OP25B の後の spam 対策
～MSA の踏み台問題～

赤桐壮人
楽天株式会社

加瀬正樹
ニフティ株式会社

加藤理人
ビッグローブ株式会社

Janog34

混ぜる

1. ちょっと垂らす (5分)
2. そっと混ぜる (15分)
3. かき混ぜる (10分)
4. こぼす (10分)

ちょっと垂らす

メール関係の団体の紹介

- M3AAWG
  - 2003.11 アメリカで発足した Anti-spam の団体
  - 現在は、Messaging, Mobile, Malware
- JEAG
  - 2005.2 発足、自然消滅、すでに web もない
  - OP25B を推進した団体
- dkim.jp
  - 2008.11 発足 2013.5 close
  - DKIM の普及率 40% 達成 (流量比)

DMARC

みなさん DMRAC を宣言しましょう

```
$dig _dmarc.nifty.com txt
_dmarc.nifty.com          IN   TXT"v=DMARC1\; p=none”
```

(その他の例)

```
$ dig _dmarc.aol.com txt +short
"v=DMARC1\; p=reject\; pct=100\; rua=mailto:d@rua.agari.com\; ruf=mailto:d@ruf.agari.com
\;”

$ dig _dmarc.yahoo.com txt +short
"v=DMARC1\; p=reject\; sp=none\; pct=100\; rua=mailto:dmarc-yahoo-rua@yahoo-inc.com,
mailto:dmarc_y_rua@yahoo.com\;"

$ dig _dmarc.gmail.com txt +short
"v=DMARC1\; p=none\; rua=mailto:mailauth-reports@google.com”
```

今後、デファクト化の気配

DMARC

導入状況

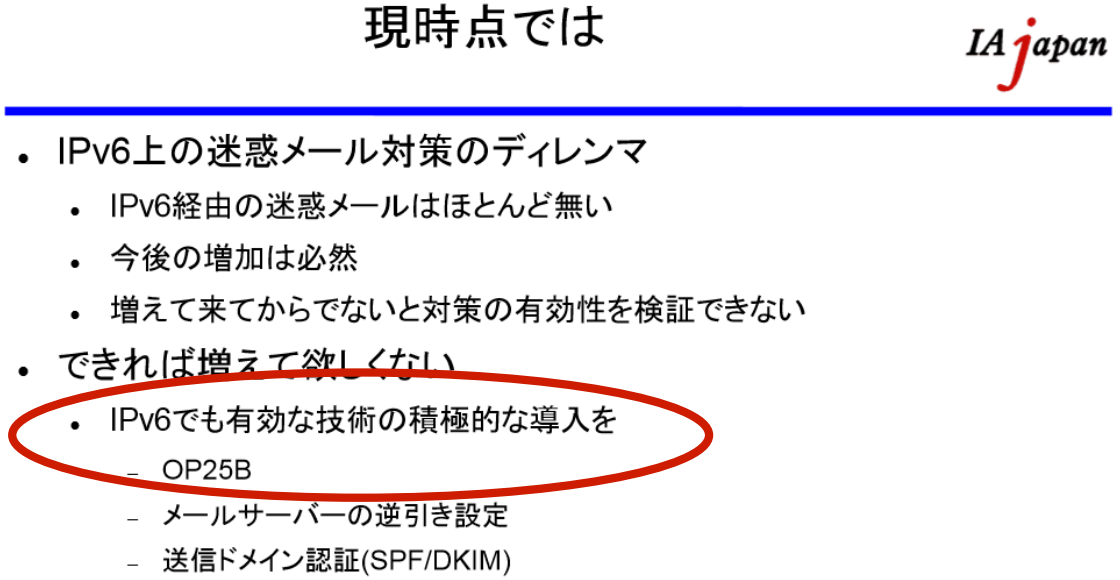
	ISP	対応状況	備考・updates
1	ニフティ	◯	none
2	BIGLOBE	◯	とりあず、会社ドメイン（none）
3	楽天	◯	none
4	Infoseek	◯	7/14サービスドメイン対応（none）
5	Yahoo!	◯	一部サービスドメイン対応（**quarantine**）
6	IIJ	◯	none
7	DTI	◯	none
10	CNCI	◯	none
11	K-opti.com	予定	7 月下旬

※ 赤桐、加瀬、加藤調べ。一部でも対応していれば ◯ としてカウント。間違いはあるかもしれません。

持ち帰って社内調整お願いします！

IPv6 の OP25B

- ✓ IPv4上でのOP25Bは2005年～2006年ごろ各社対応完了
- ✓ 25/tcp 遮断は影響もあったがそれ以上に導入効果も大
- ✓ IPv6普及に伴い**IPv6 の OP25B も必要**



