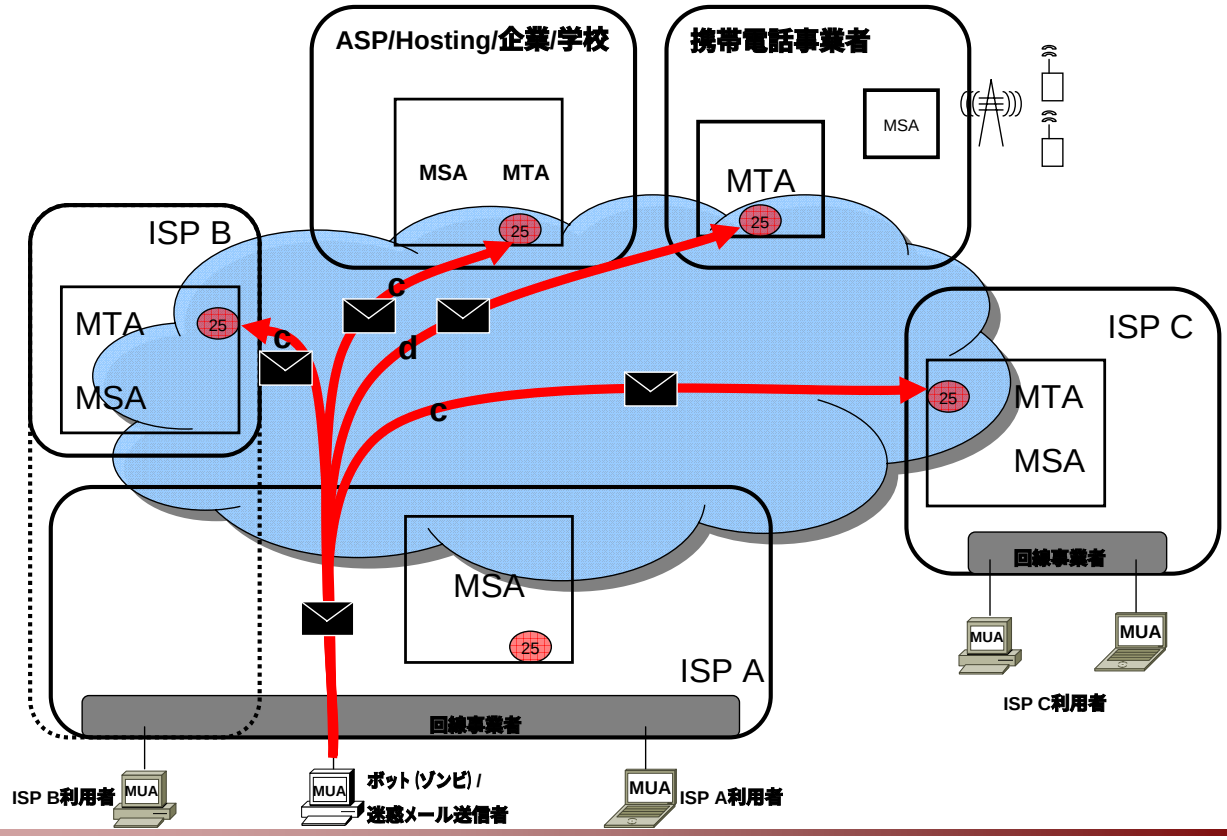
Copyright (c) 2006 JEAG. All rights reserved.

送信パターンⅠ:SMTP AUTHに基づく送信通数制限が有効



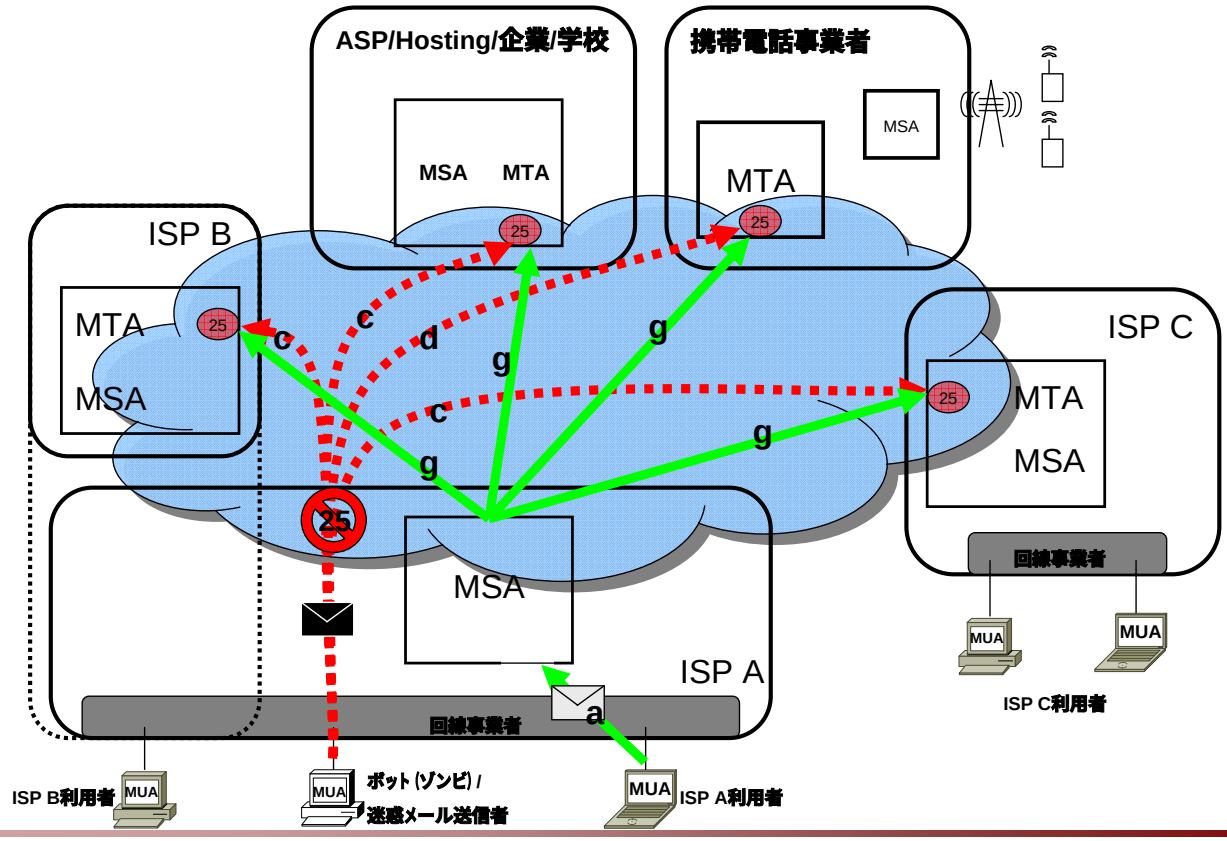
Copyright (c) 2006 JEAG. All rights reserved.

送信パターンII



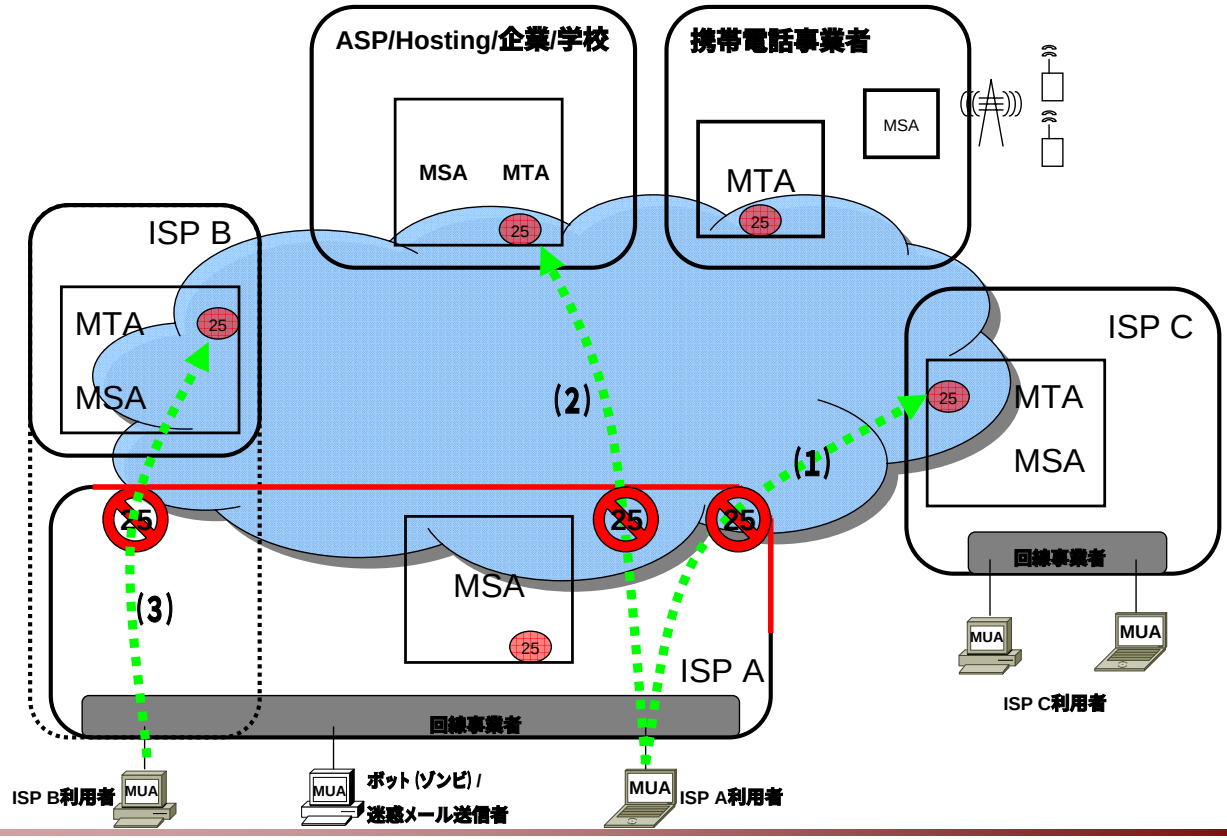
Copyright (c) 2006 JEAG. All rights reserved.

