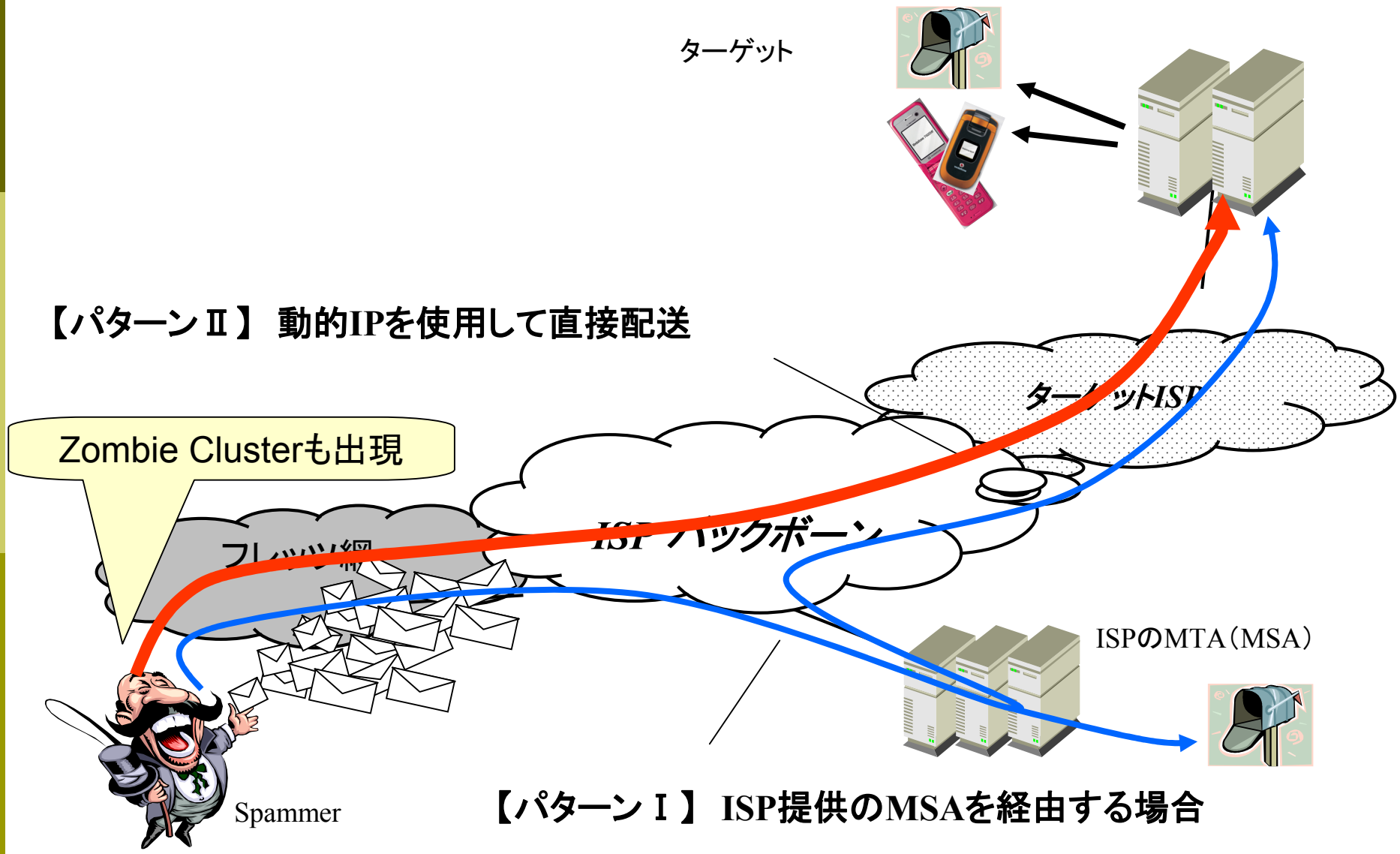
JEAG
Japan Email Anti-Abuse Group

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）

Spamの配送手段の整理



Spamの配送手段の整理

パターンⅠ

ISPの提供するメールサーバをRelayして送信するパターン

⇒ SMTP AUTHを必須として、送信通数制限が有効

パターンⅡ

ISPの提供する動的IPからダイレクトに送信するパターン

⇒ Outbound Port 25 Blockingが有効

パターンⅢ

固定IPを取得して堂々と送信するパターン

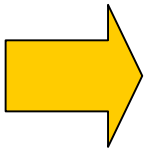
⇒ 今のところ受信フィルタでも対応できる

OP25Bのポイント

OP25Bを実施した場合

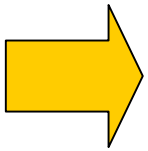
問題点

ISP接続から、動的IPをSourceとした、Destination が25の通信が不可能になる



自分の利用しているISPの外部にあるメールサーバへ25番で投稿できなくなる

Ex) ぷららユーザは hi-hoのMSAが使えない



OP25Bの問題をクリアするためにはこの問題を解決する必要がある

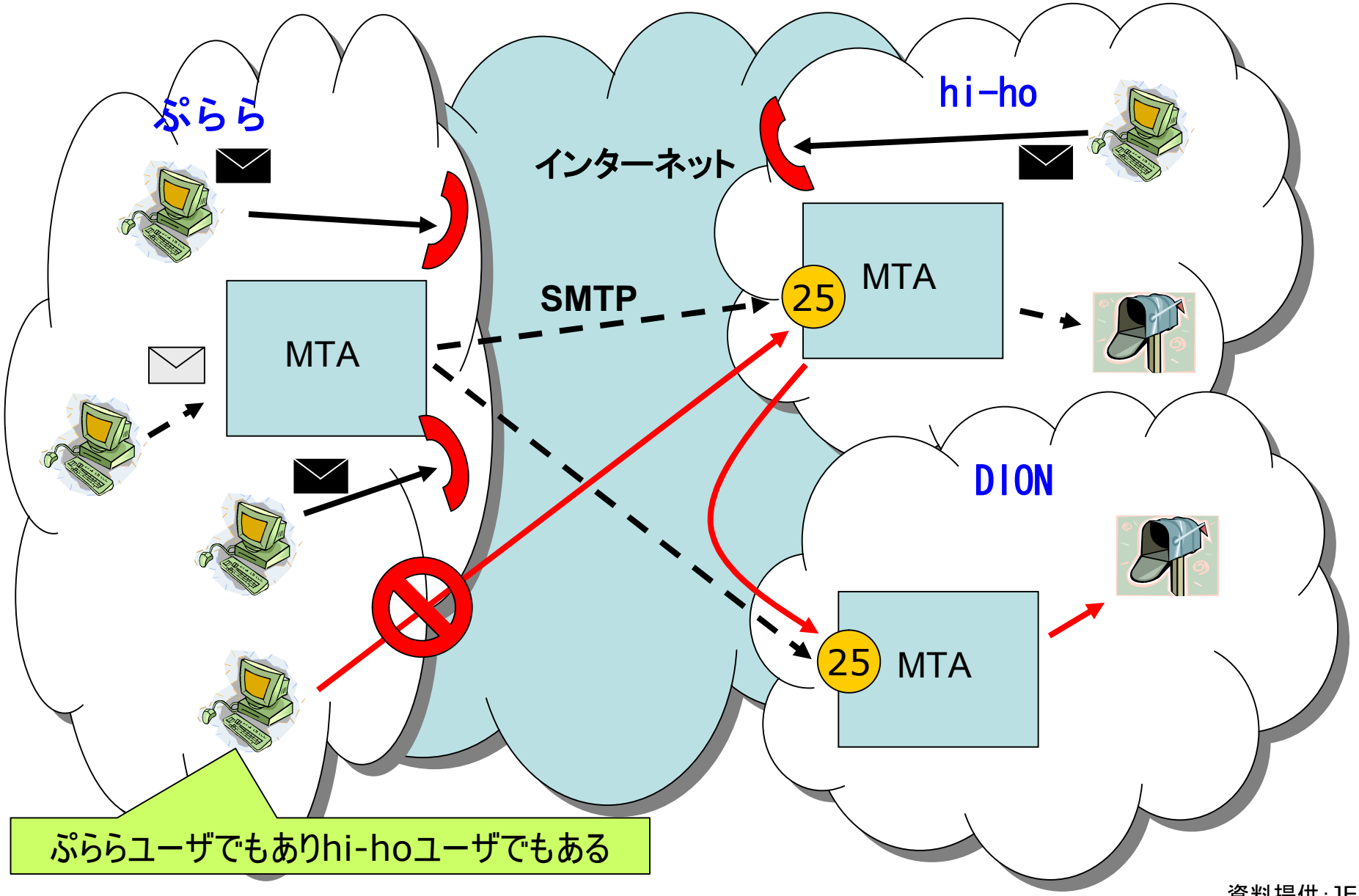
解決策

解決策

MTA（配送サーバ）とMSA（投稿サーバ）の棲み分け

- 投稿は port 587（MSA）、配送は port 25（MTA）
- Port 587 では、SMTP AUTHを必須にする
- MSAでは送信数制限を実施する