＜2011年5月 第9回迷惑メール対策カンファレンスより引用＞

Janog とメール

『汚れたIPv4アドレスのクリーニングについて考えよう』

迷惑メール送信でIPが汚れる

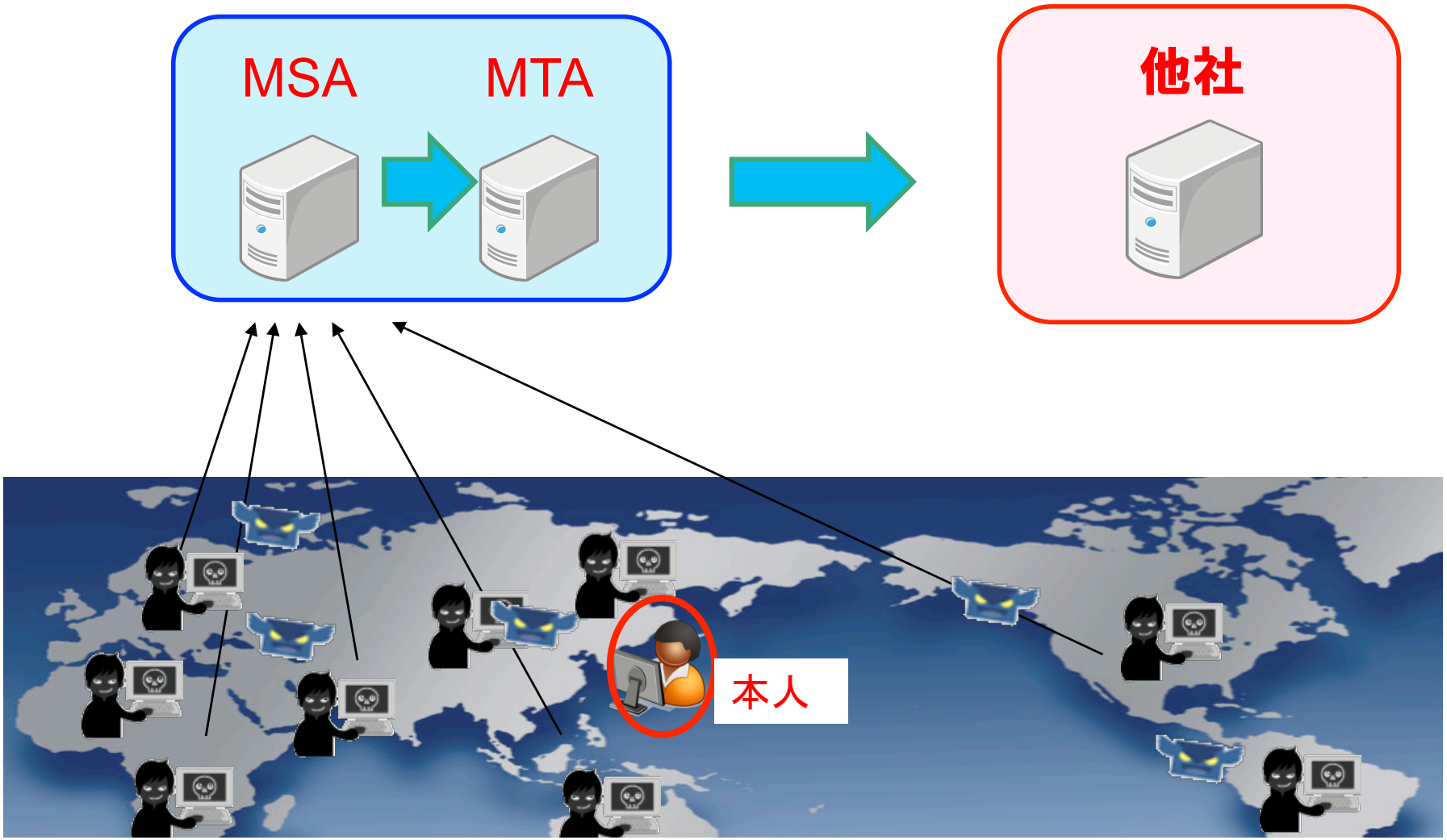
(BlackListにのったIPからはメール届かない)

迷惑メールを送信している会員がいる？

NEW

本人以外がアカウント悪用して送信しているようだ

本人以外の送信とは

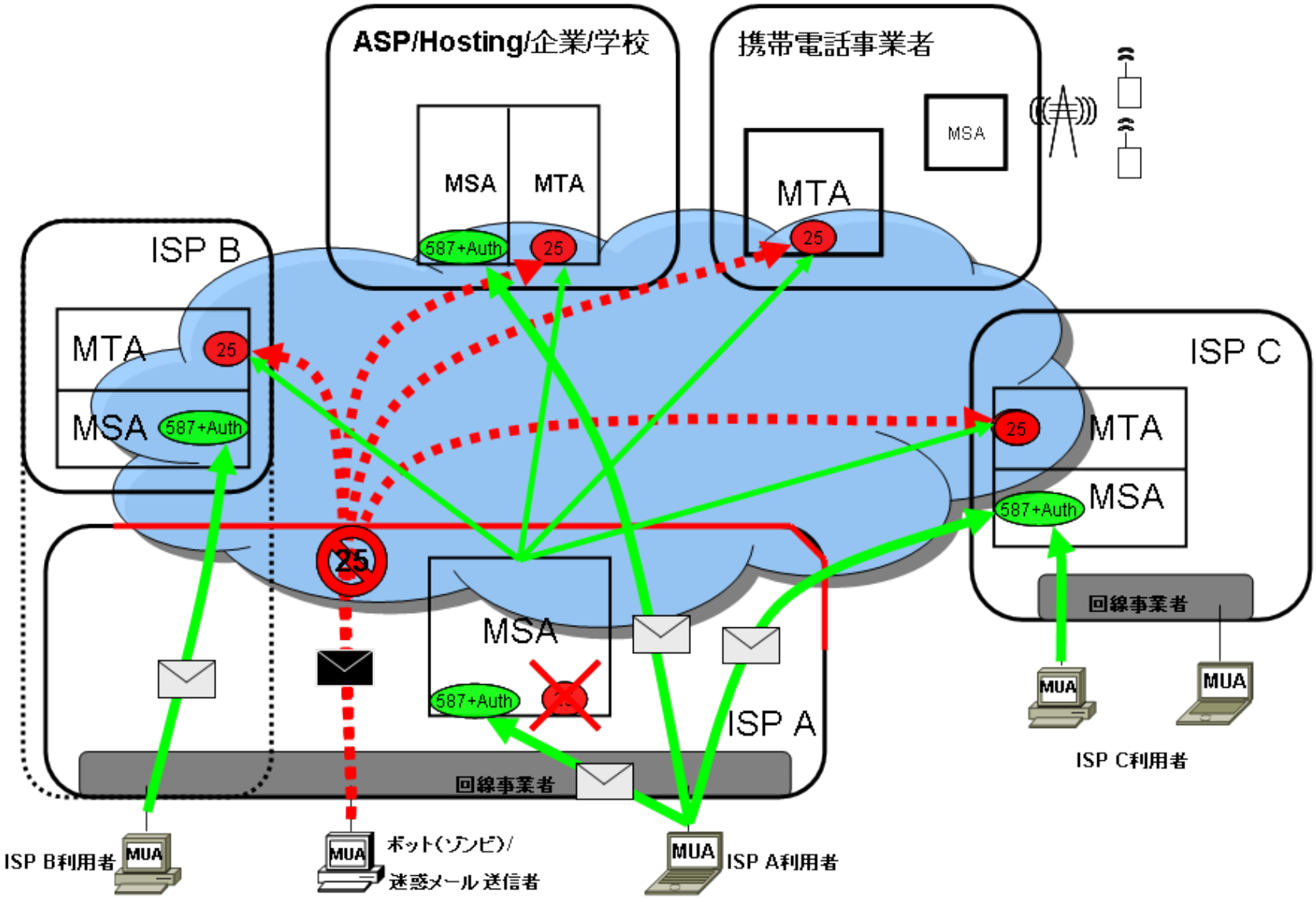


本人でない誰かがアカウントを悪用して送信

そっと混ぜる

OP25B の後の spam 対策

OP25B で想定していた世界



対策のポイントを MSA (Outbound MTA) に集中

OP25B で想定していた世界

- 廃止
  - 第三者投稿
  - POP before SMTP
  - Non auth MSA

- 対策ポイントを MSA(587) の SMTP AUTH に集中する
  - SMTP AUTH + AUTH ID basis の送信量コントロールまで想定