送信パターンII : OP25B が有効



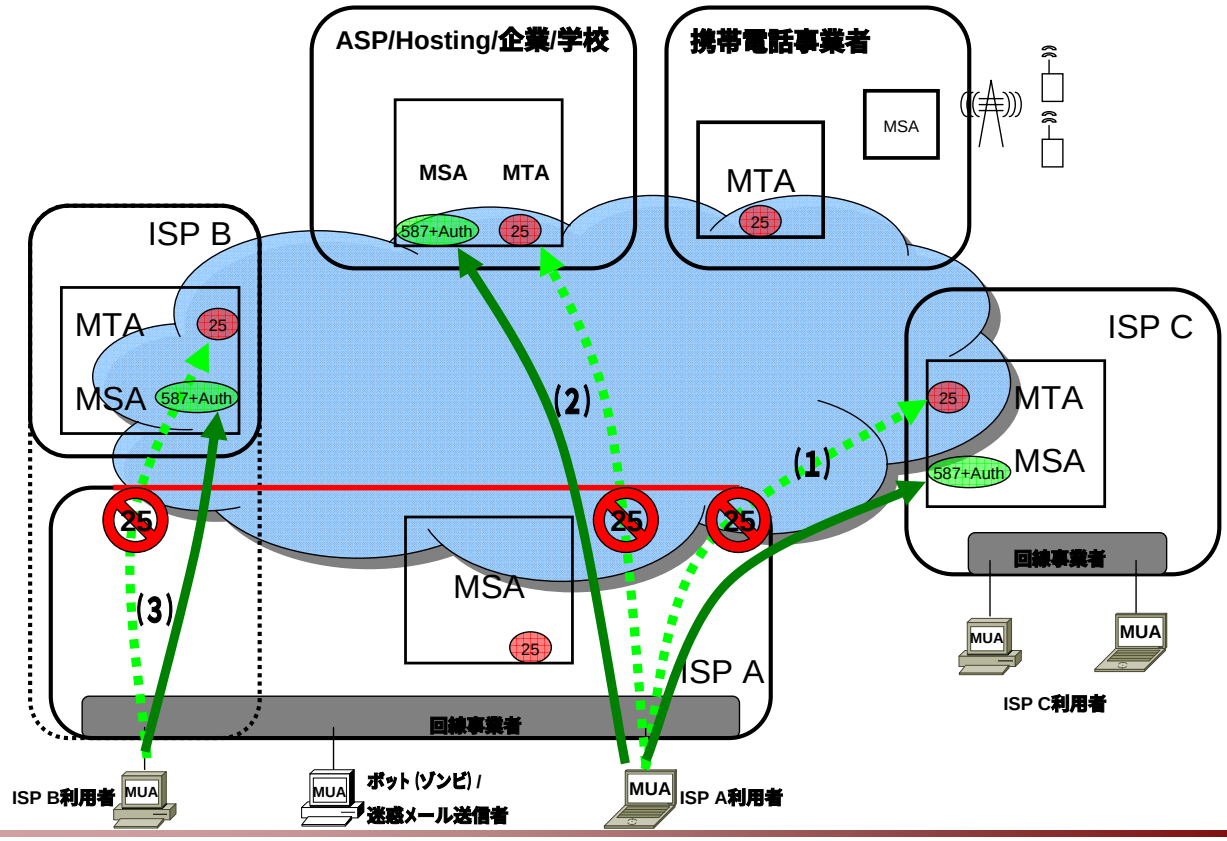
Copyright (c) 2006 JEAG. All rights reserved.

完全なOP25Bを実施するに当たっての問題点：第三者サーバへの投稿



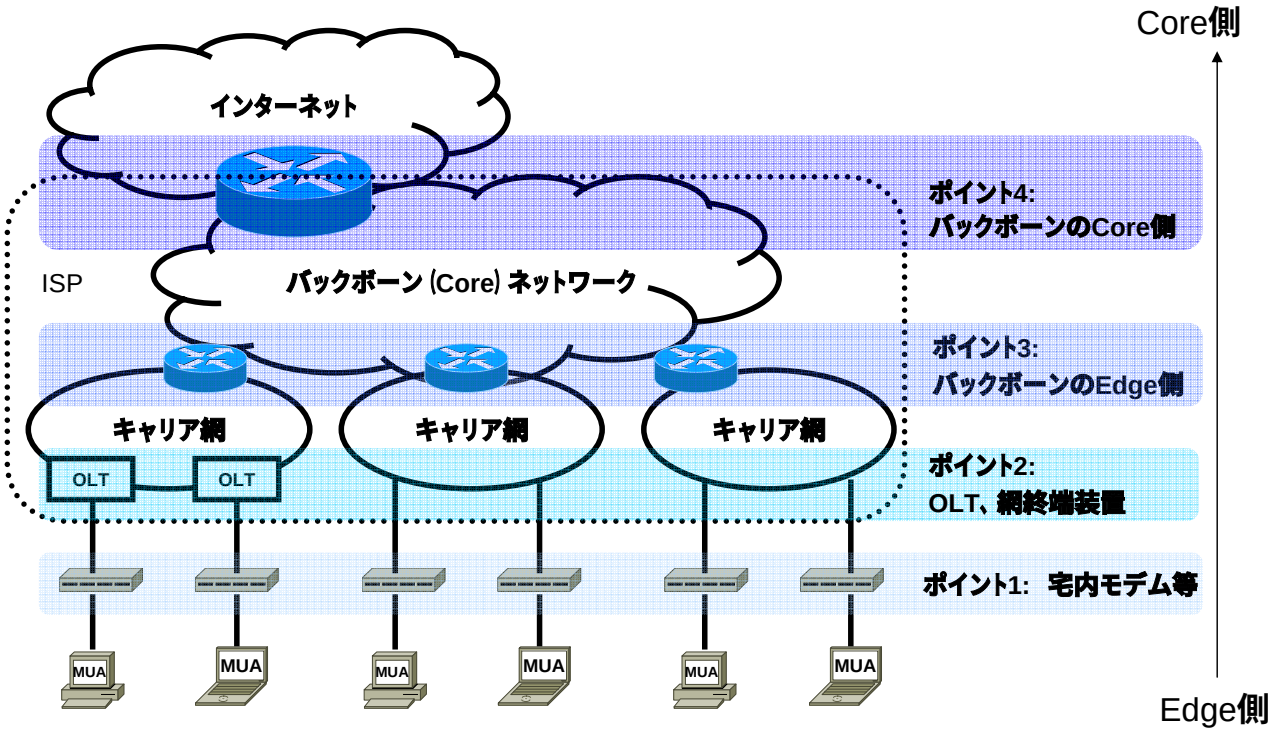
Copyright (c) 2006 JEAG. All rights reserved.

完全なOP25Bを実施するに当たっての問題点：第三者サーバへの投稿



Copyright (c) 2006 JEAG. All rights reserved.

ブロッキングポイント



Copyright (c) 2006 JEAG. All rights reserved.