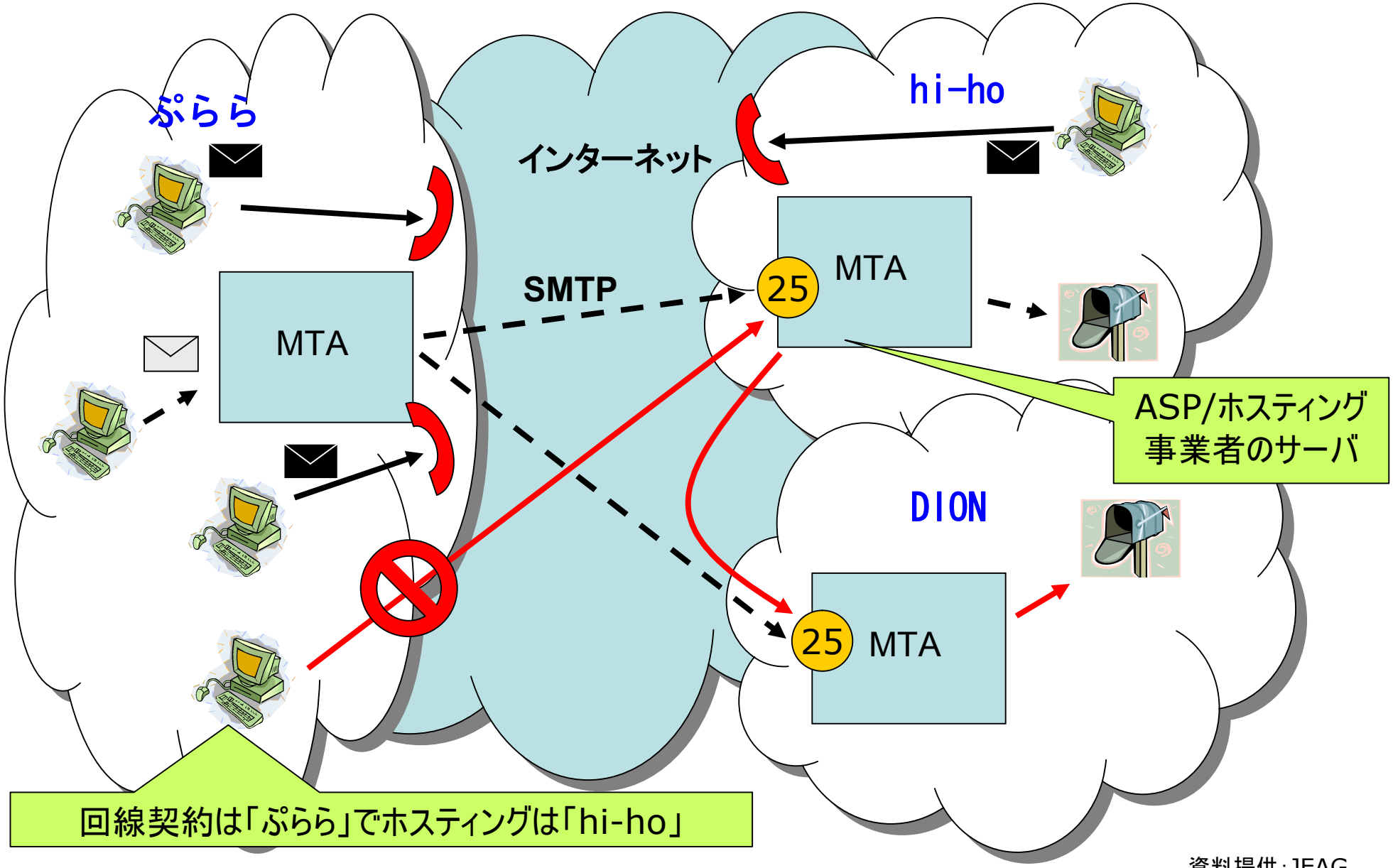
OP25Bの問題点



資料提供:JEAG

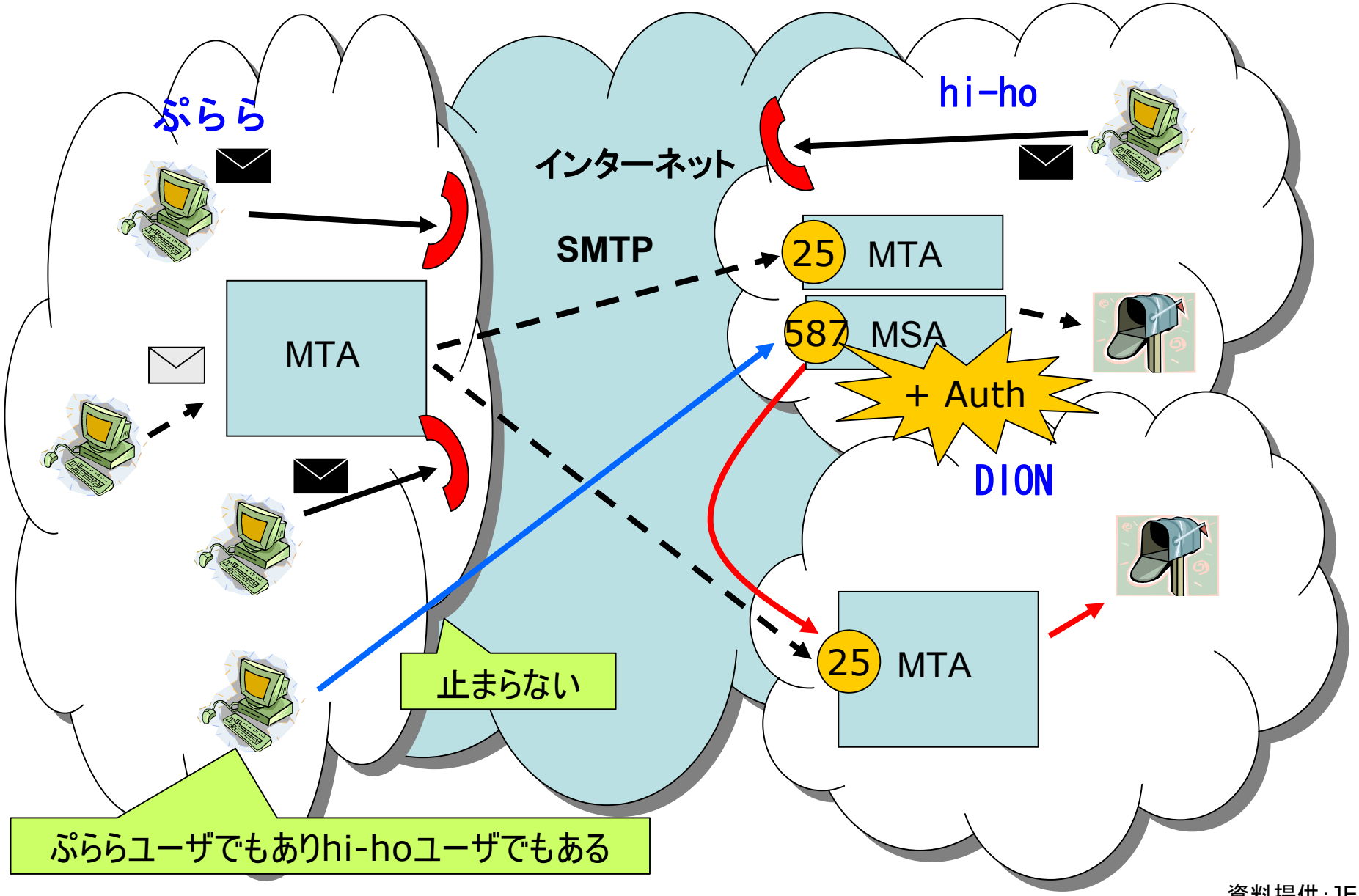
JEAG
Japan Email Anti-Abuse Group

ASPやホスティングでも事情は同じ



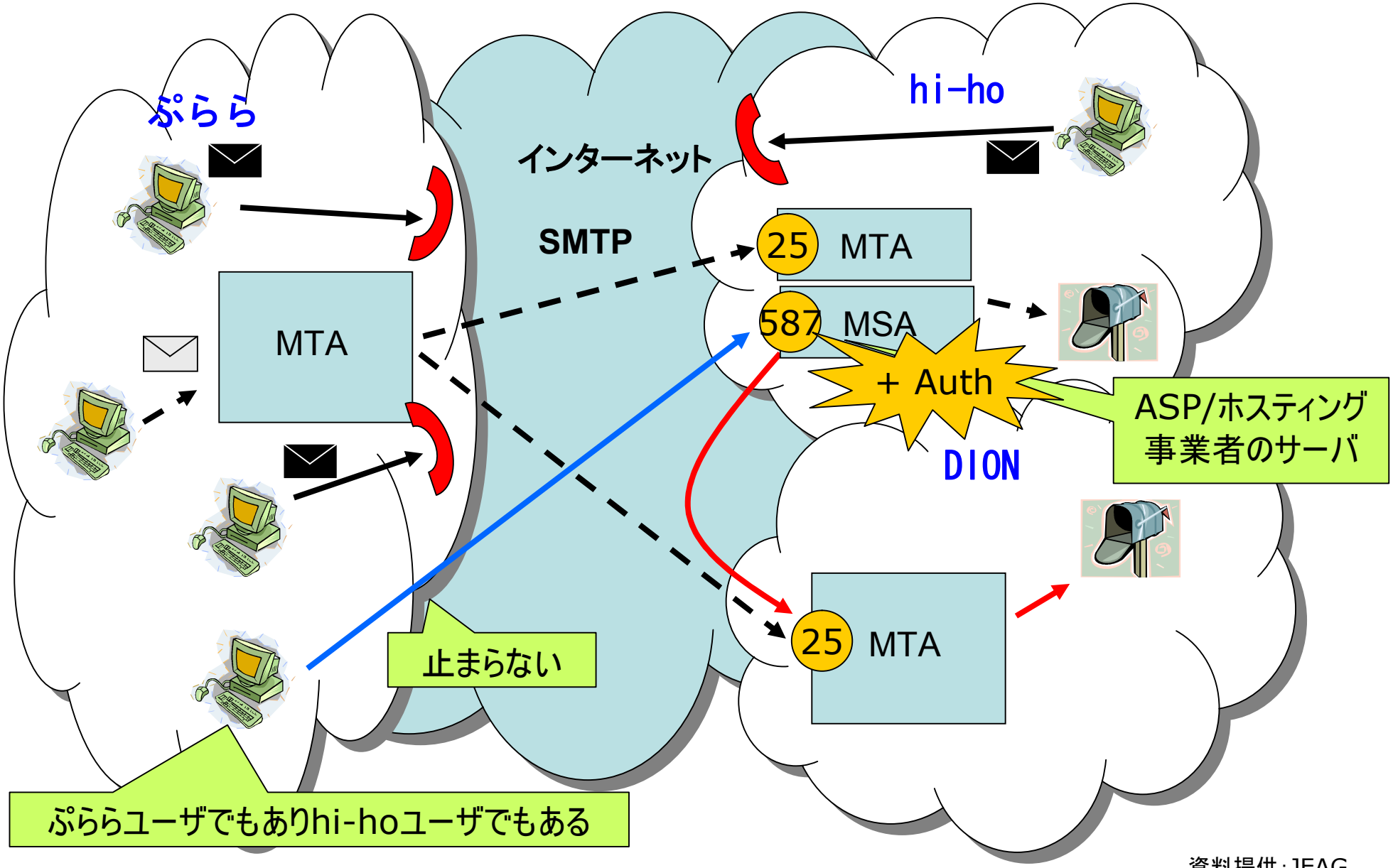
資料提供：JEAG

OP25Bの問題点



資料提供:JEAG

OP25Bの問題点



資料提供：JEAG

JEAG
Japan Email Anti-Abuse Group