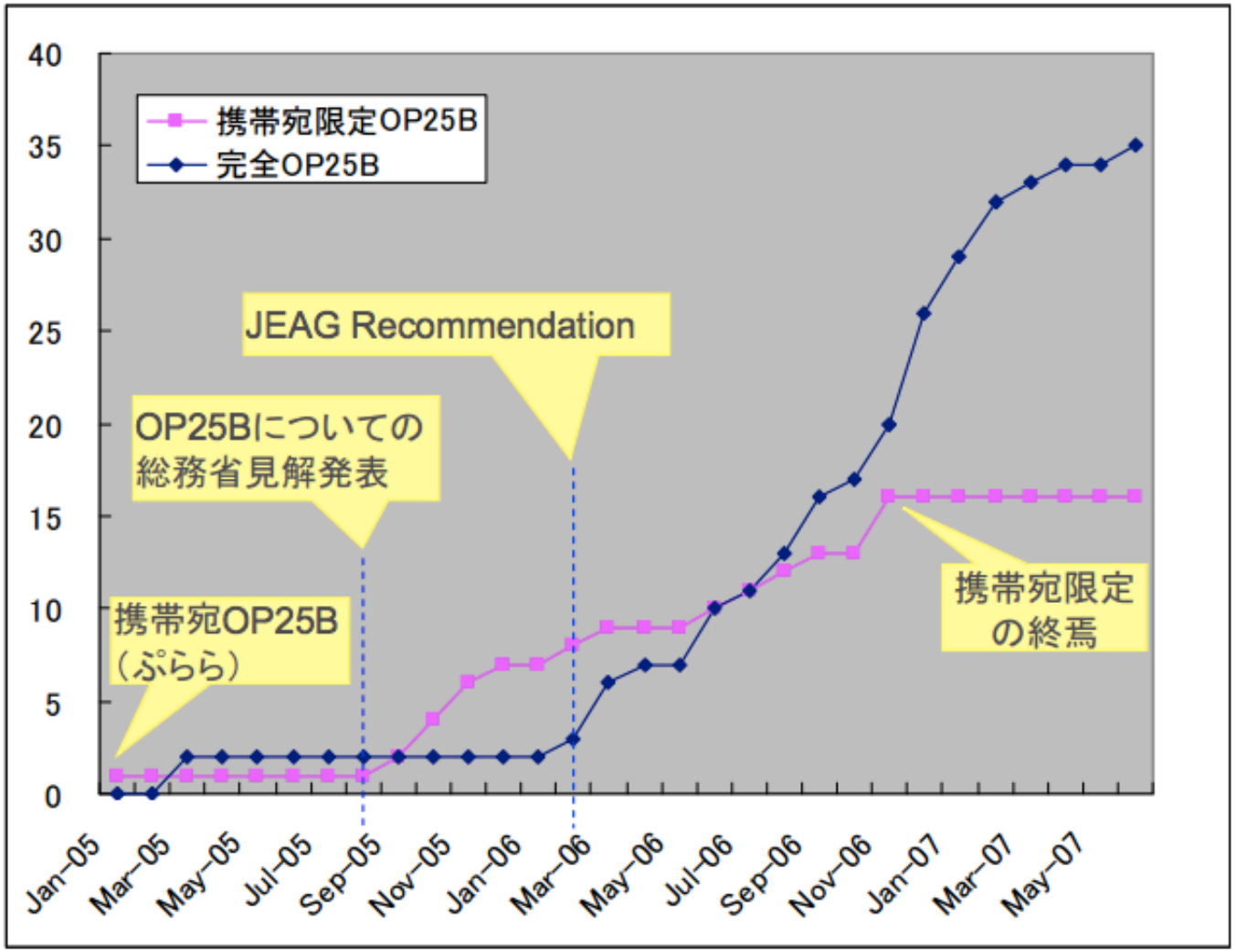
Spammer が MSA を踏み台にすることまでは想定

OP25B の効果1

統計情報
当日のみ公開

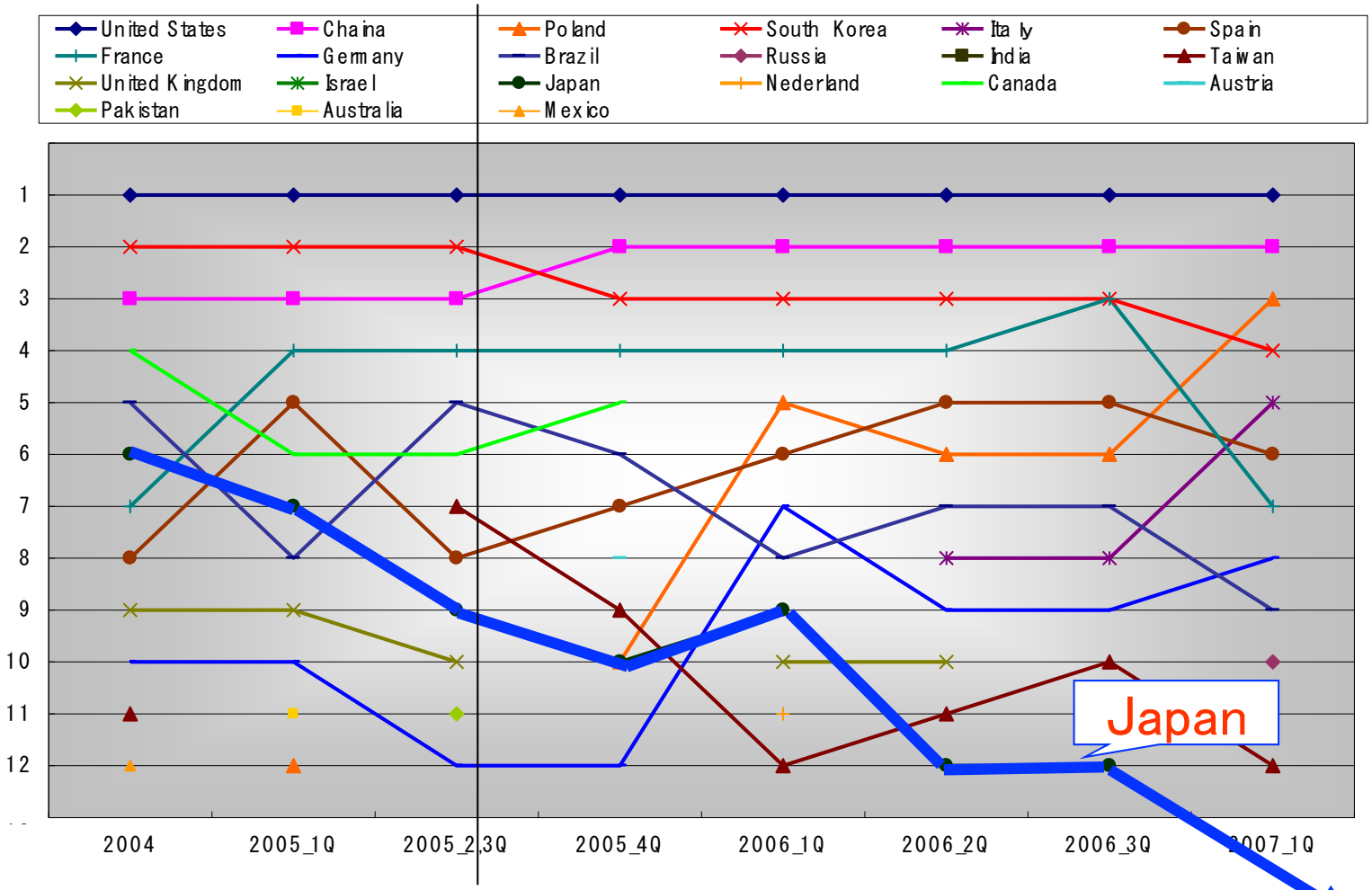
自社動的IP発の spam は完全に止められる

OP25B の普及状況



2005年9月あたりから一気に普及

OP25Bの効果2 (国別spam送信数ランキング)