Recommendについて

【 Recommend 5】SMTP Authによる通数制限の実施

【 Recommend 4】Outbound Port 25 Blockingの実施

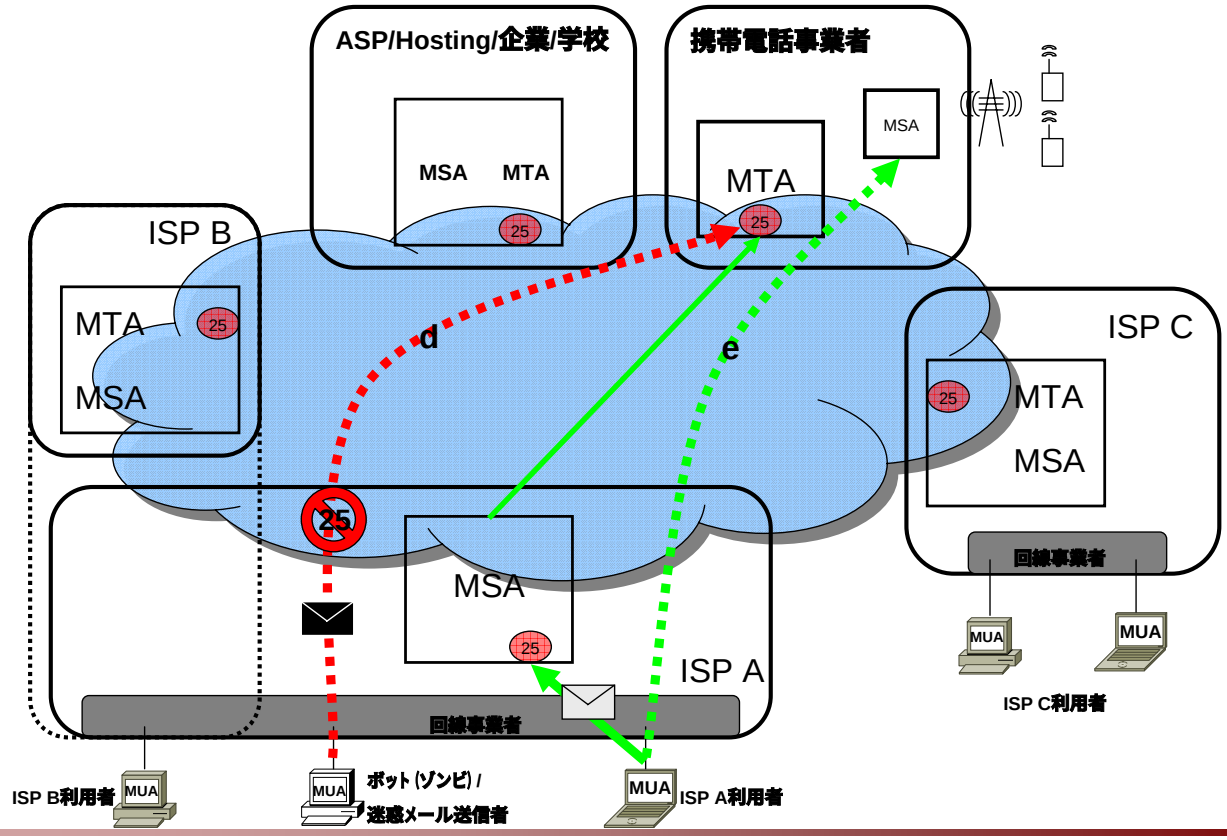
【 Recommend 3】MSA(587+Auth)とMTAの分離

【 Recommend 2】Submission Port (587) の利用者への提供

【Recommend 1】携帯電話宛限定OP25Bの実施

Copyright (c) 2006 JEAG. All rights reserved.

Recommend 1 : 携帯電話あて限定のOP25B



Copyright (c) 2006 JEAG. All rights reserved.

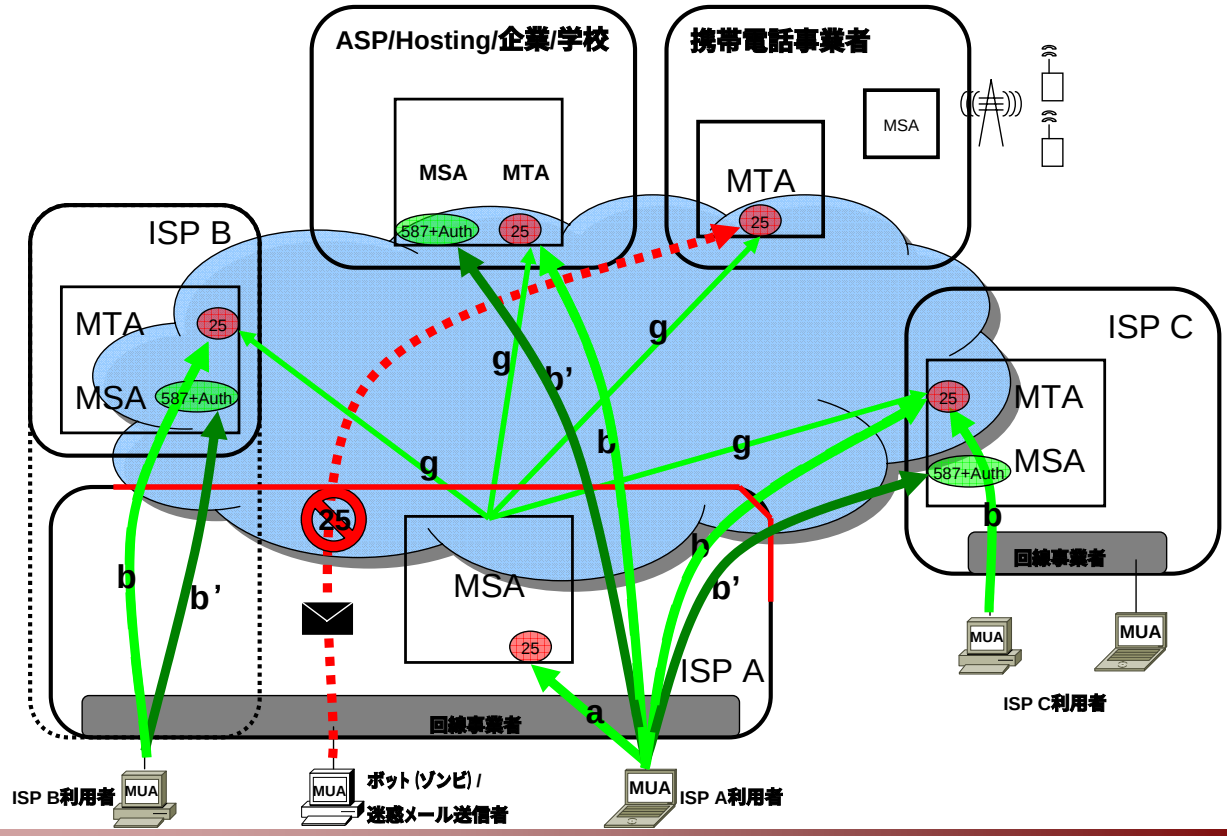
Recommend 1 : 携帯電話あて限定のOP25B

◆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。

- 対象 ： ISP
- 携帯電話宛の迷惑メールは現在でも非常に多い
- その発信源はISPの動的IP
- 携帯電話事業者のMSAは携帯電話からの投稿しか受け付けない
  - → 動的IPからの接続は基本的に「投稿」
  - → Blockしても問題にならない

Copyright (c) 2006 JEAG. All rights reserved.

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



Copyright (c) 2006 JEAG. All rights reserved.

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 を提供しなければならない。

- 対象 ： Global IP Addressから投稿を受け付ける MSA の管理者

◆MSA には SMTP AUTH を実装しなければならない
(SMTP AUTHを実装していない MSA(587) は提供してはならない)

- 認証しなかったら25が587に変わるだけ

○ 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。

- 認証しておかないと自ドメインが狙い打ちにあう

○ POP ID/Password は AUTH ID/Password と同一にするのが望ましい。

- MUAへの配慮(AUTH IDの設定が無い場合は自動的にPOP ID)

◆MSA では POP before SMTP を提供してはならない。

- AUTHで同じことができる上に、PBSはセキュリティホールになりえる

Copyright (c) 2006 JEAG. All rights reserved.

Message Submission (RFC 2476)

- Dec. 1998

Message Submission for Mail (RFC 4409)

- Apr. 2006

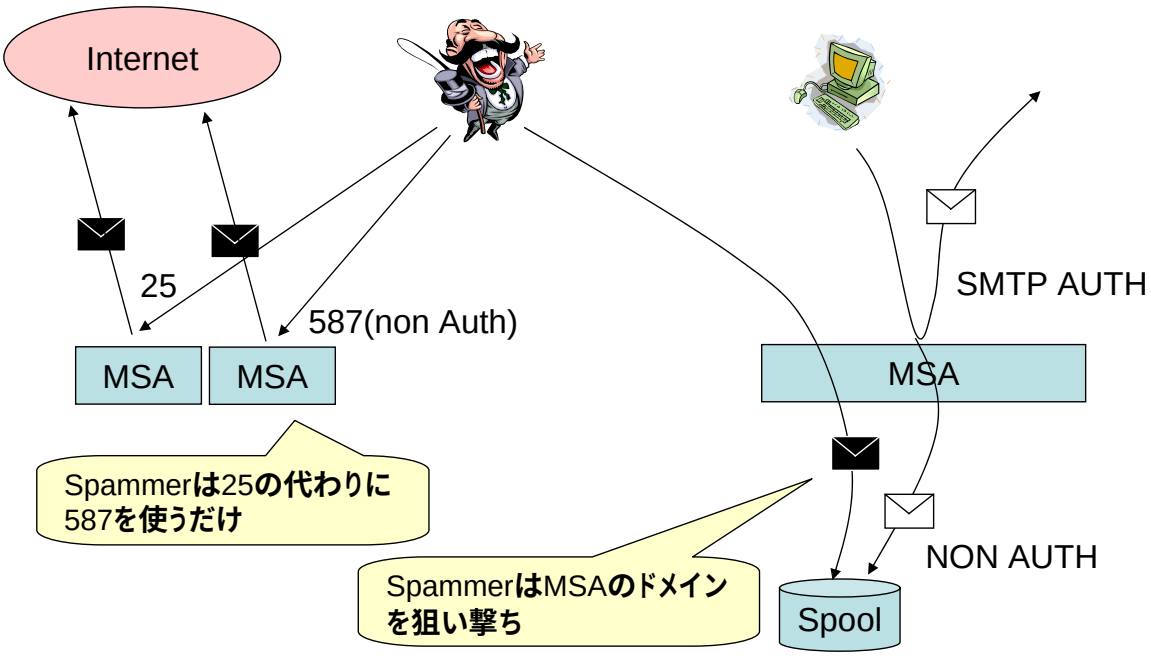
- RFC2476 → RFC4409

  Require Authentication : Optional Actions → Mandatory Actions

Copyright (c) 2006 JEAG. All rights reserved.