マイルストーン

【Goal 1】携帯電話宛限定OP25Bの実施

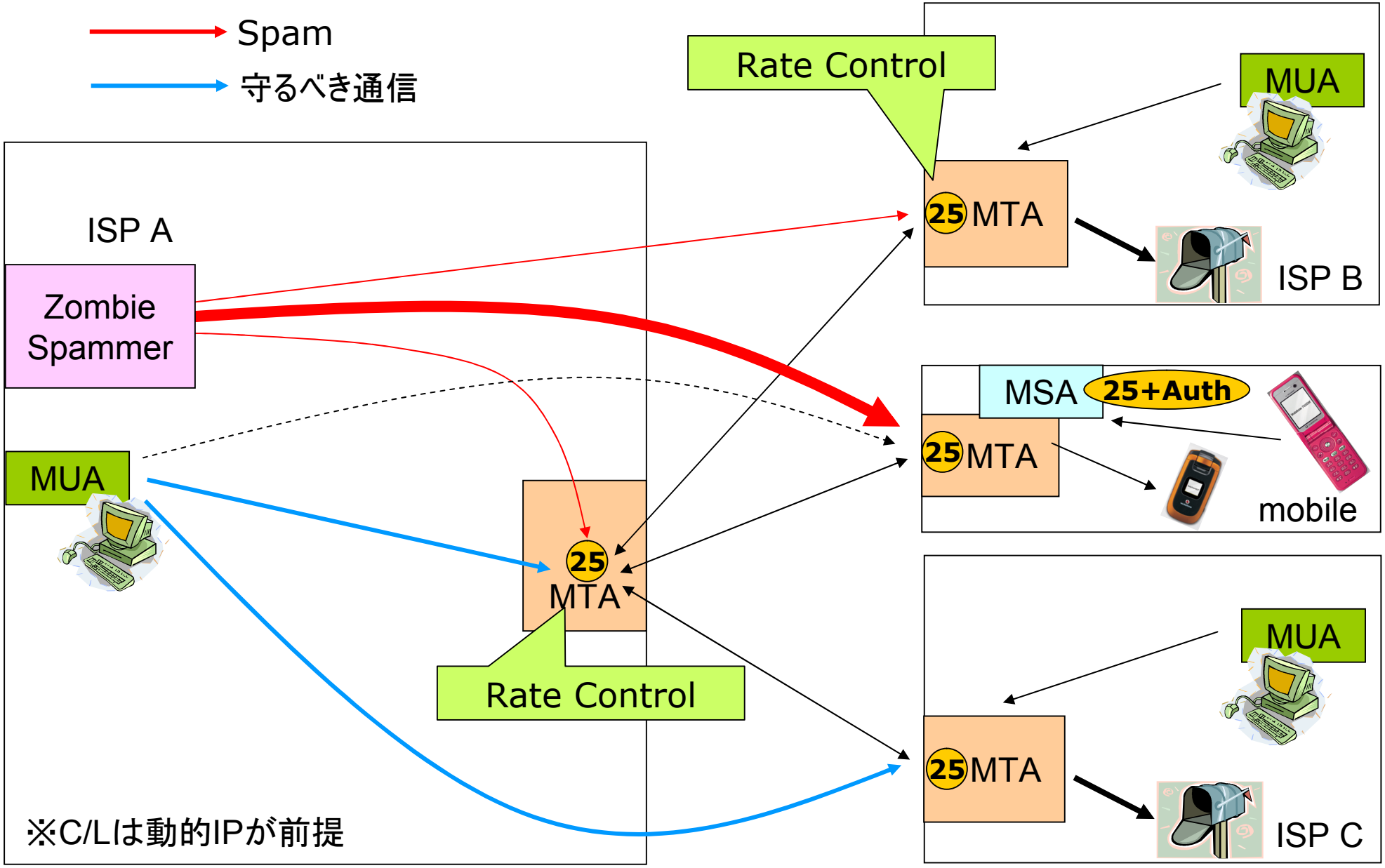
【Goal 2】Message Submission (587)の普及

【Goal 3】MTAとMSAの棲み分け

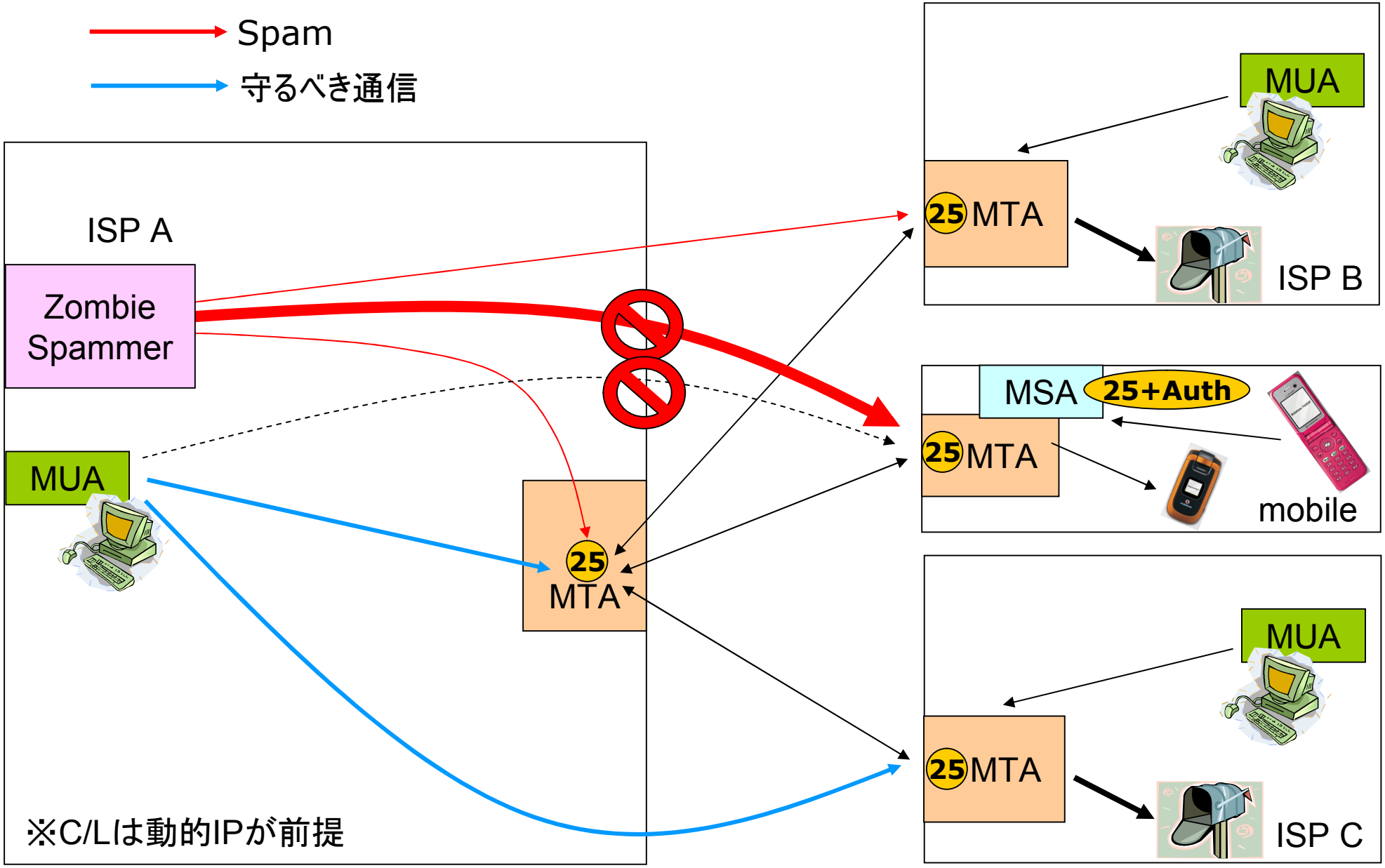
【Goal 4】Outbound Port 25 Blockingの実施

【Goal 5】SMTP Authによる通数制限の実施

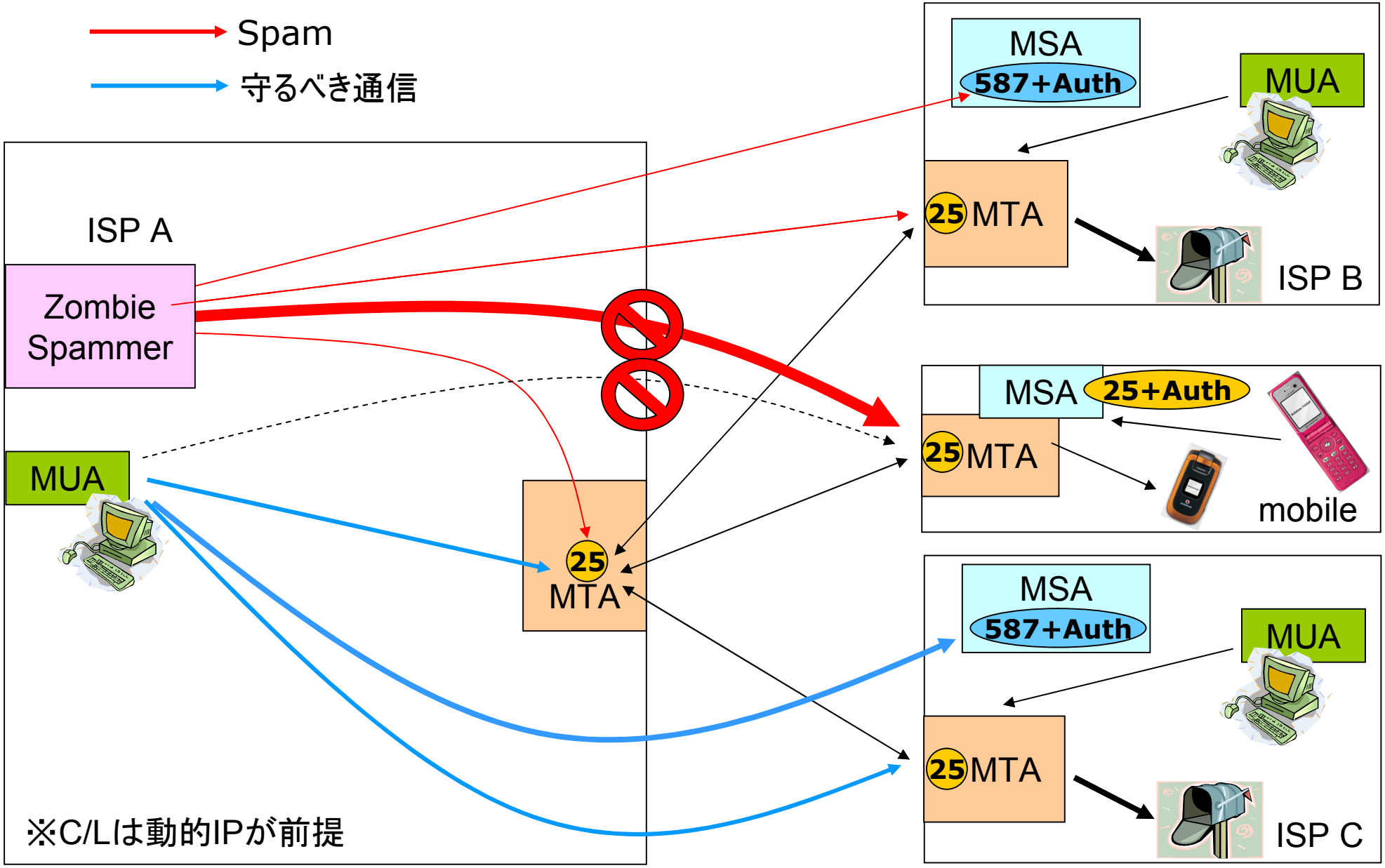
