国内外のスパム脅威と対策の動向

マルチメディア推進フォーラム

Part 501

2010/4/22

NTTサービスインテグレーション
基盤研究所

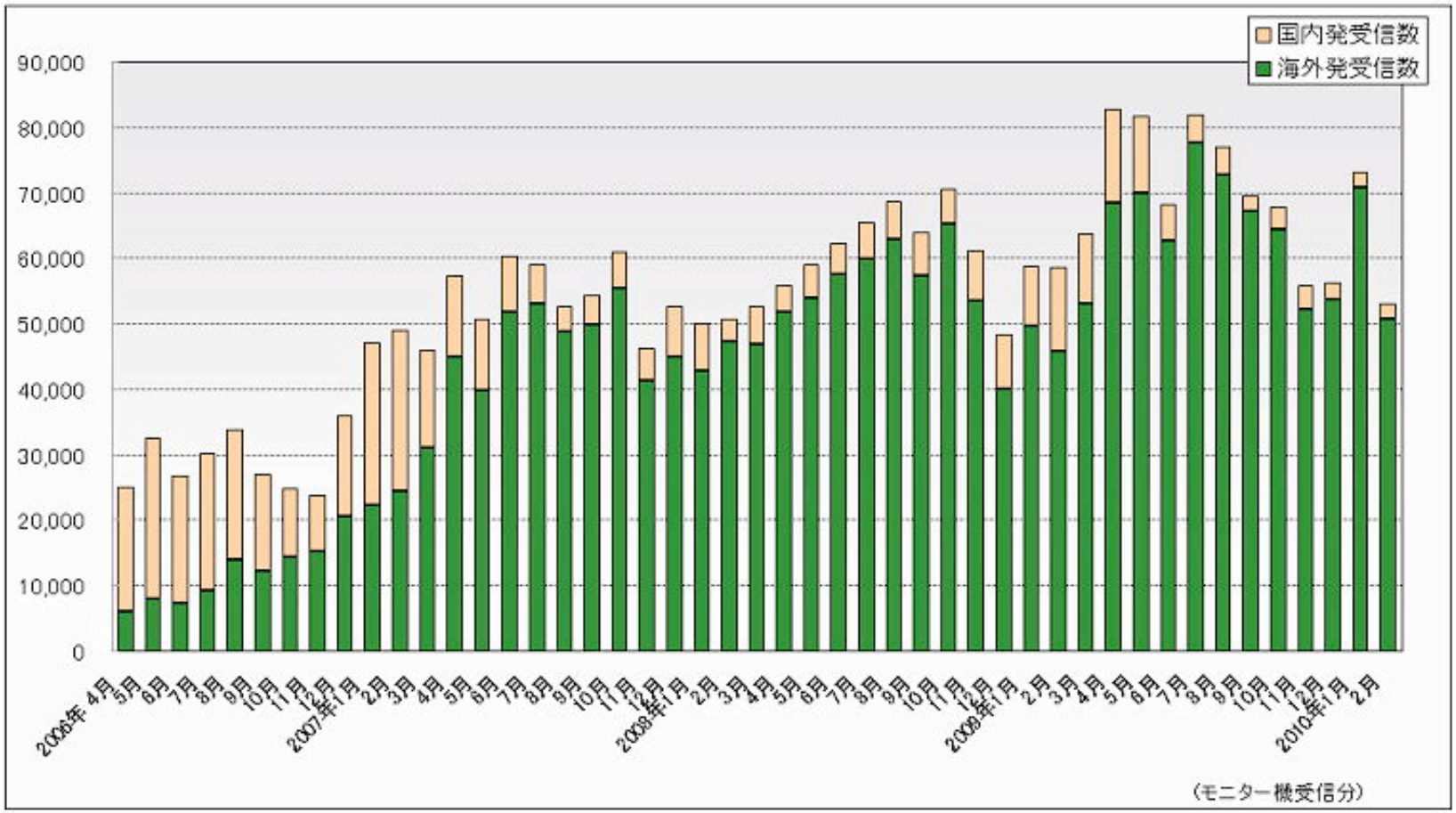
森　達哉

アジェンダ

- スパムの増大とそれに伴なうコスト
- スパムの実態と代表的な対策技術
- スパムが増大し続ける主要因
- スパムボットの実態と対策
- ボットネット対策の根本的な難しさ