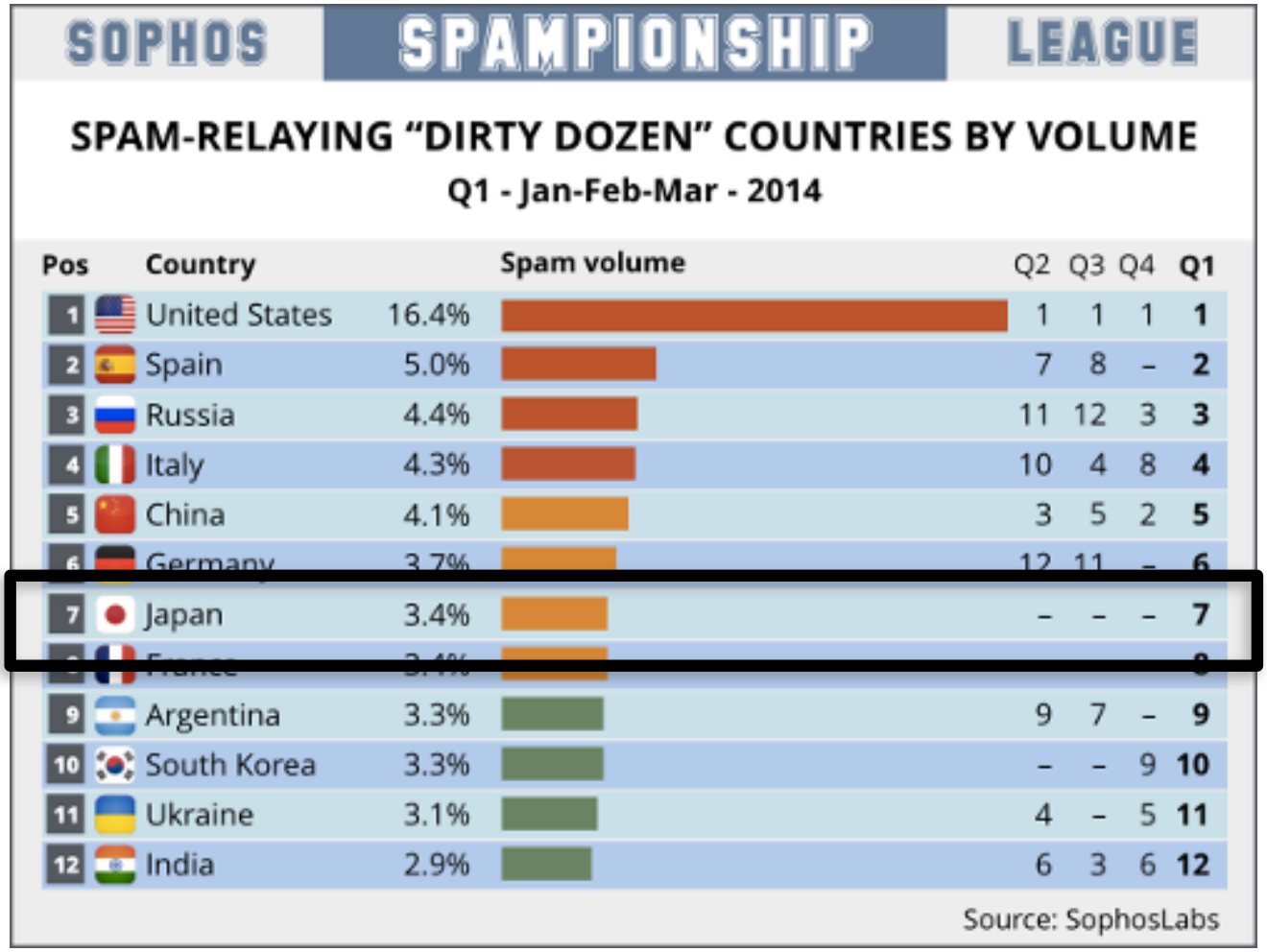


2005.9

Rank 33, 0.60% on Feb 2010

http://www.sophos.com

現状



SOPHOS SPAMPIONSHIP LEAGUE

SPAM-RELAYING "DIRTY DOZEN" COUNTRIES BY VOLUME

Q1 - Jan-Feb-Mar - 2014

Pos	Country	Spam volume	Q2	Q3	Q4	Q1
1	United States	16.4%	1	1	1	1
2	Spain	5.0%	7	8	–	2
3	Russia	4.4%	11	12	3	3
4	Italy	4.3%	10	4	8	4
5	China	4.1%	3	5	2	5
6	Germany	3.7%	12	11	–	6
7	Japan	3.4%	–	–	–	7
8	France	3.4%				8
9	Argentina	3.3%	9	7	–	9
10	South Korea	3.3%	–	–	9	10
11	Ukraine	3.1%	4	–	5	11
12	India	2.9%	6	3	6	12

Source: SophosLabs

http://www.sophos.com/ja-jp/press-office/press-releases/2014/04/ns-dirty-dozen-q1-2014.aspx