動的IPをSourceとしたSpamの配送経路



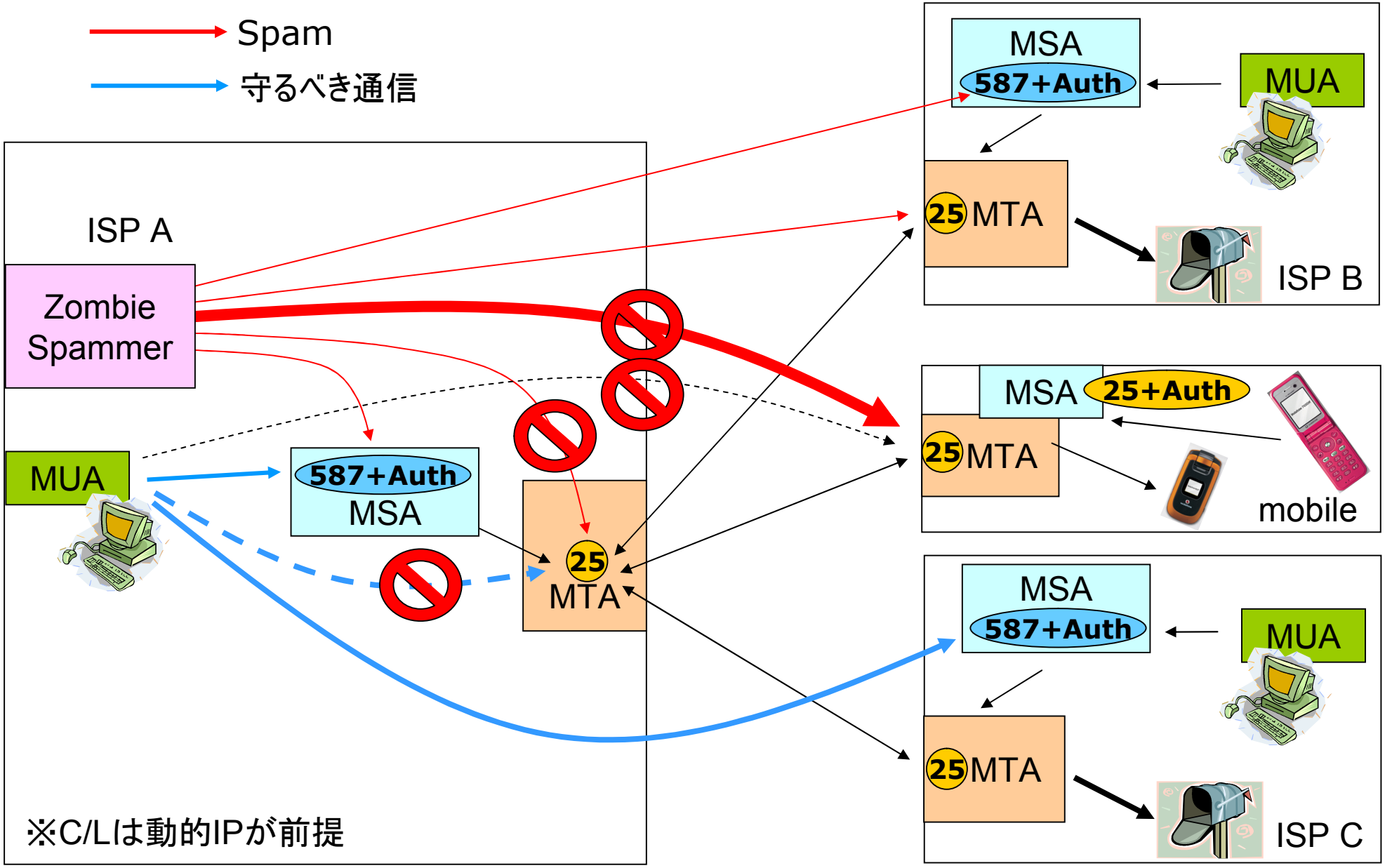
GOAL1：携帯宛限定OP25B



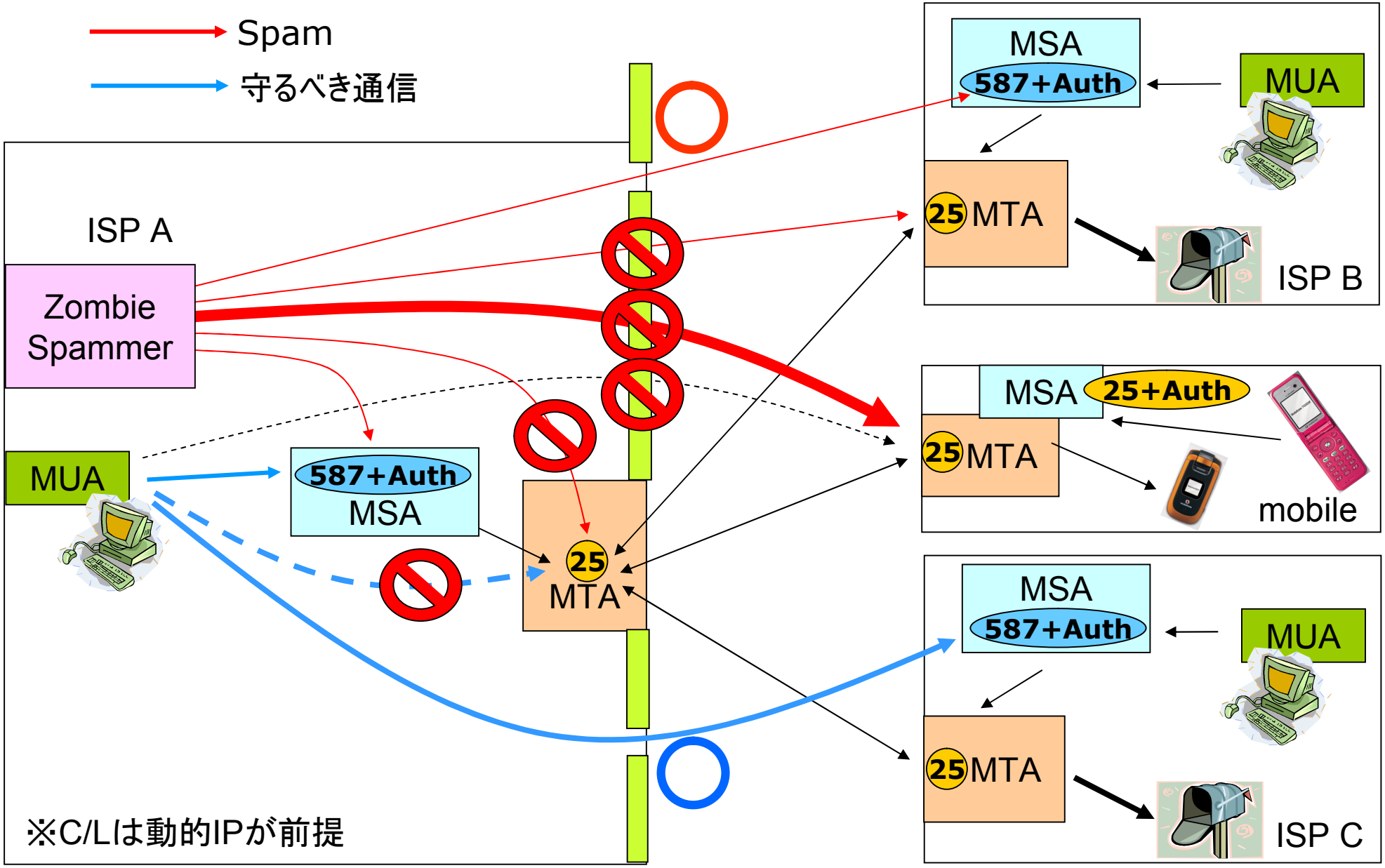
Goal 2 : Message Submissionの普及



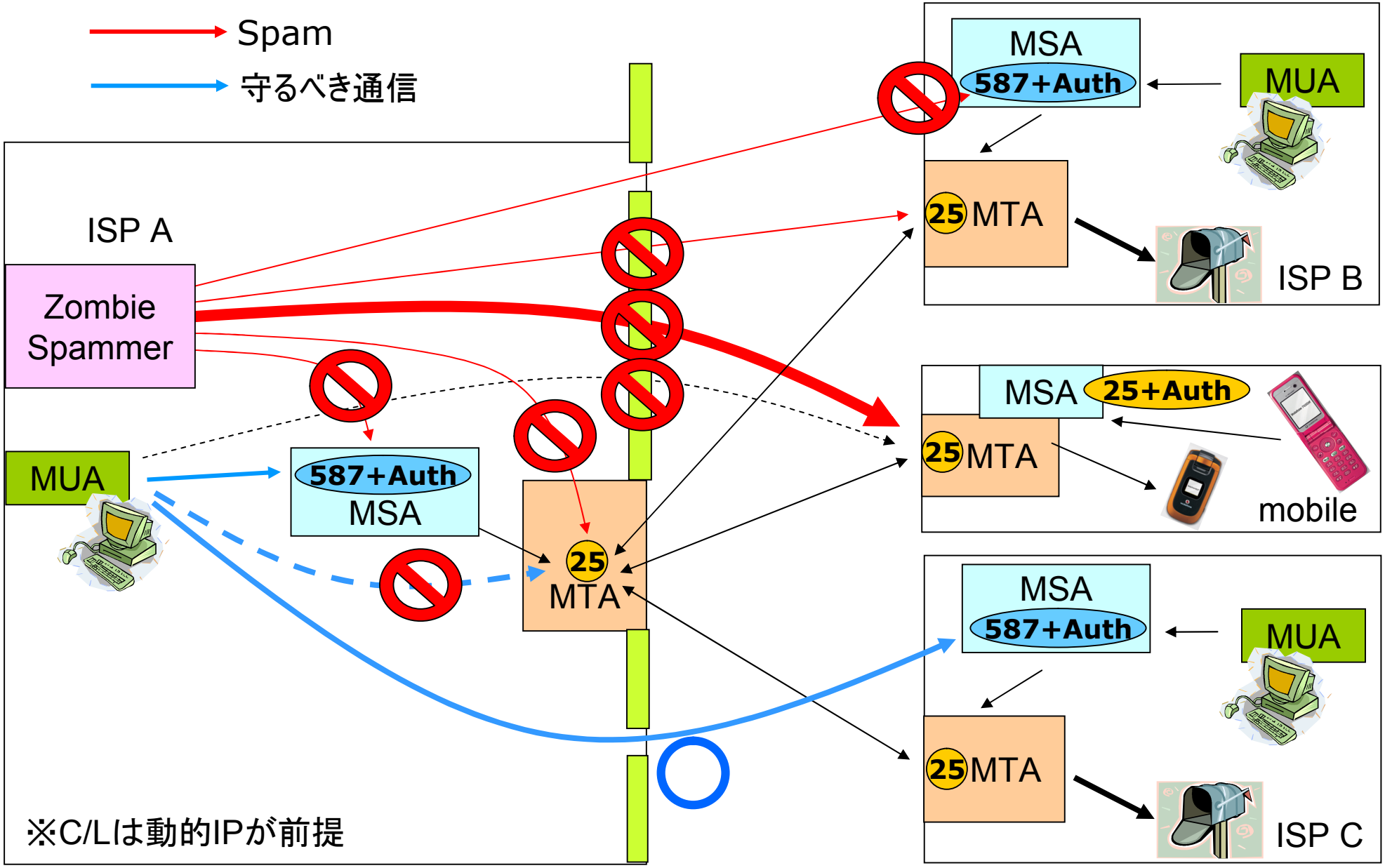
Goal 3：MTAとMSAの棲み分け



Goal 4 : Outbound Port 25 Blockingの実施

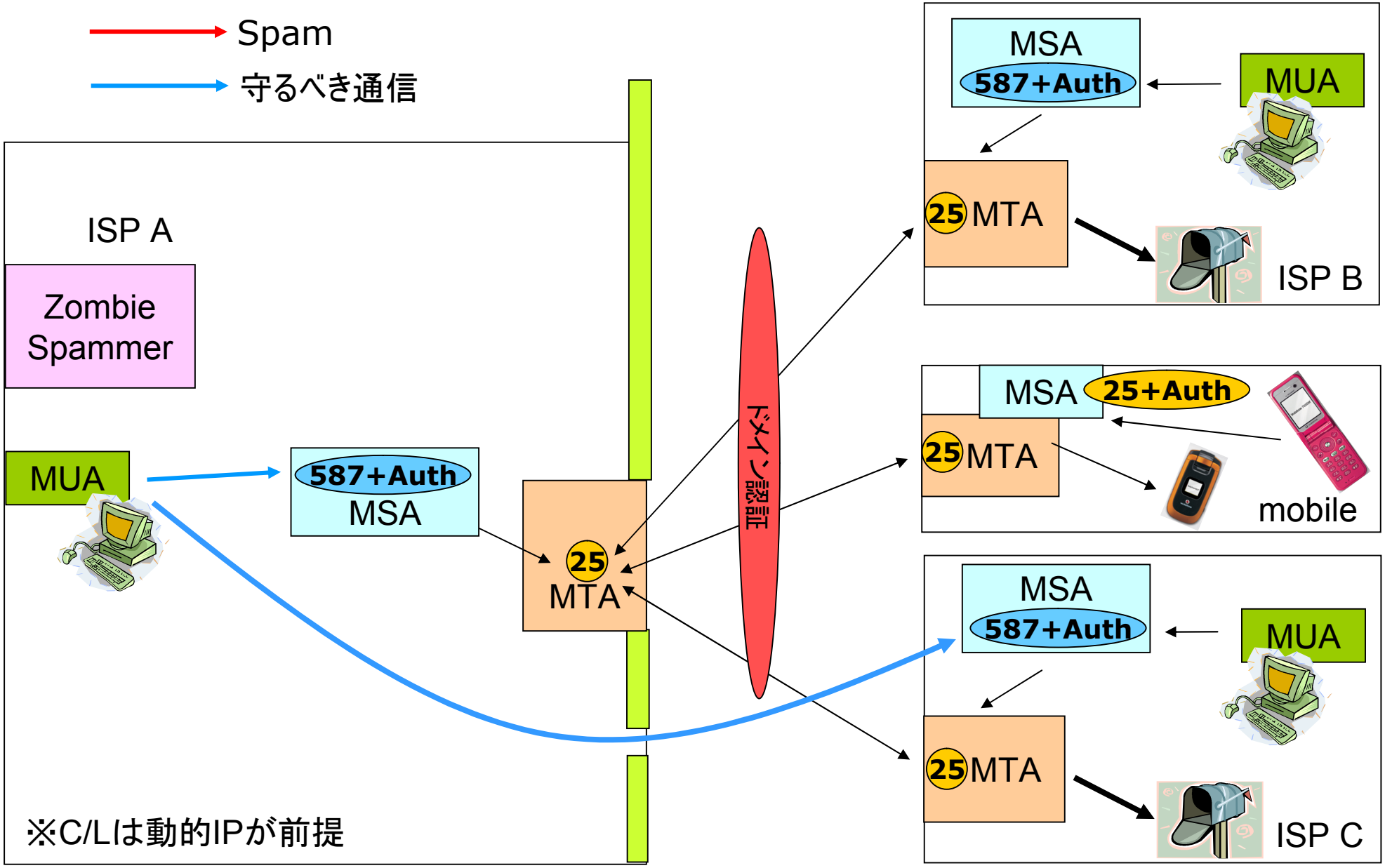