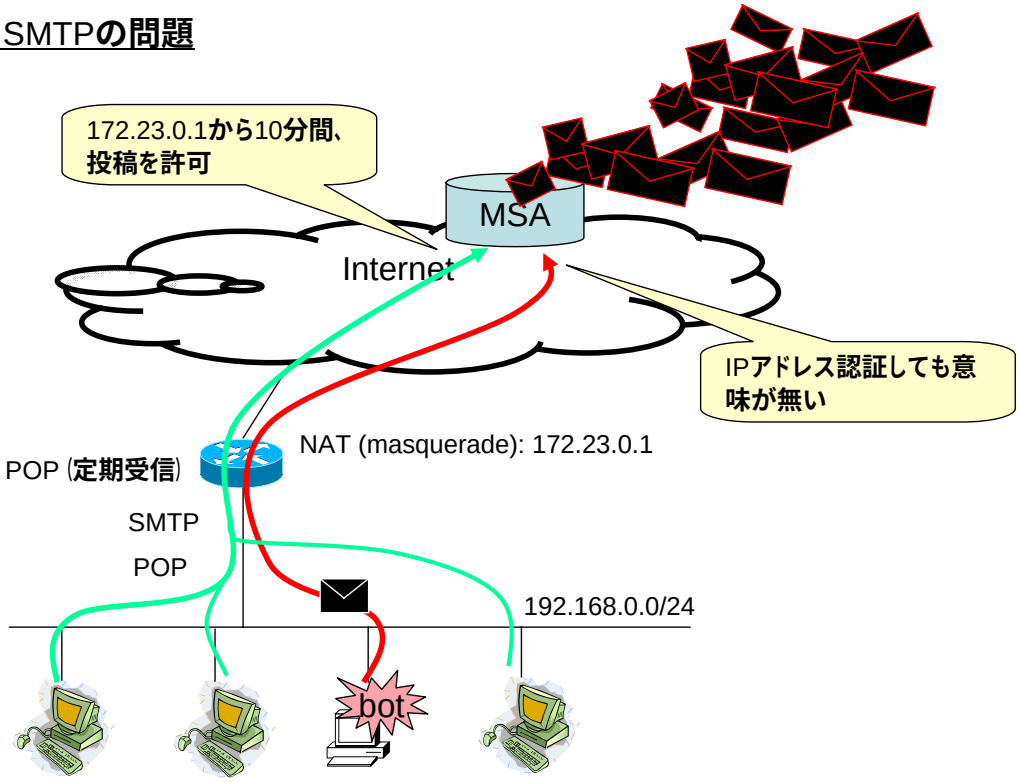
1) Port 587でAuthをしないと？

2) Local Domain宛にAuthをしないと？

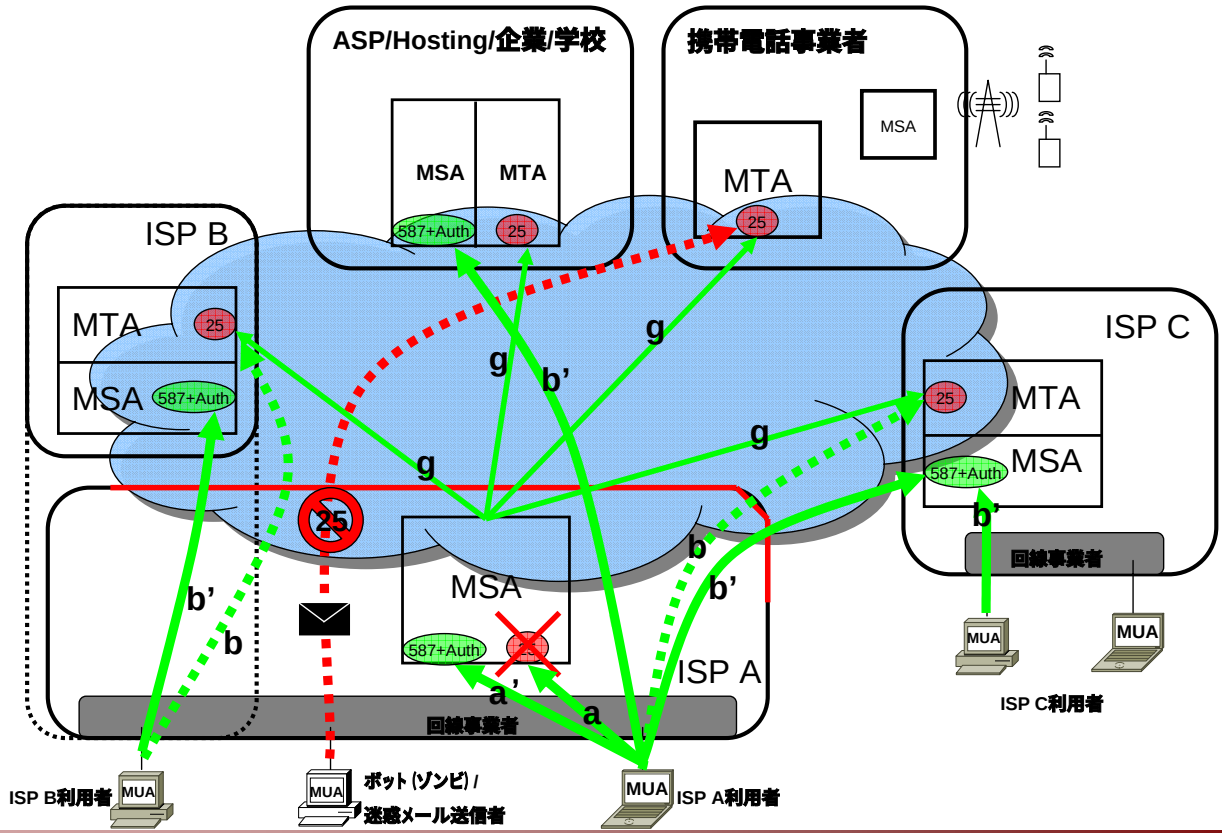


Copyright (c) 2006 JEAG. All rights reserved.

POP before SMTPの問題



Copyright (c) 2006 JEAG. All rights reserved.



Copyright (c) 2006 JEAG. All rights reserved.

◆すべてのメールの投稿にSMTP AUTHを実施する

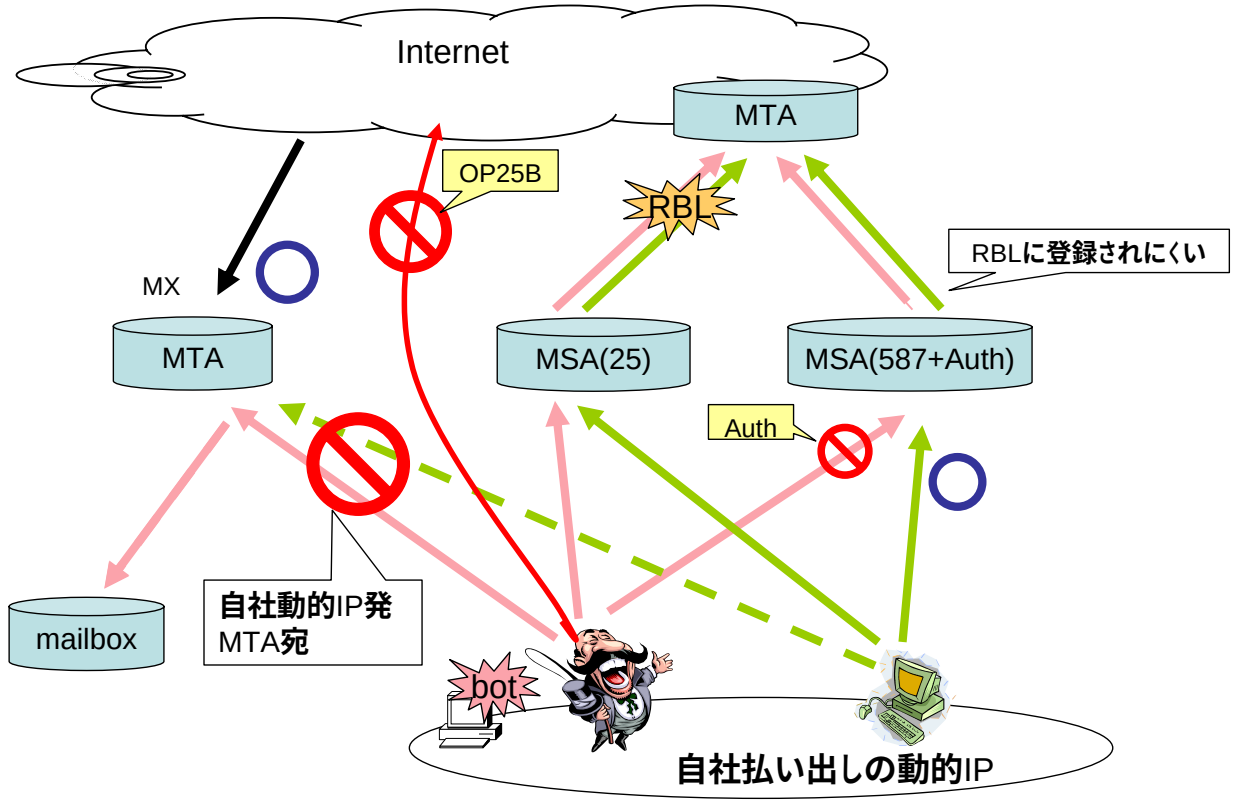
- メールの投稿には、MSA(587+Auth) を利用しなければならない
- MSA(25) は将来的に廃止するべきである
- 対象 ： Global IP Addressから投稿を受け付ける MSA の管理者