日本、久々の Worst 10 ランクイン

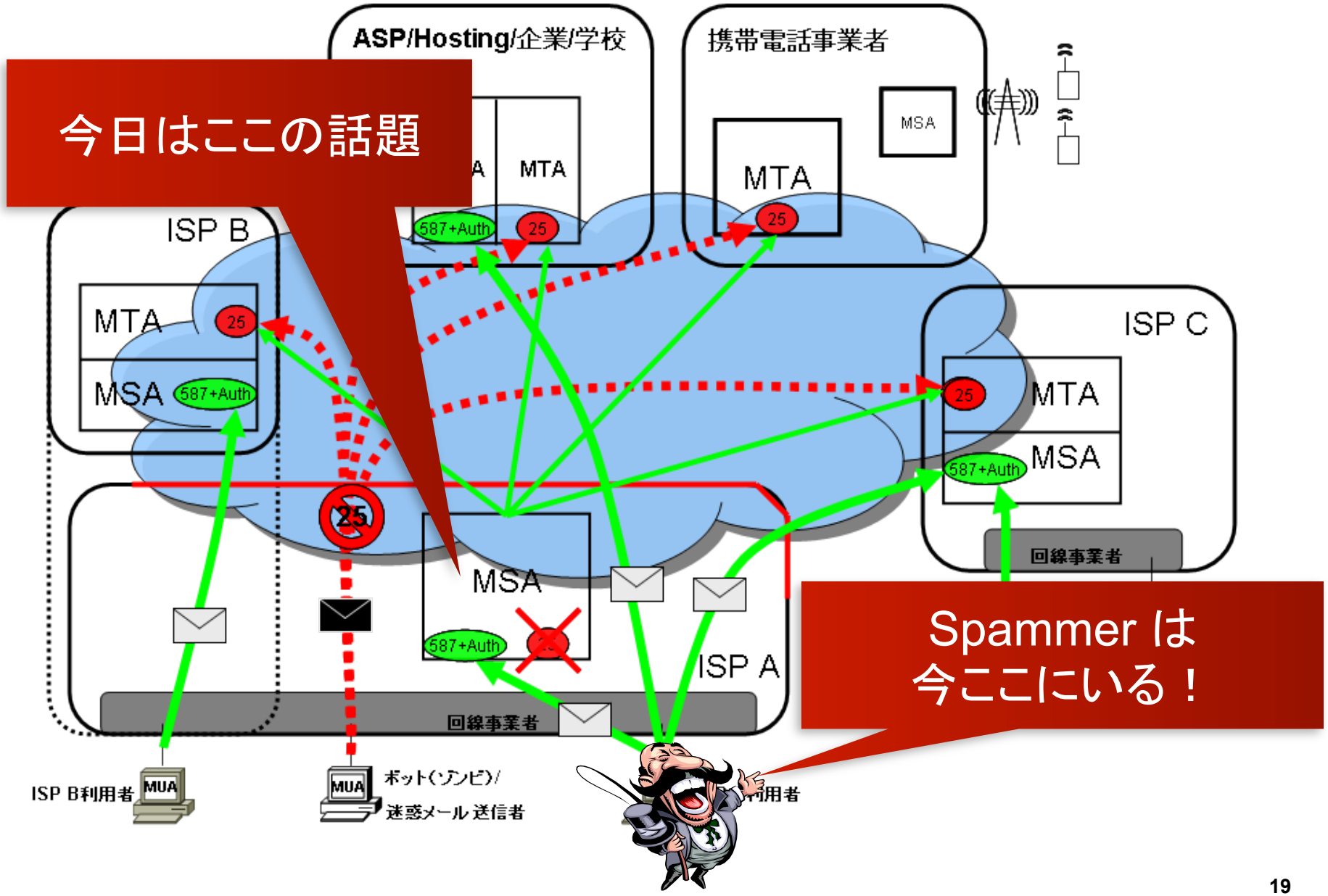
Spammer はどこ？

動的 IP からは送信できない

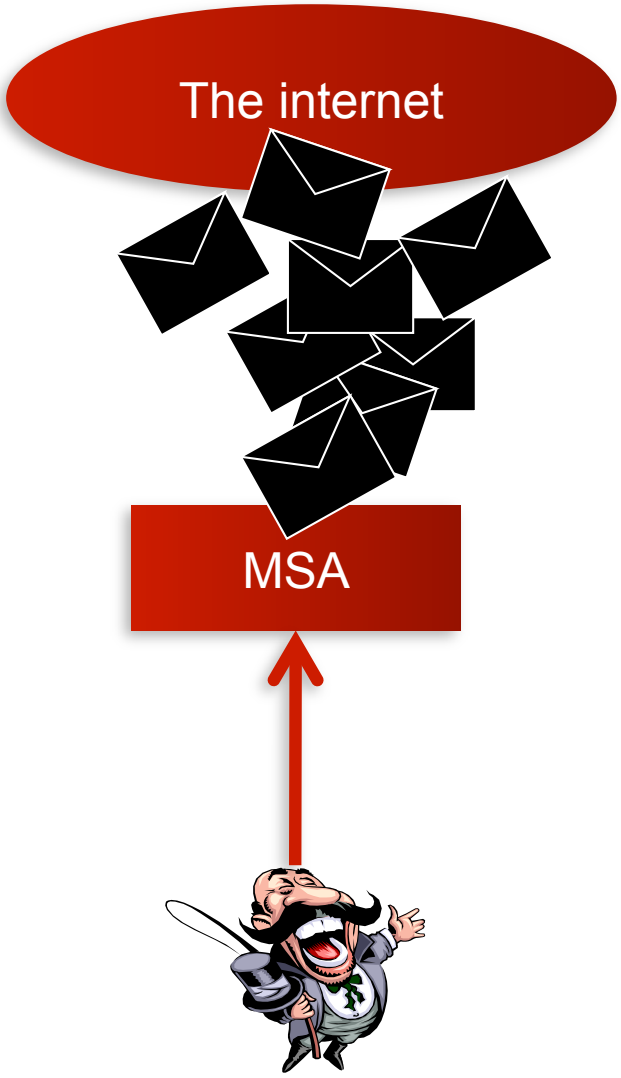
Spammer は日本に戻ってきた

Spammer はどこにいるのか？

現状の spam


今日はここの話題
ASP/Hosting/企業/学校
携帯電話事業者
MSA
MTA
MTA
587+Auth
25
25
ISP B
MTA
25
MSA
587+Auth
ISP C
25
MTA
MSA
587+Auth
回線事業者
25
MSA
587+Auth
25
ISP A
回線事業者
Spammer は
今ここにいる！
ISP B利用者
MUA
MUA
ボット(ゾンビ)/
迷惑メール送信者