Goal 5：SMTP Authによる通数制限

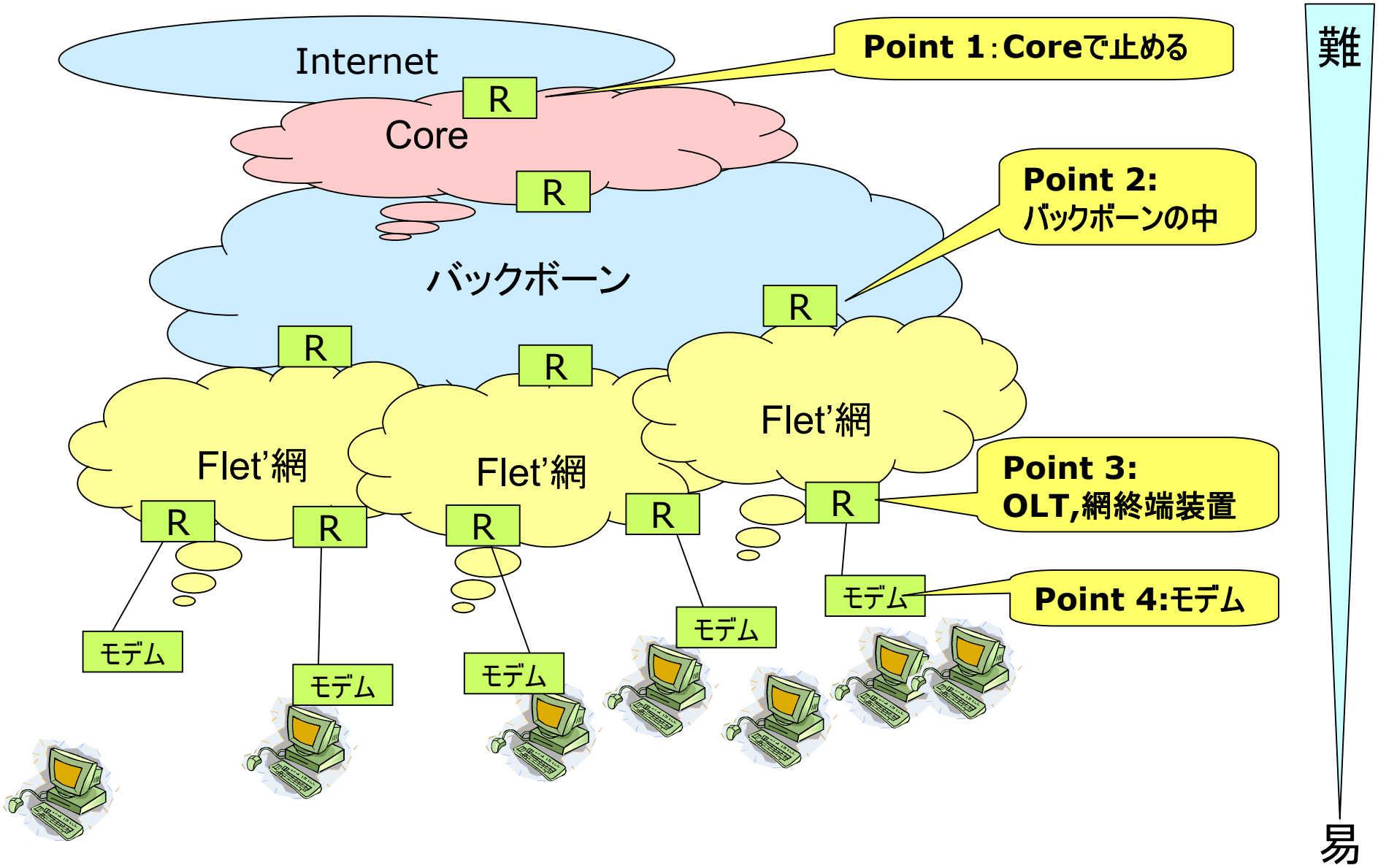


JEAG
Japan Email Anti-Abuse Group

参考：ドメイン認証



Blocking Pointについて



JEAG
Japan Email Anti-Abuse Group

それぞれの特徴

Point 1 : Core

- L2のNetworkを利用しているISPに多く、Blocking Pointは1箇所。ハイリスク。
- すべてトラフィックを捌くので高価なルータが必要

Point 2 : バックボーン