◆Recommend 5への布石

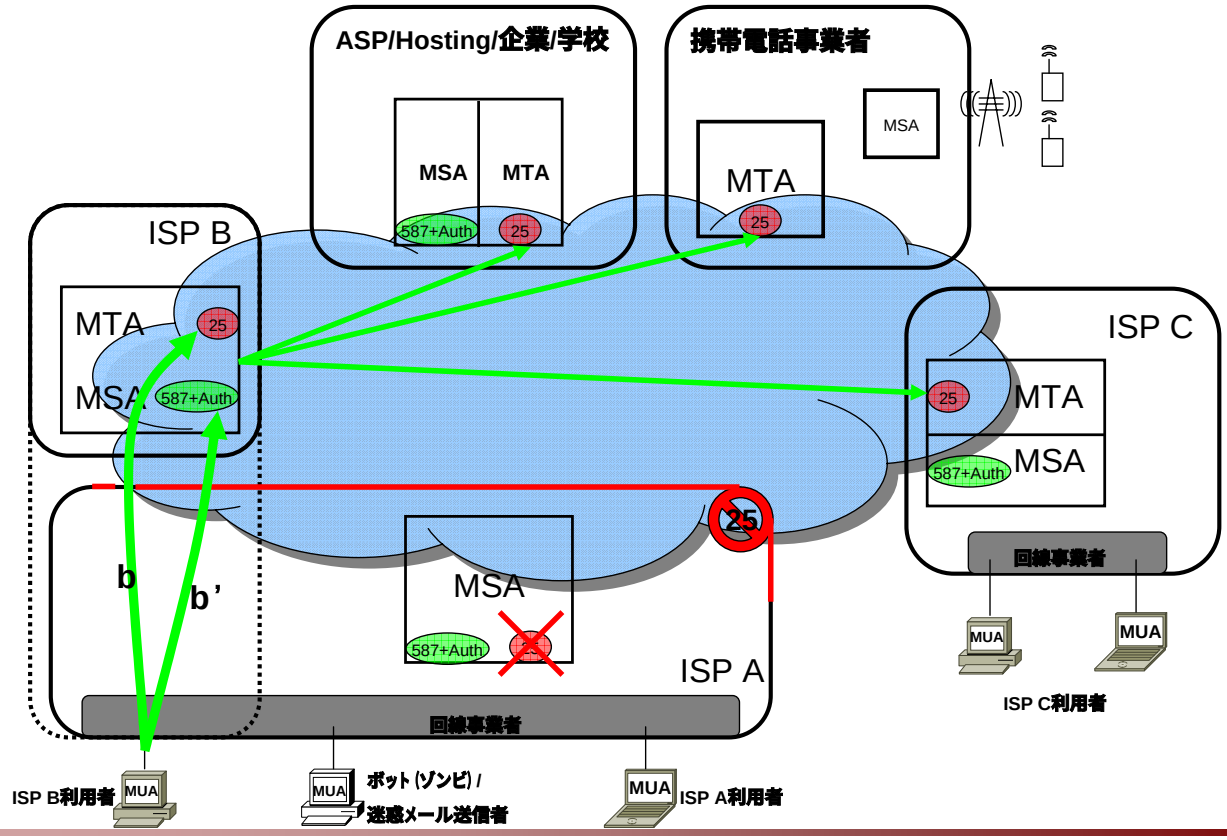
- MSA における送信数制限

Copyright (c) 2006 JEAG. All rights reserved.

(参考情報) MSA(25)、MTA(25)、MSA(587+Auth)は分離したほうがよい



Copyright (c) 2006 JEAG. All rights reserved.



Copyright (c) 2006 JEAG. All rights reserved.

モデル A の ISP

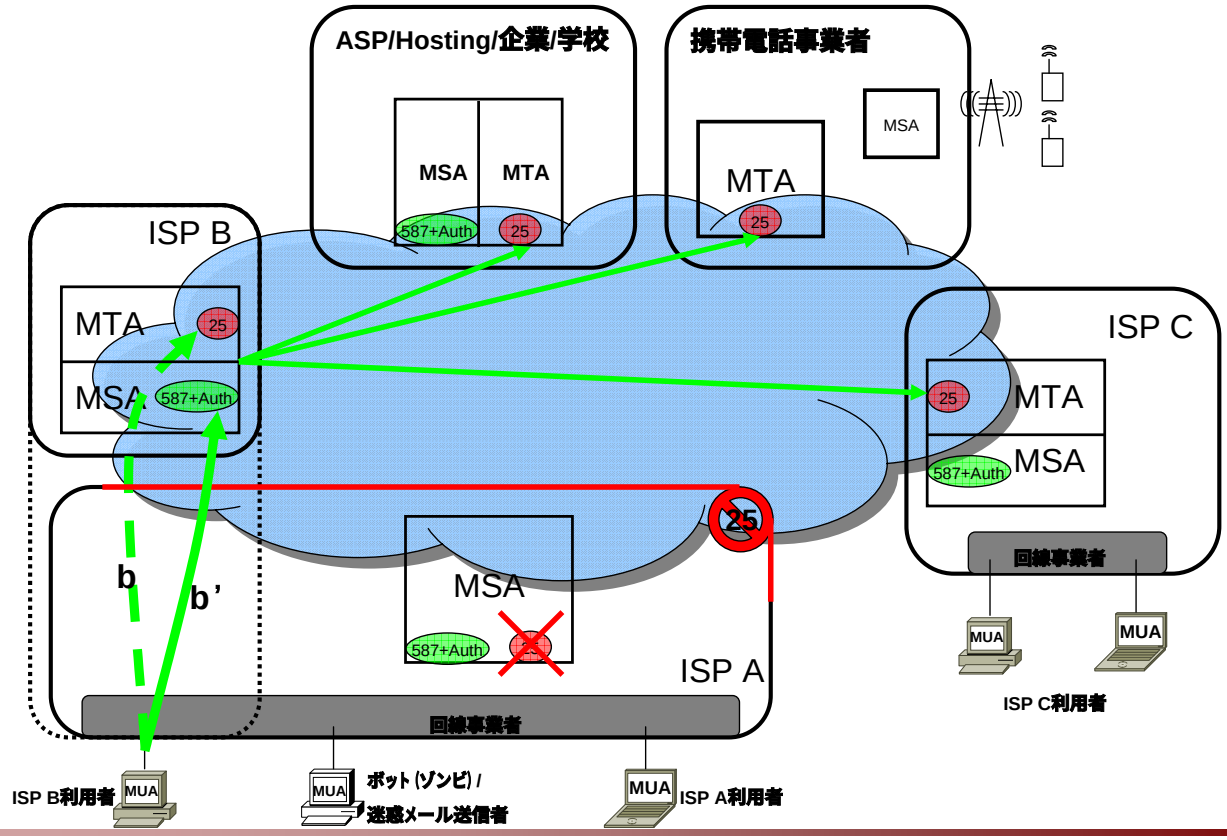
- OP25Bを行う場合、ISP Bにも影響が出る
- この場合、モデル B の ISPのMSAへの通信をPermitする
  → ただし、これは期間限定（長くても1年程度）

モデル B の ISP

- モデル A の ISP の OP25B の依頼は受ける
- MSAのアドレスブロックをできるだけ少なくまとめる
- 全ユーザがMSA(587+Atuh)を使うように移行を行う

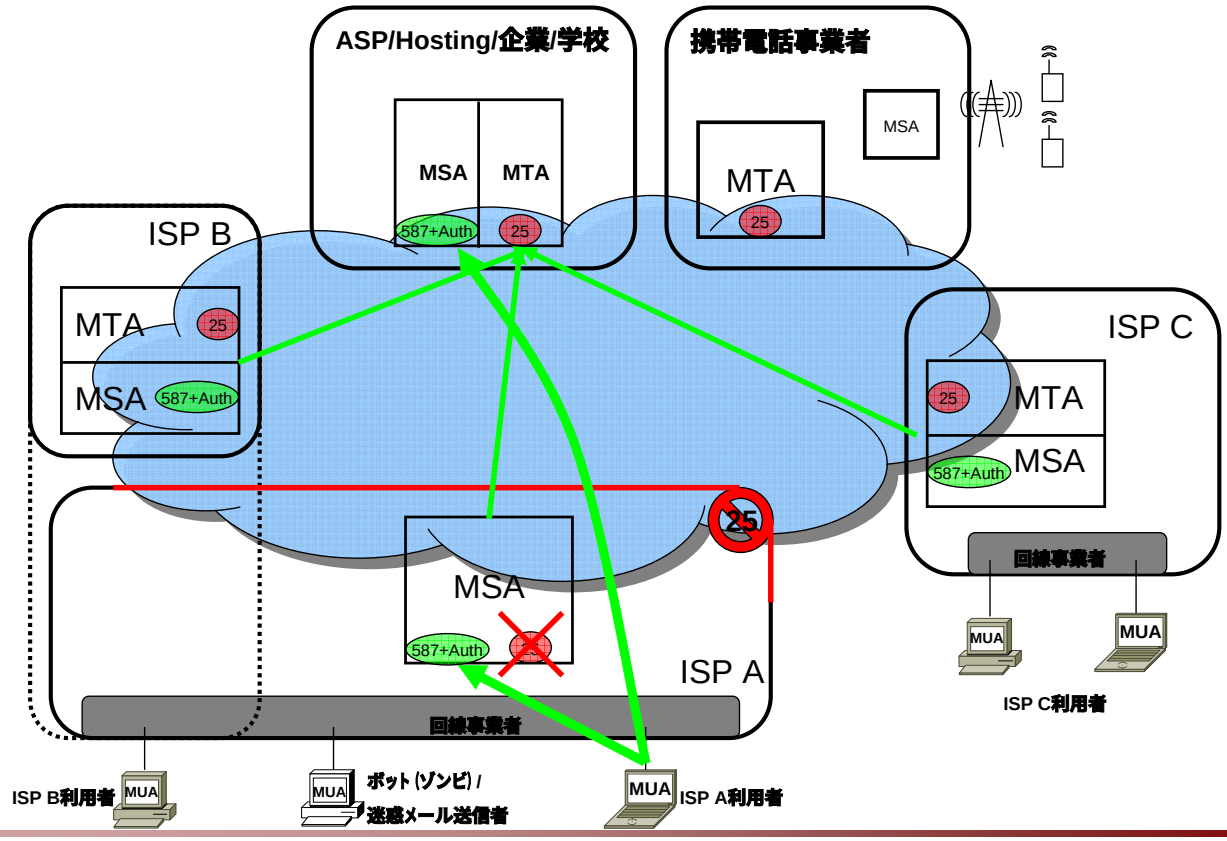
Copyright (c) 2006 JEAG. All rights reserved.