今日の Scope



TELNET MSA **587**

220 OK

EHLO USER

250 OK

AUTH LOGIN

Spammer は AUTH ID と Password を持っている

どれくらいの ID が不正利用されるか

0.2～0.3%

調査期間：2013年、2014年（約1年半）

500 人にひとりくらいは ID を盗まれている

悪用が発覚し、停止したID数（月別）

統計情報
当日のみ公開

ID不正利用の傾向（ニフティ）

統計情報
当日のみ公開

日本からどれくらい spam が送信されているか

http://www.vade-retro.com/en/

http://www.cloudmark.com/en

日本の ISP 各社

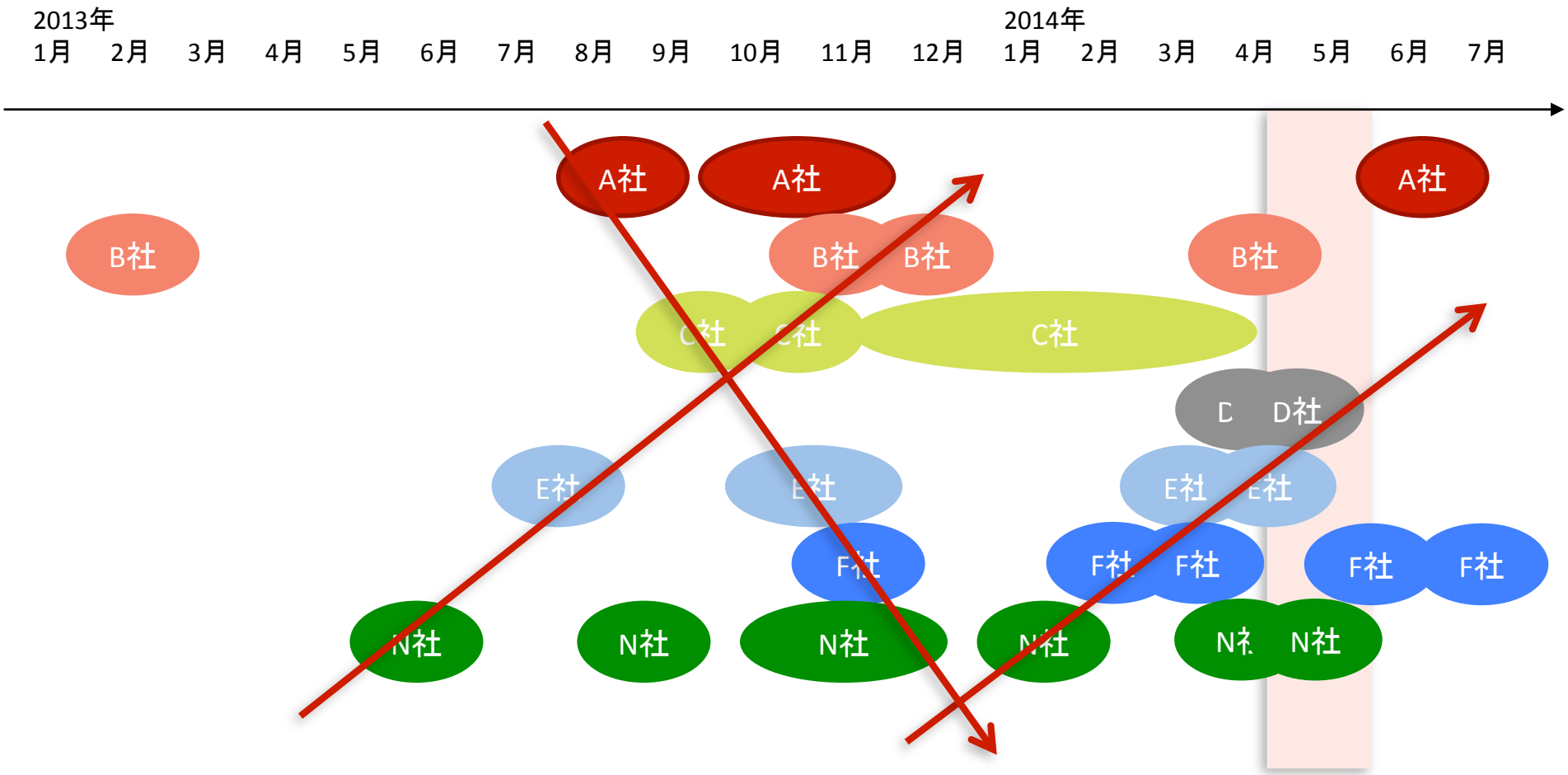
VadeRetro 社、Cloudmark 社、ISP 各社の協力

日本の ISP からどれくらい spam は送信されているか？

統計情報
当日のみ公開

紺社 → 橙社 → 青社 → ピンク社 → 灰色社 → 黄色社

日本の ISP からどれくらい spam は送信されているか？

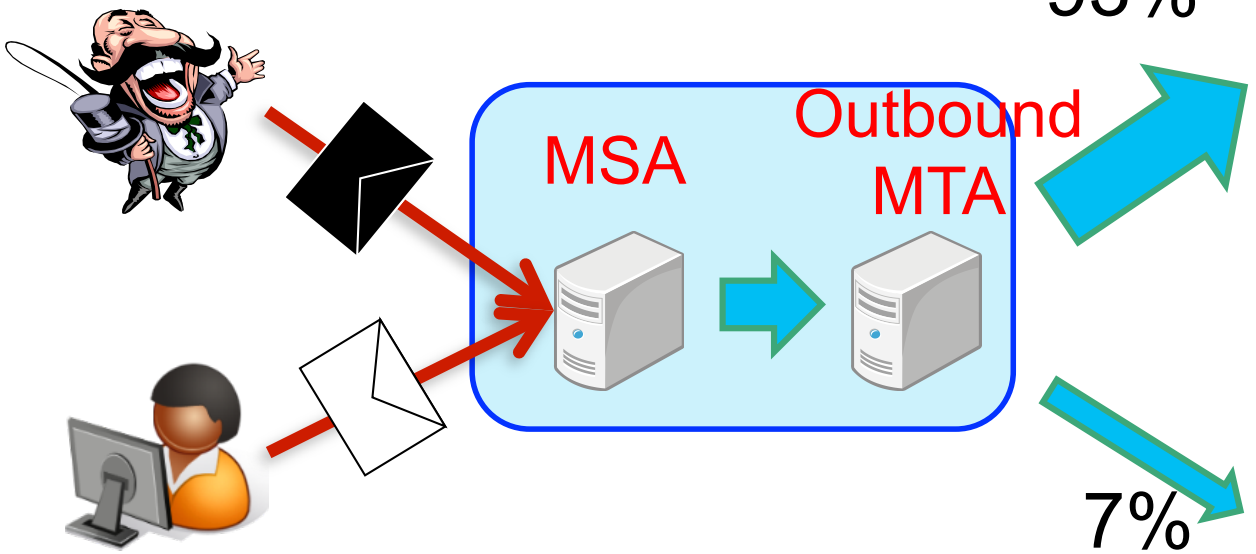


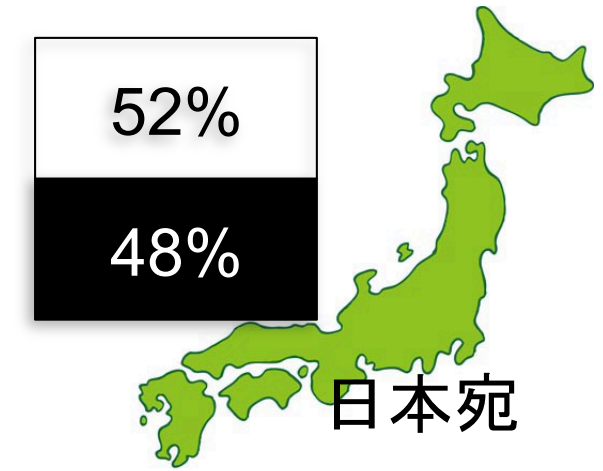
※ ISP 各社の協力の下、赤桐、加瀬、加藤の調査による

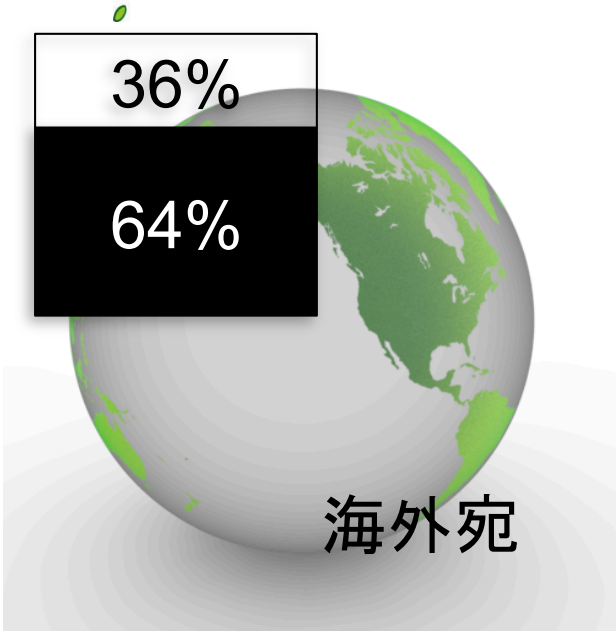
Spammer の民族大移動

ISP から送られるメール

CLOUDMARK







日本発日本宛が多い

約 50% が Spam

どれくらいが spam か？

統計情報
当日のみ公開

ISP 別の統計

自分のところからどれくらい spam が送信されているか

調べてほしい方は
赤桐まで

janog@akagiri.com

VADE-RETRO
NEXT-GEN EMAIL FILTERING

CLOUDMARK

かき混ぜる

議論

議論

1. どんな対策をするのか？
2. そもそも ID/Password を取られないためには？
3. Spammer はどこにいるのか?
4. AUTH Method はどうすればいいか？

議論

Q1. どこで対策しますか？

Spam 対策のポイント整理

Spammer

MUA(乗取)

「踏まれない」

- ✓ AntiVirus
- ✓ リテラシ

MSA(送信)

「送らせない」

- ✓ Rate Control
- ✓ Reputation
- ✓ Content Filter

※ Outbound MTA

MTA(受信)

「届かせない」

- ✓ Reputation
- ✓ ドメイン認証
- ✓ Content Filter

User

MUA(閲覧)