- クラシックなパターン。Blocking Pointが全国に散る。
- 2次ISPを抱えていることが多い

Point 3 : OLT,網終端装置

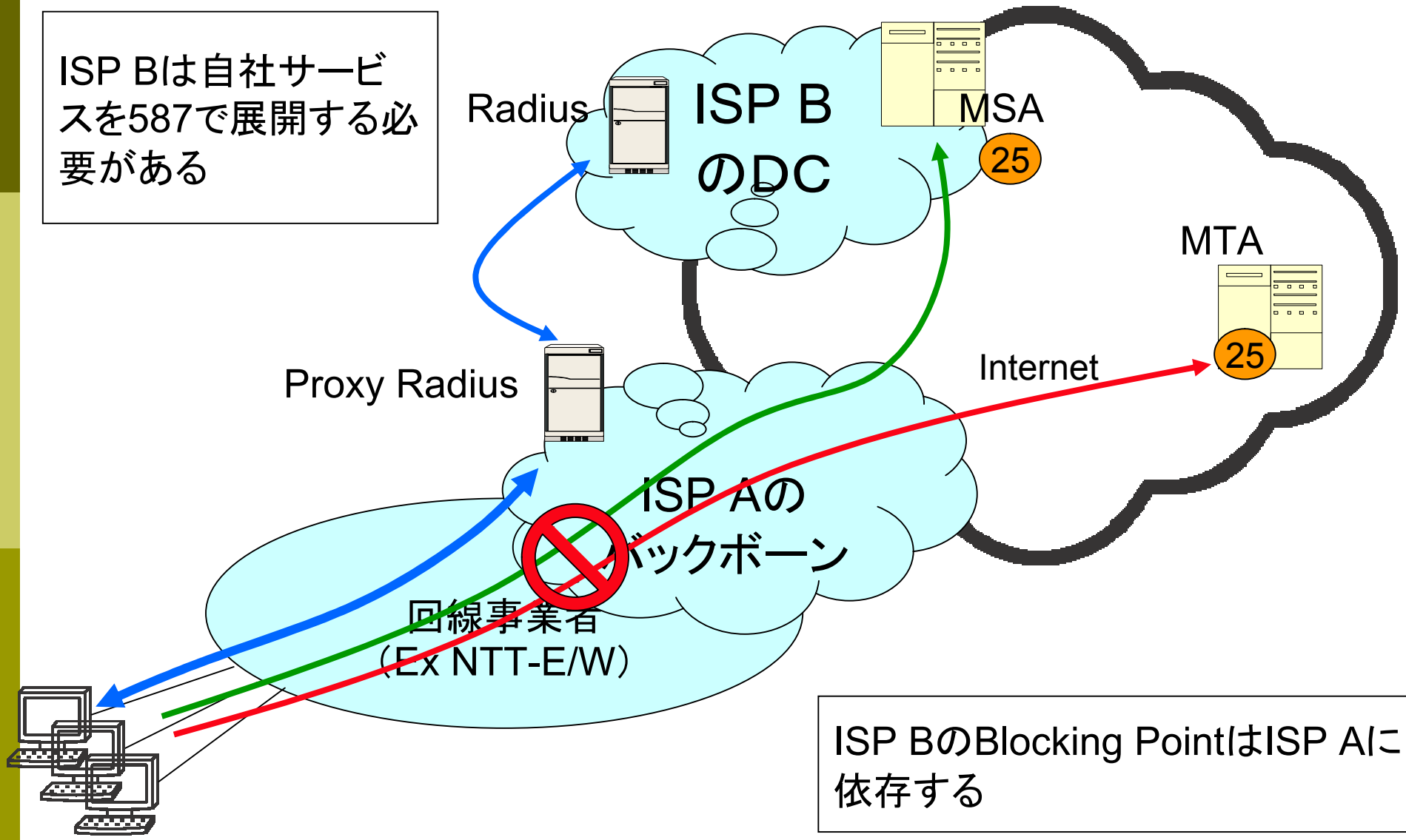
- 回線提供事業者側の装置でBlockする。アメリカではメジャーな方法。
- 日本の場合、NTT東西に依るところが多いのと、法律・制度的に厳しい。

Point 4 : モデム

- CATV事業者に多い。ファームをセンタからControlできる。
- ここでBlockできるのが一番楽。

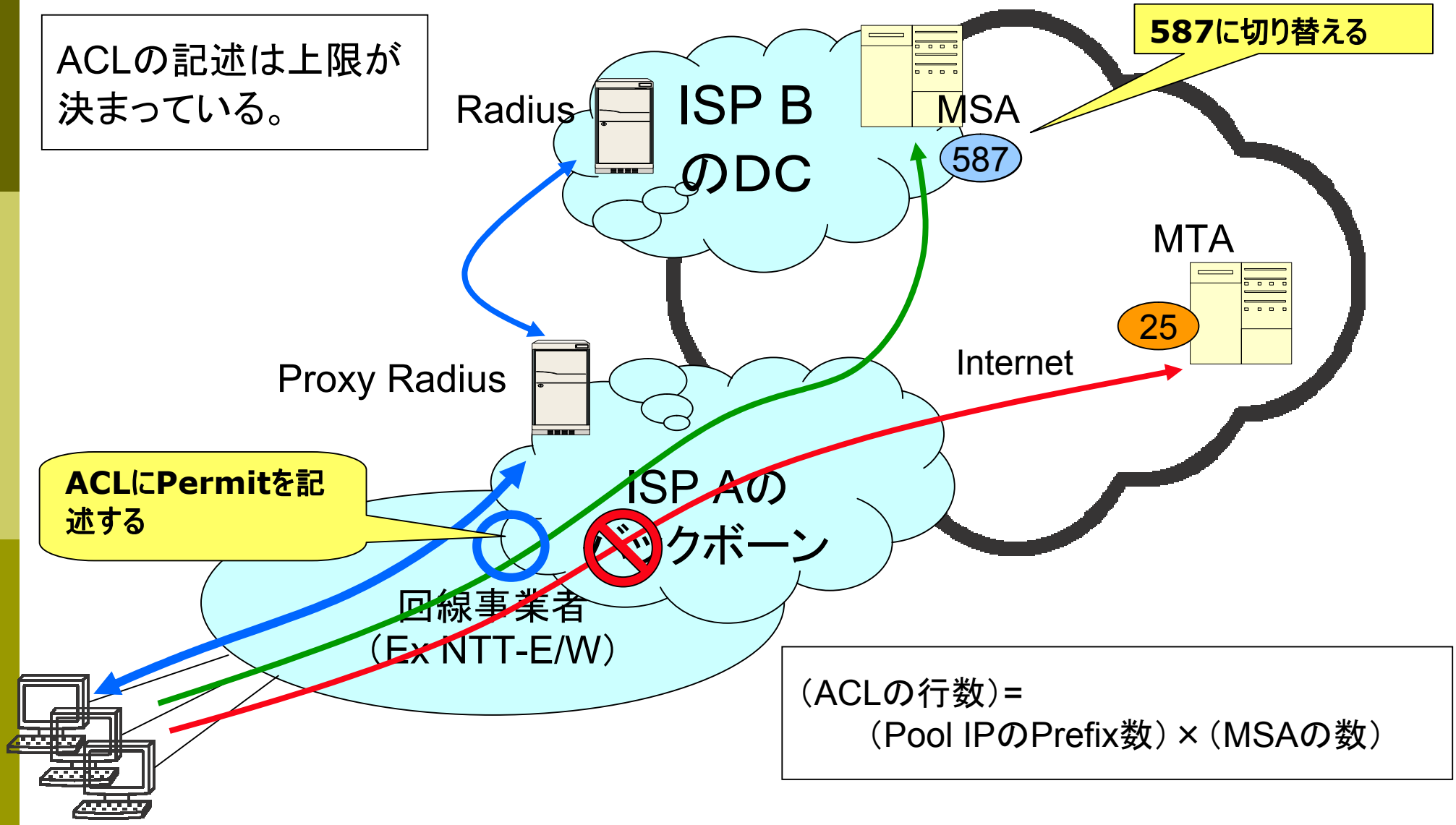
Point 5 : 上位のISP

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

Point 5：上位のISP（回避策）



Point 5

Point 5 : 上位のISP

- 逆引きが、1次側の場合と、2次側の場合がある
  -> 1次側の場合は、2次側を区別できないので1次側のポリシーと合わせる
  -> 2次側の場合は、区別は可能だが、1次側のACLが爆発する
- 2次ISPは自社ユーザを587に移行しなくてはならない
  -> MSAを上位ISPのCoreにおけば回避は可能