Recommend 3.1：モデル A およびモデル B の ISP：移行完了後



Copyright (c) 2006 JEAG. All rights reserved.

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



Copyright (c) 2006 JEAG. All rights reserved.

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

- 対象 ： Global IP Addressから投稿を受け付ける MSA の管理者

  (特にHostingやASP事業)

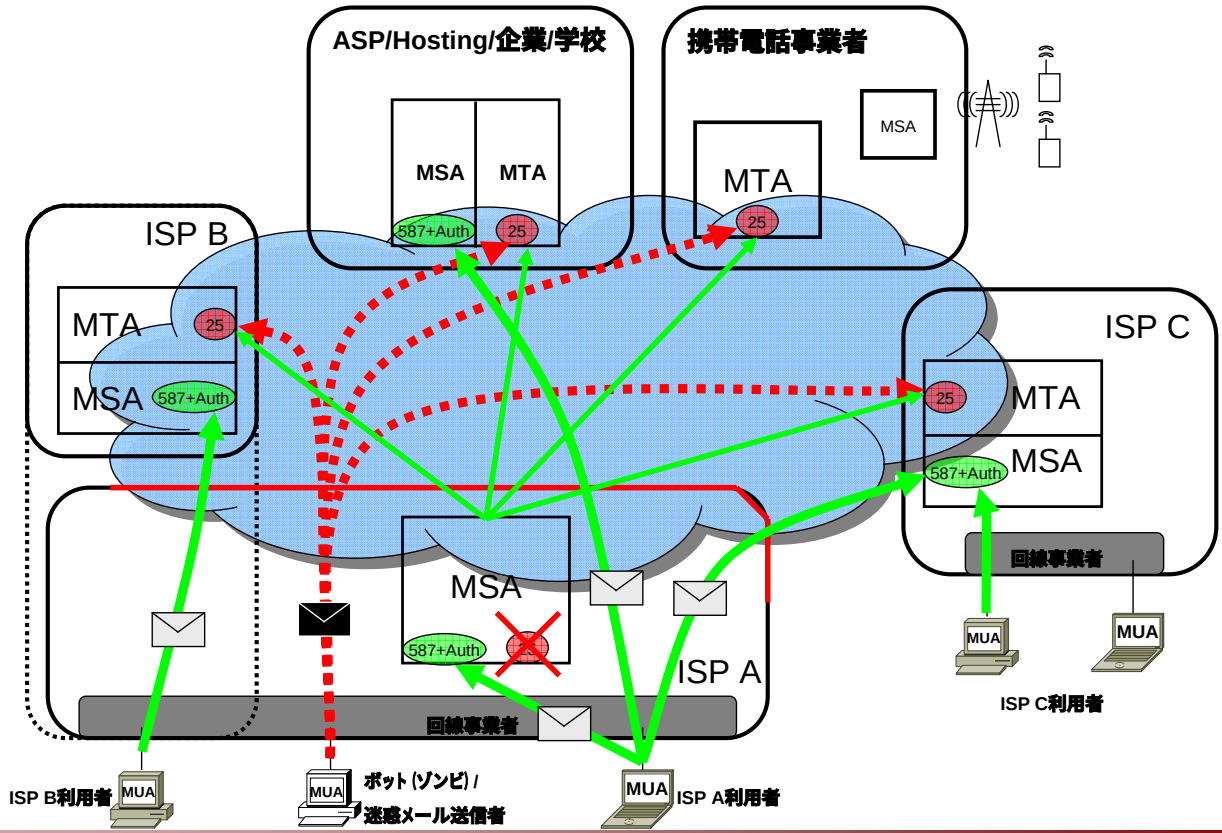
- ISPがOP25Bを実施すると、メールの投稿を受け付けられなくなる
- ISPのOP25Bの実施ペースがかなり早い

  → 6月～7月に数社が実施

  → OP25Bの実施の早いISPは代替MSAを準備するべき

Copyright (c) 2006 JEAG. All rights reserved.

Recommend 4：OP25Bの実施



Copyright (c) 2006 JEAG. All rights reserved.

◆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

- 対象 ： ISP
- モデルAのISPは「第三者サーバの代替 MSA」を提供するべきである
  - → MSA(587+Auth)の対応が遅れた事業者のMSAの代替（これはエンドユーザの救済でもある）
  - → 中継サーバは期間限定で提供するべきである

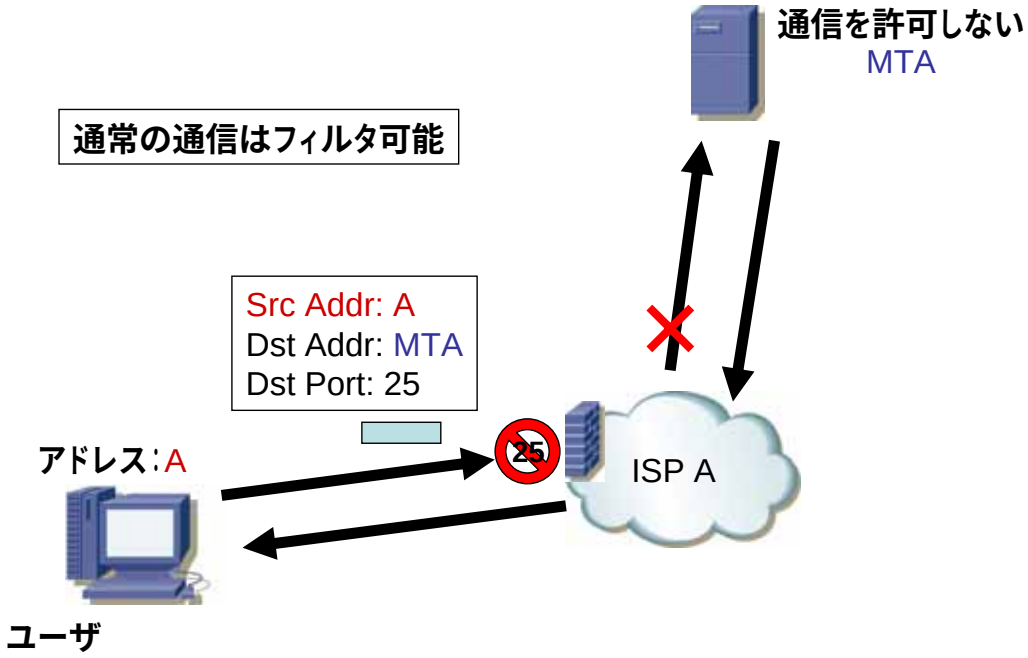
Copyright (c) 2006 JEAG. All rights reserved.