「見せない」

- ✓ Visualize

時代の流れ

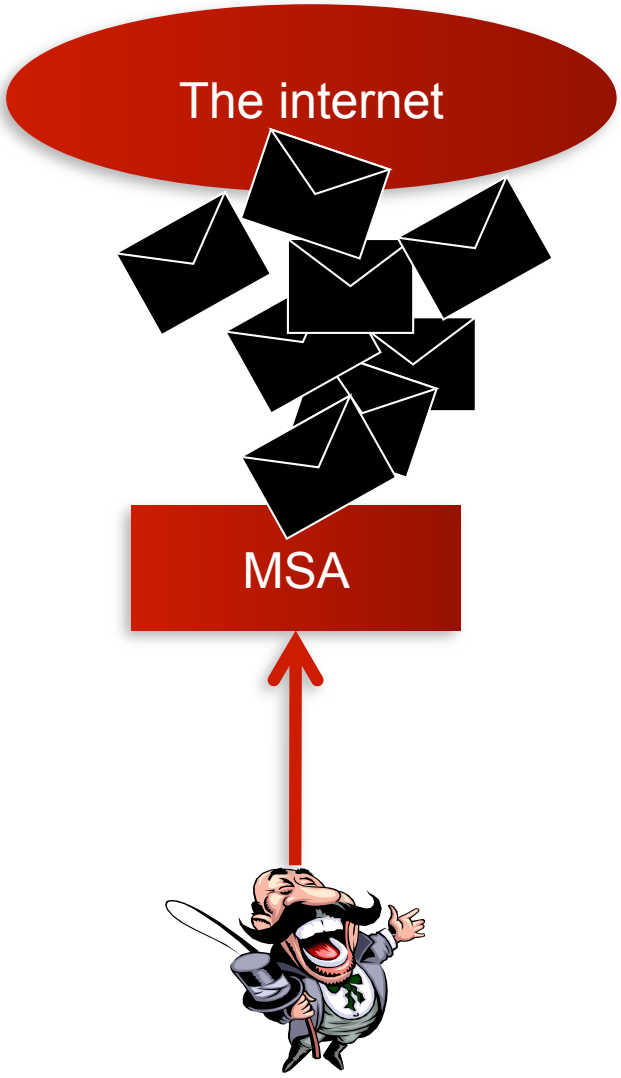
議論

Q2. そもそも ID/Password を取られないためには？

議論

以後は、MSA (Outbound MTA) での対策の議論

議論



TELNET MSA **587**

220 OK

EHLO USER

250 OK

AUTH LOGIN

Spammer は ID/Password を持っている前提

議論

Outbound Filtering

議論

Q3. Spammer はどこにいるのか？

2013年11月某日

統計情報
当日のみ公開

2014年1月某日

統計情報
当日のみ公開