1次ISPからOP25Bの依頼があったら協力をお願いします

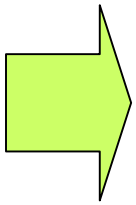
m(_ _)m

Point 5：上位のISP（回避策）

1．上位ISP側でACLにてPermitする

2．上位ISPの指定したPrefixへMSAを移動する

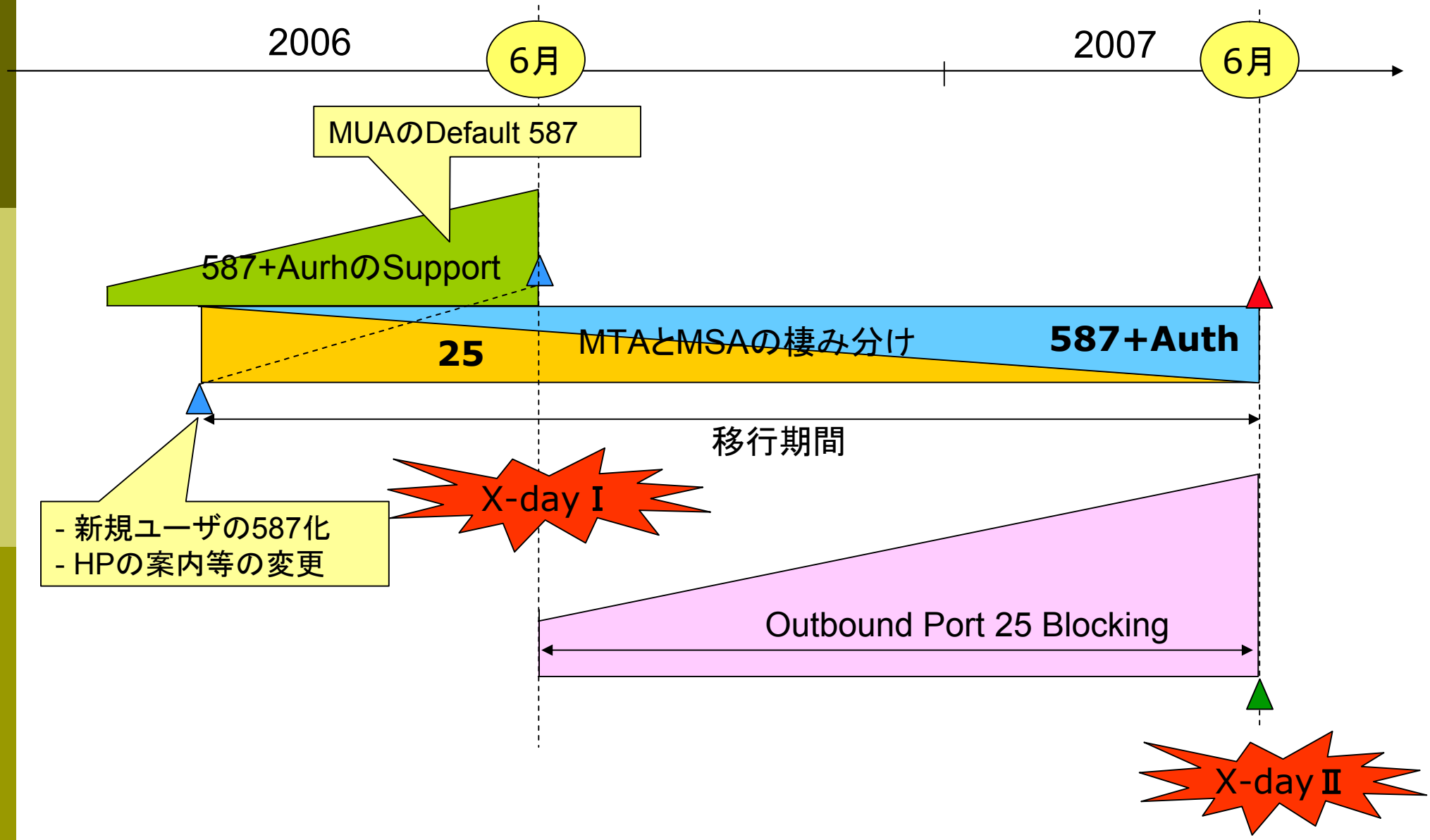
3．全ユーザ587+Authを利用してもらう



これらの組み合わせで実施

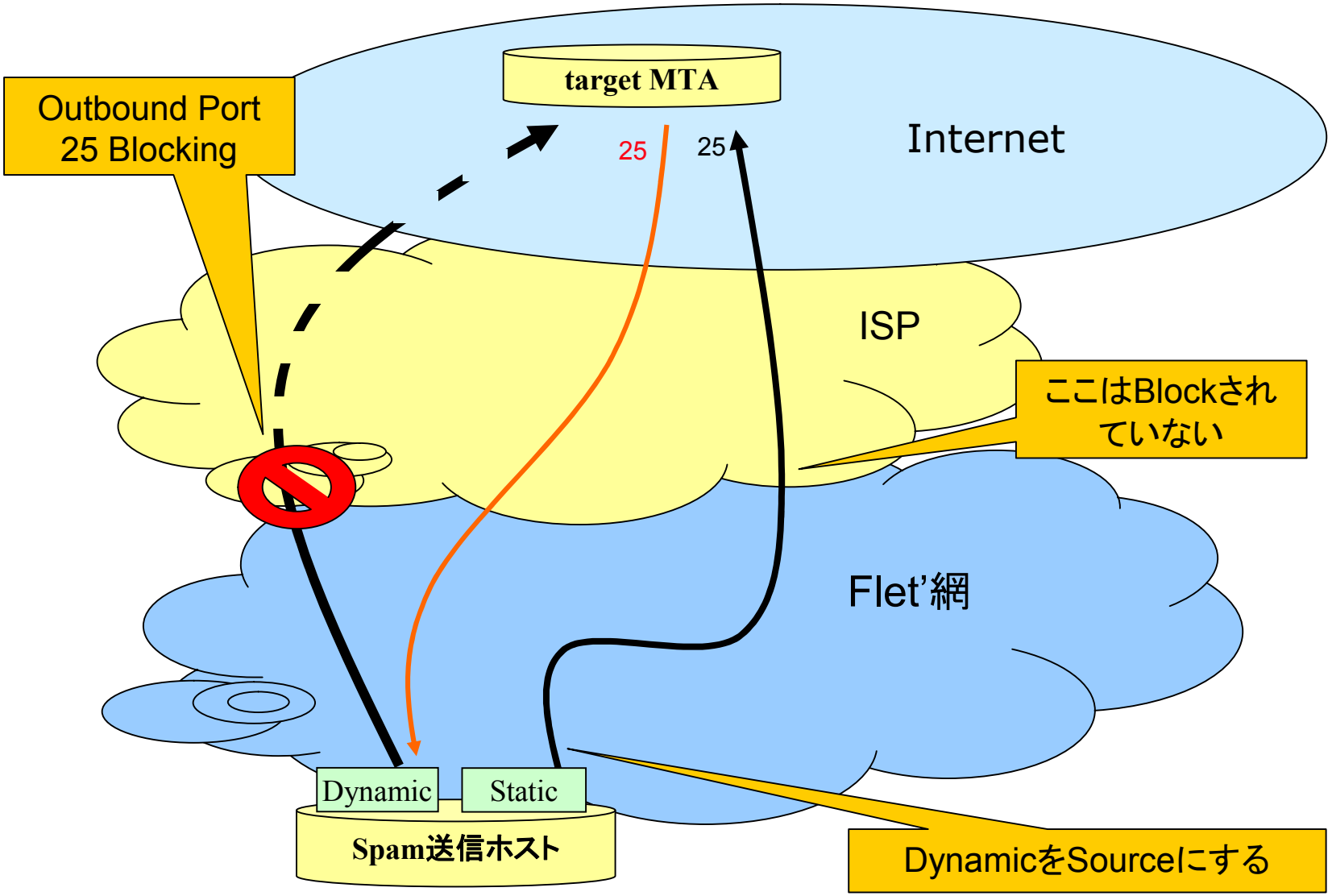
JEAG
Japan Email Anti-Abuse Group

ロードマップ（X-dayの設定）



JEAG
Japan Email Anti-Abuse Group

Asymmetric routing attack



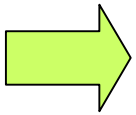
Asymmetric routing attack

1. Spam送信ホストは動的IPをSourceとしてメール固定IPからメールを送信する。
2. 応答は動的IP経由で戻ってくる。

   Source:25 Destination:1025
3. 固定IPはOP25Bの対象外のため、Source IPを動的IPとしたまま送信が可能
4. これを防ぐためにはISP側にて以下をBlockする必要がある。

   Source　　:External :25

   Destination　:Dynamic IP,Any



Inbound Port 25 Blocking

（補足スライド）参考：動的IPのMTA