◆Asymmetric Routing Attack 対策を実施するべきである

- 自社が動的IP側のとき（Inbound Source Port 25 Blocking）
  - -ISP のバックボーンネットワークから動的IPへの通信 のうち，「決められた MSA」の25番ポートを Source Port とする通信のみを許可し，「これ以外の MSA」の25番ポートをSource Port とする通信は全て制限する
- 自社が固定IP側のとき (Source Address Validation)
  - -Source Address Validationを実施し，固定･動的 IP から ISP のバックボーンネットワーク方向への通信で送信元アドレスの詐称を防止する

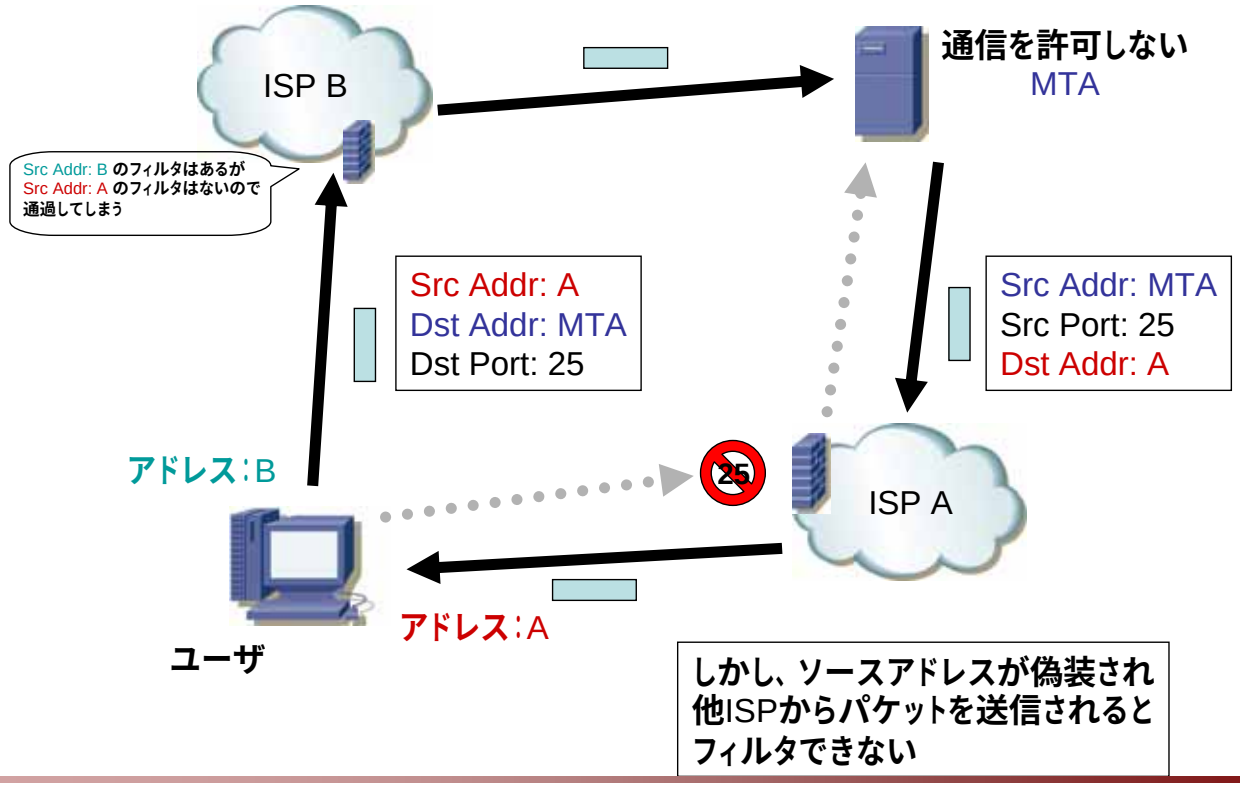
Copyright (c) 2006 JEAG. All rights reserved.

Outbound Port 25 Blocking



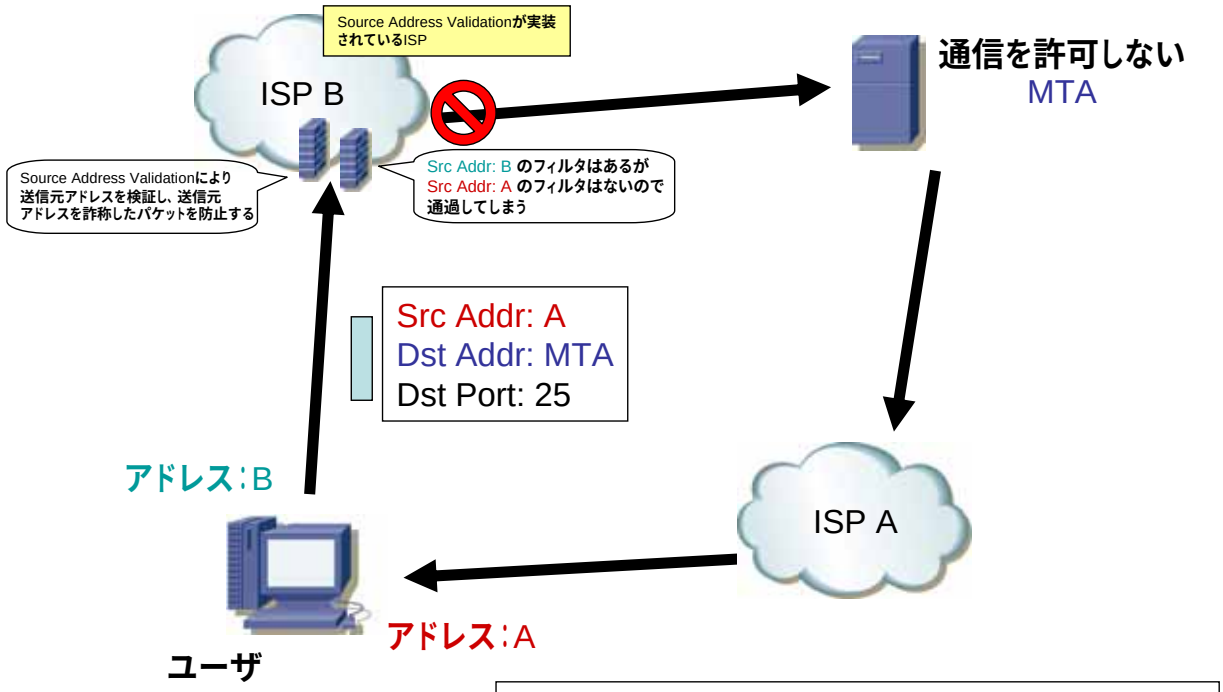
Copyright (c) 2006 JEAG. All rights reserved.

上り方向にフィルタをかけたが、Asymmetric Routing Attackによりフィルタをすり抜けてしまう場合



Copyright (c) 2006 JEAG. All rights reserved.

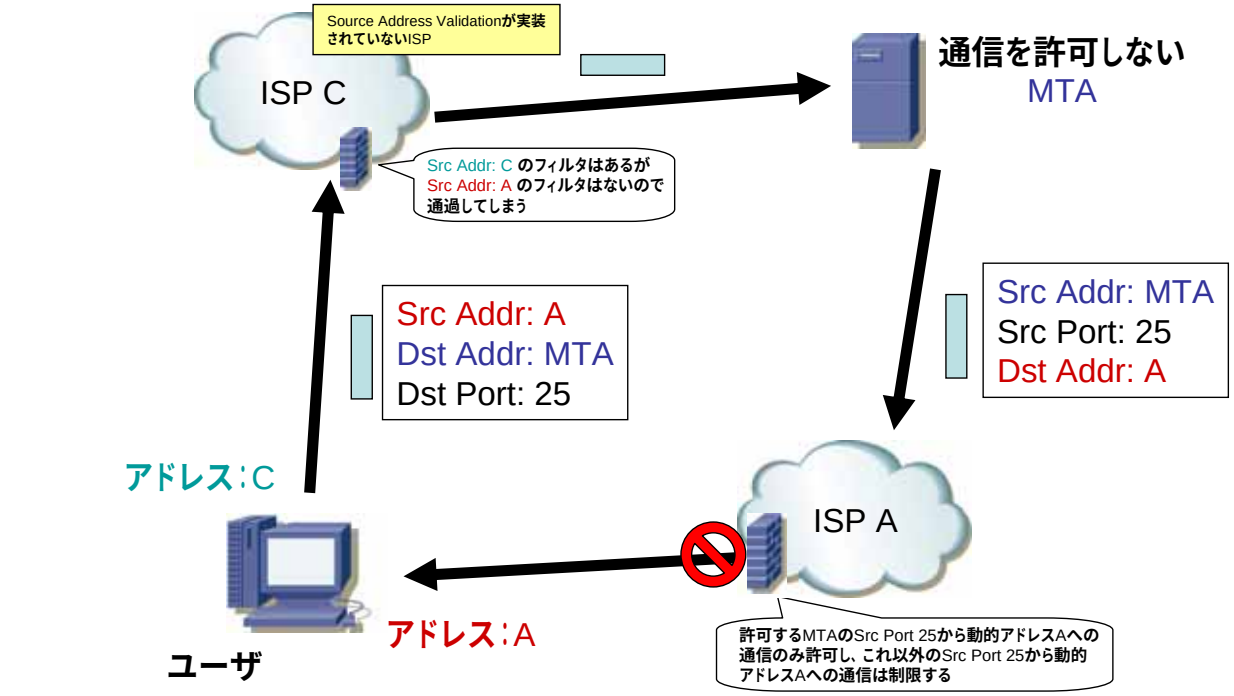
Source Address ValidationによりAsymmetric Routing Attackを防ぐ



ISP BのSource Address Validationによって
送信元アドレスが詐称されたパケットは破棄される

Copyright (c) 2006 JEAG. All rights reserved.