2014年6月某日

統計情報
当日のみ公開

送信元の国

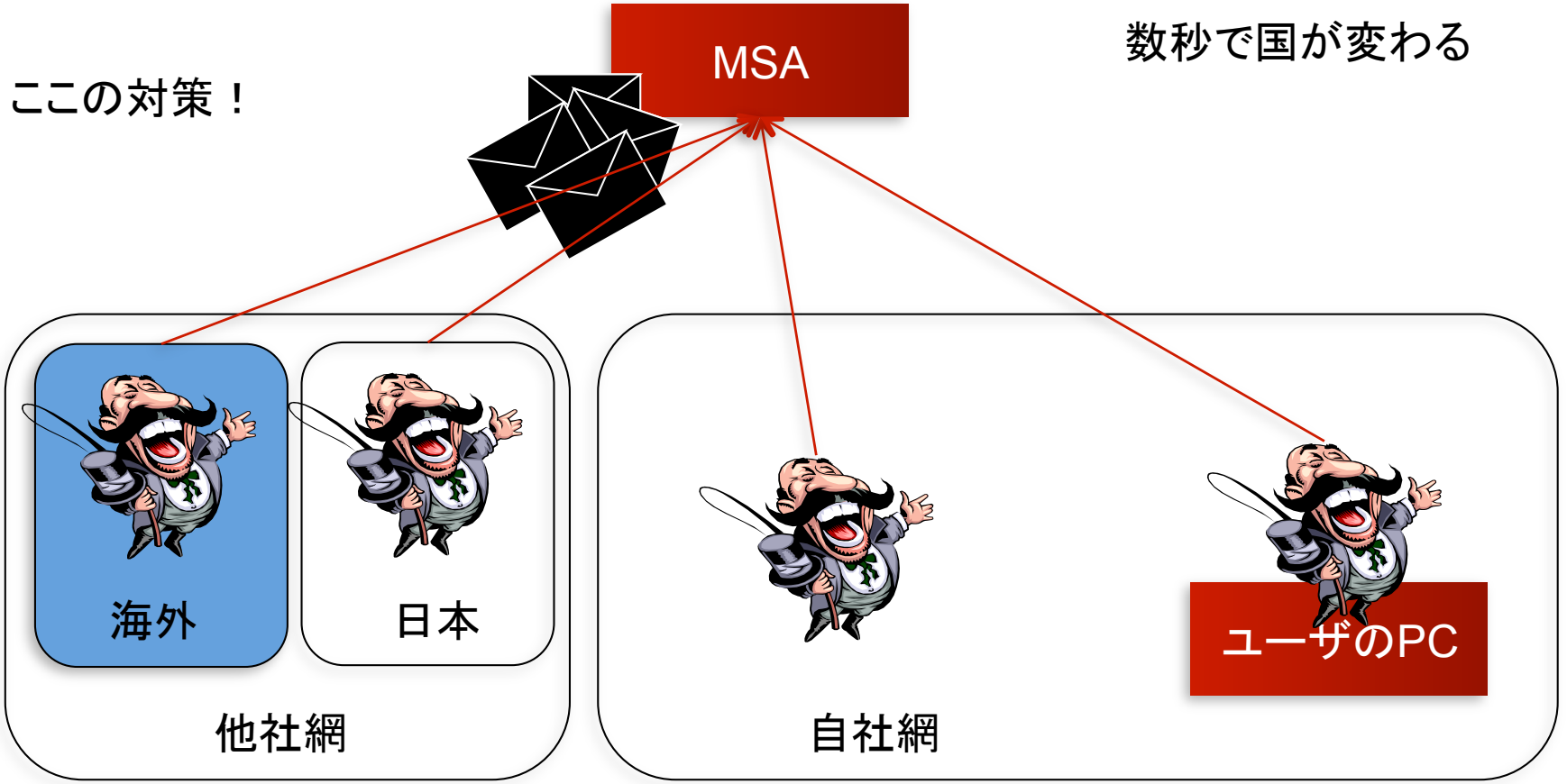
統計情報
当日のみ公開

具体例：ある会員の送信元

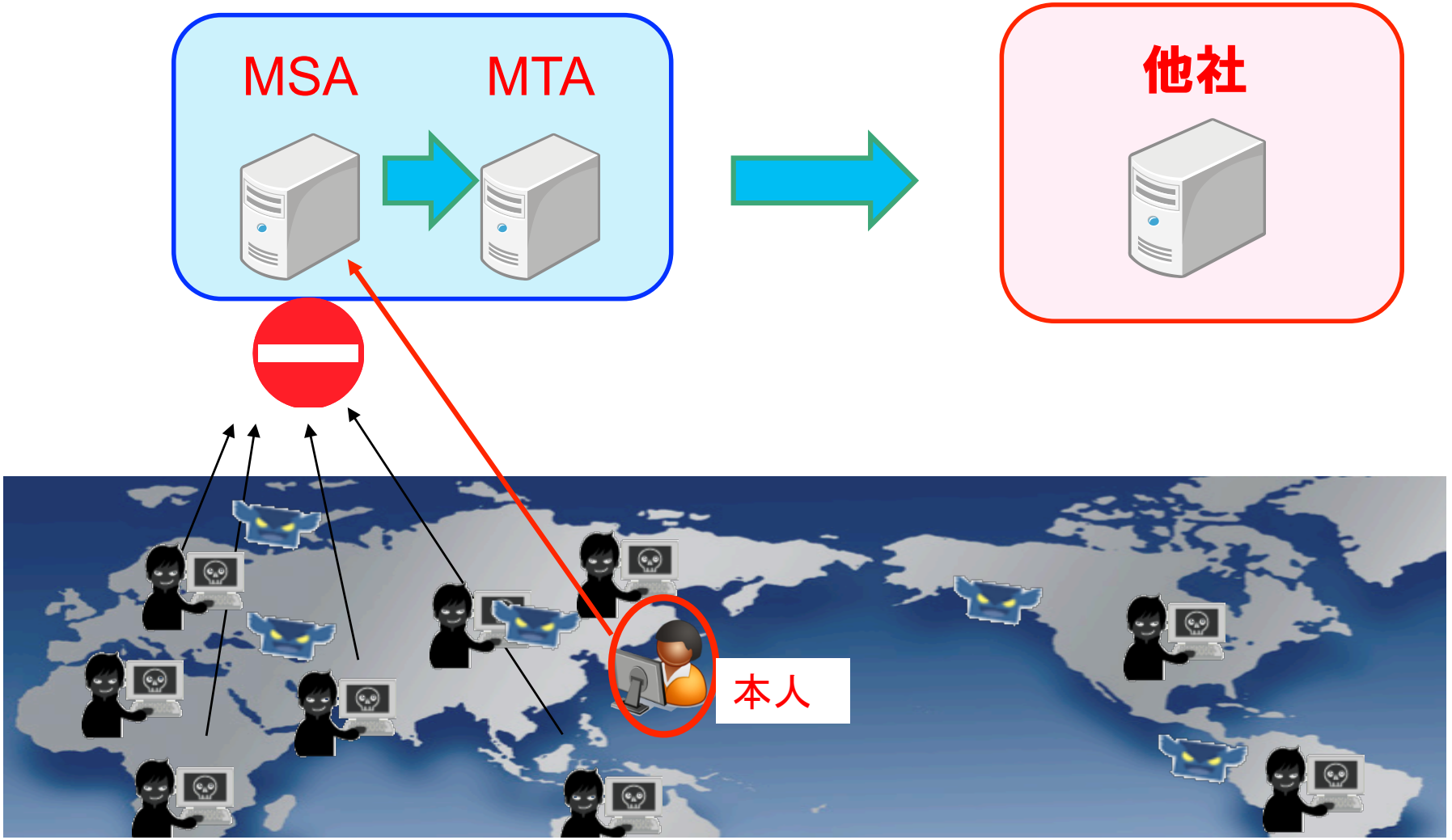
統計情報
当日のみ公開

ユーザの「瞬間移動」

Spammer はどこにいるのか？



対策案



海外からの接続をコントロール

議論

Q4. AUTH Method はどうすればいいか？

SMTP AUTH の Method

統計情報
当日のみ公開

Spammer には LOGIN が人気

議論

CRAM-MD5 だけの提供にしたら効果あり？

こぼす

対策の方針

- 当日のみ