下り方向にフィルタをかけてAsymmetric Routing Attackを防ぐ

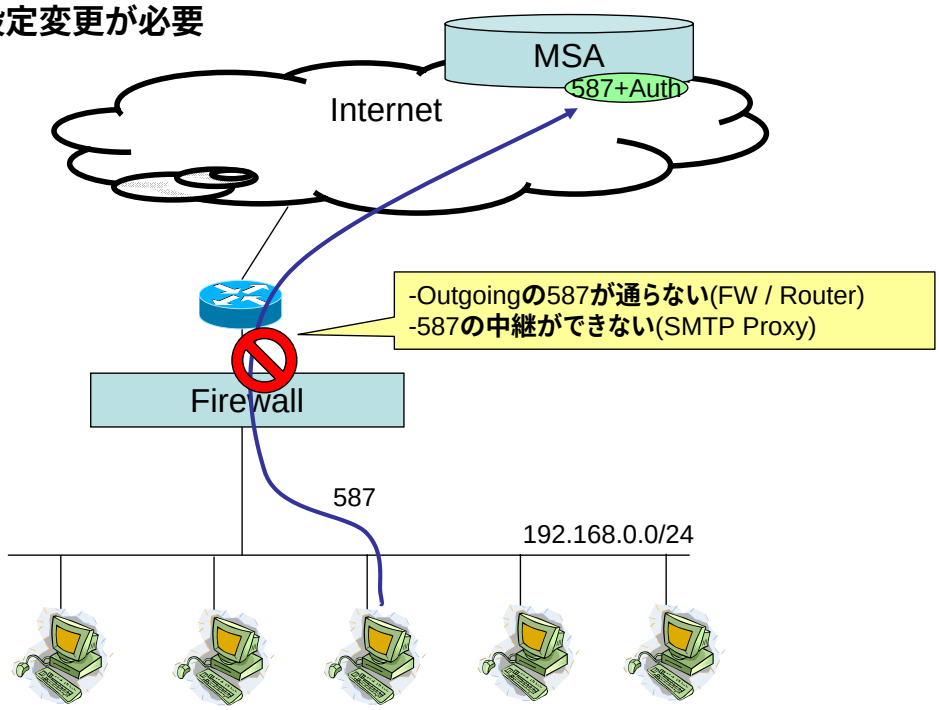


ISP CはSource Address Validationが実装されていないため送信元アドレスが詐称されたパケットは通過してしまう。ISP A側で下り方向にフィルタをかけることでTCPの通信が成立せず、メール送信を防ぐことができる

Copyright (c) 2006 JEAG. All rights reserved.

Firewall / Proxy**の問題**

- **設定変更が必要**



Copyright (c) 2006 JEAG. All rights reserved.

◆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。**

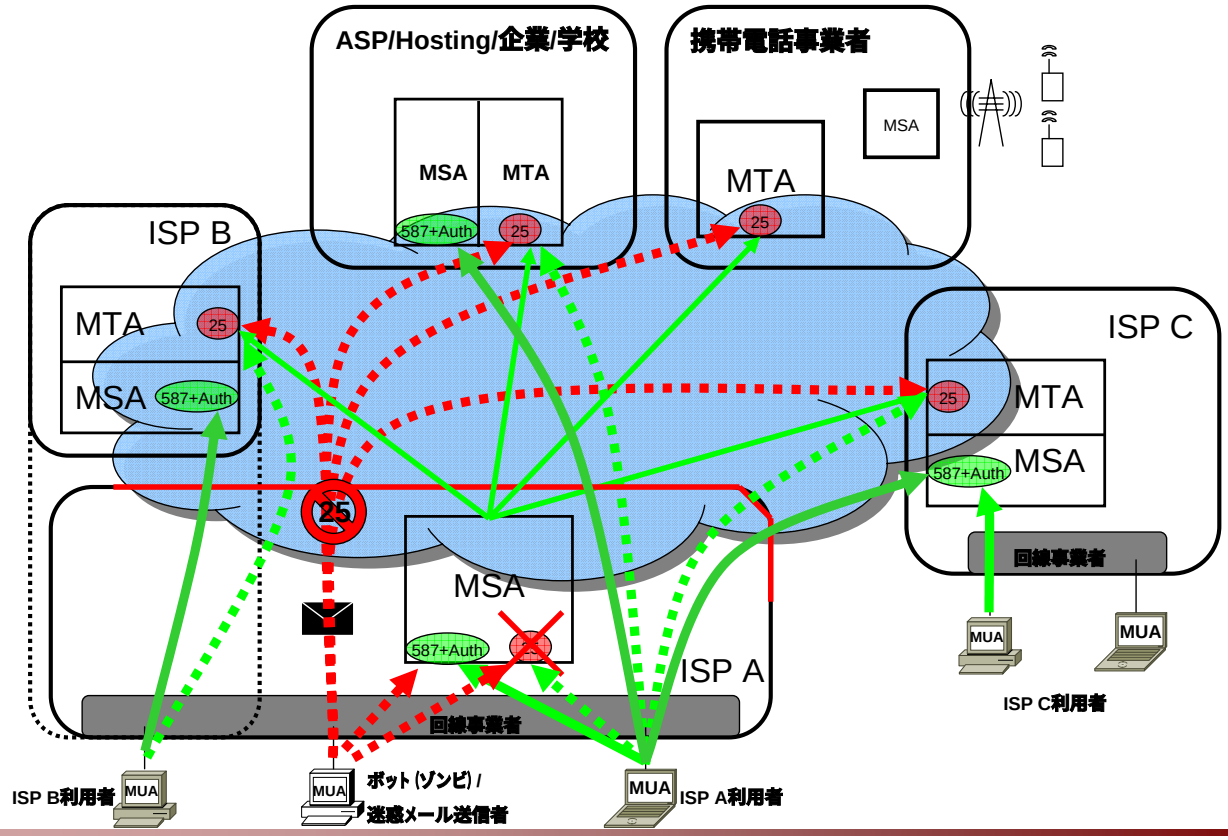
■ **対象** ： Global IP Address**から投稿を受け付ける** MSA **の管理者**

■ OP25B**により送信手段を失った**Spammer**や**bot**はパターンⅠの送信経路を利用し始める**

→ **すでにこの傾向は表れている？**

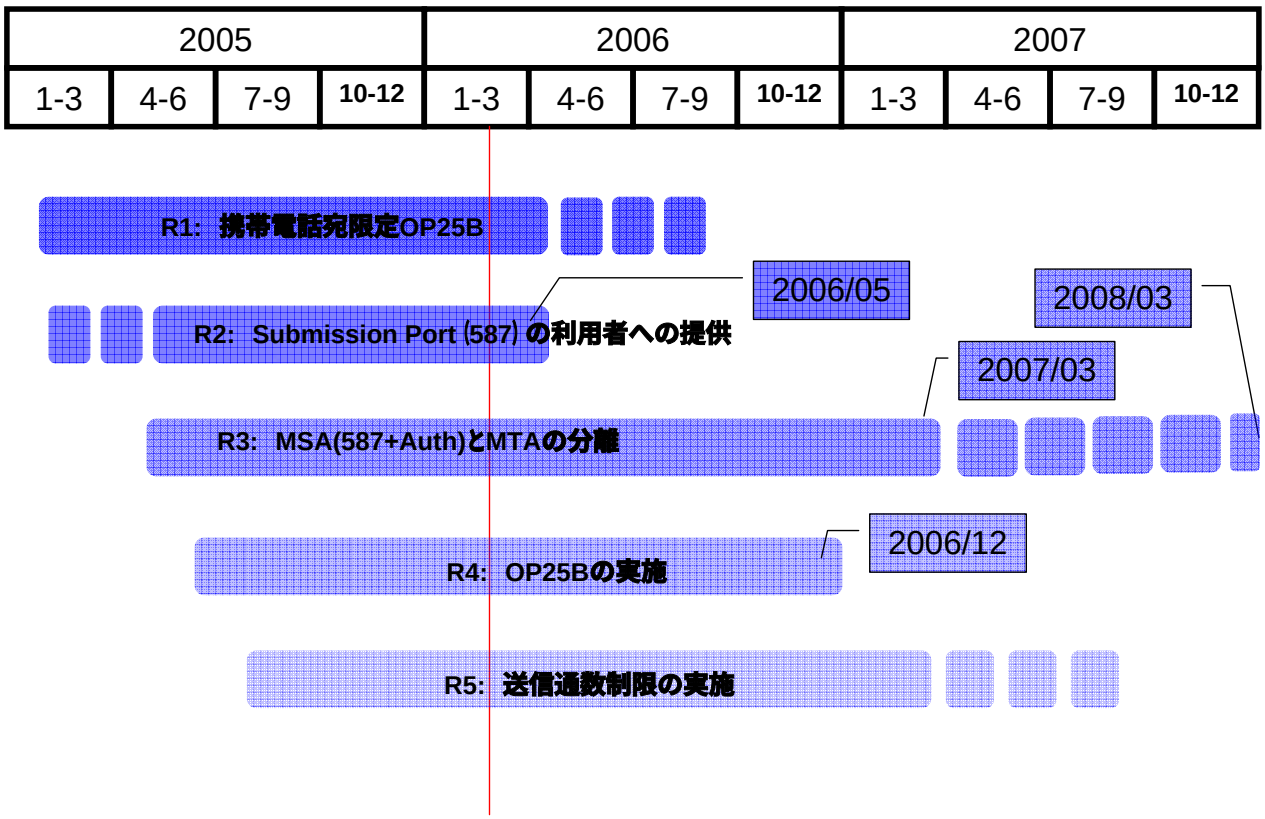
Copyright (c) 2006 JEAG. All rights reserved.

本 Recommendation の到達点



Copyright (c) 2006 JEAG. All rights reserved.

スケジュール



Copyright (c) 2006 JEAG. All rights reserved.

- 正しいメールの到達性を確保する
  → 迷惑メールを止める
- 配送はport 25、投稿はPort 587+Auth
  → MSAでは送信数制限
- 日本からSpamは出さない

Copyright (c) 2006 JEAG. All rights reserved.

- 今日の資料
  http://jeag.jpよりダウンロード可（予定）
  ユーザ名：spamconf　パスワード：antispam
  ※数日、お待ちください

Copyright (c) 2006 JEAG. All rights reserved.