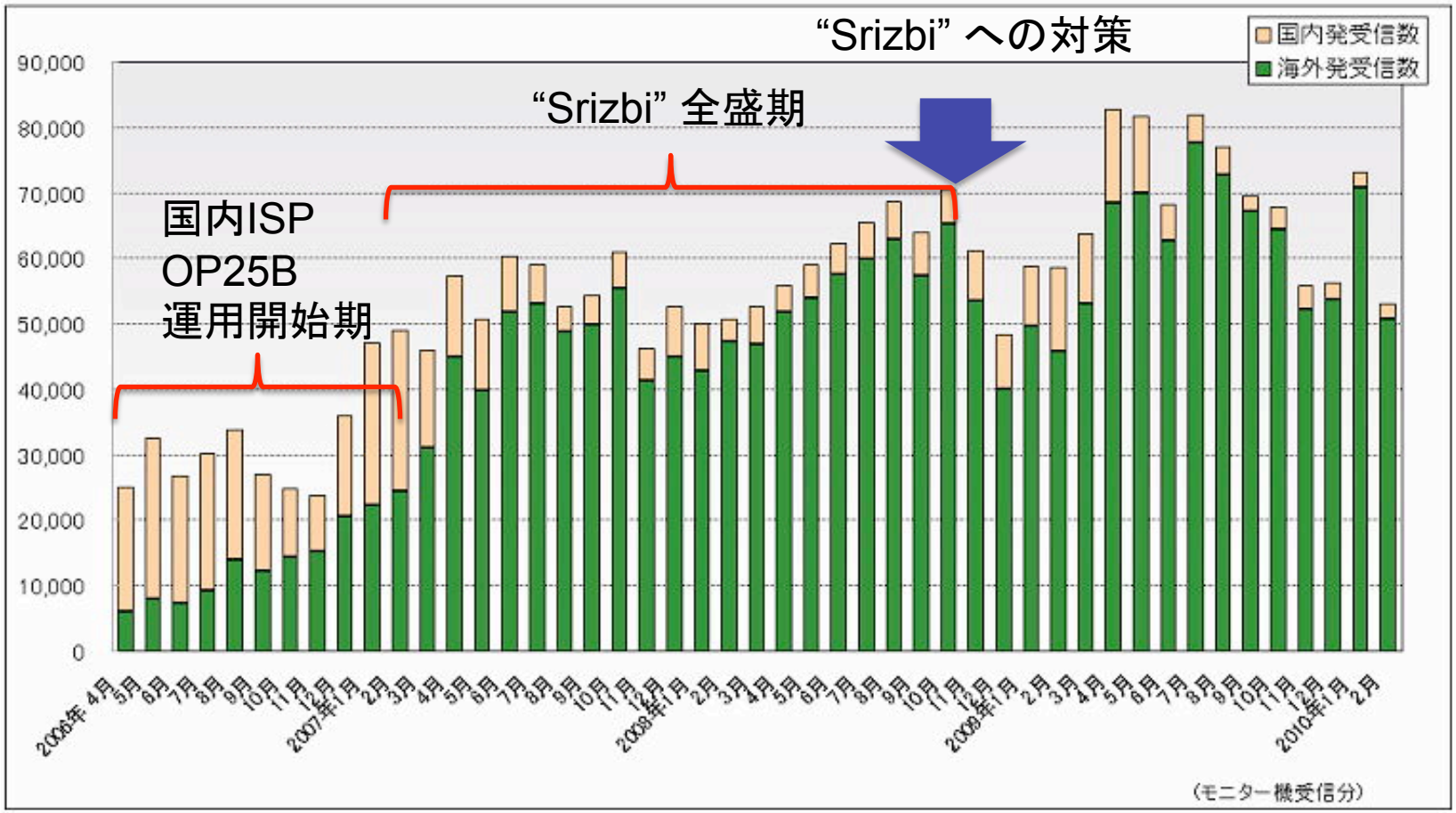
スパム増大とそれに伴なうコスト

近年の急激なスパムの増大



引用元：（財）日本産業協会　「迷惑メールの統計」H22年2月

近年の急激なスパムの増大



引用元：（財）日本産業協会　「迷惑メールの統計」H22年2月

急激なスパム増がもたらす被害

- スパム処理にともなうコスト
  - 従業員の生産性
  - スパムアプライアンス購入・メンテナンス
  - バックアップシステム等
- 電子メールサービスの断にともなうコスト
  - 顧客信頼の喪失
  - 営業機会の喪失

スパム受信のコスト計算

- Google: **Return on Investment Calculator**
  - http://www.google.com/postini/roi_calculator.html

Inputs

Number of employees with email:	3000
Number of workdays per year per employee:	245
Average hourly salary per employee:	65
Average number of spam messages per day per employee:	100
Number of seconds wasted with each spam message:	5

Calculate!

Total Cost of Spam

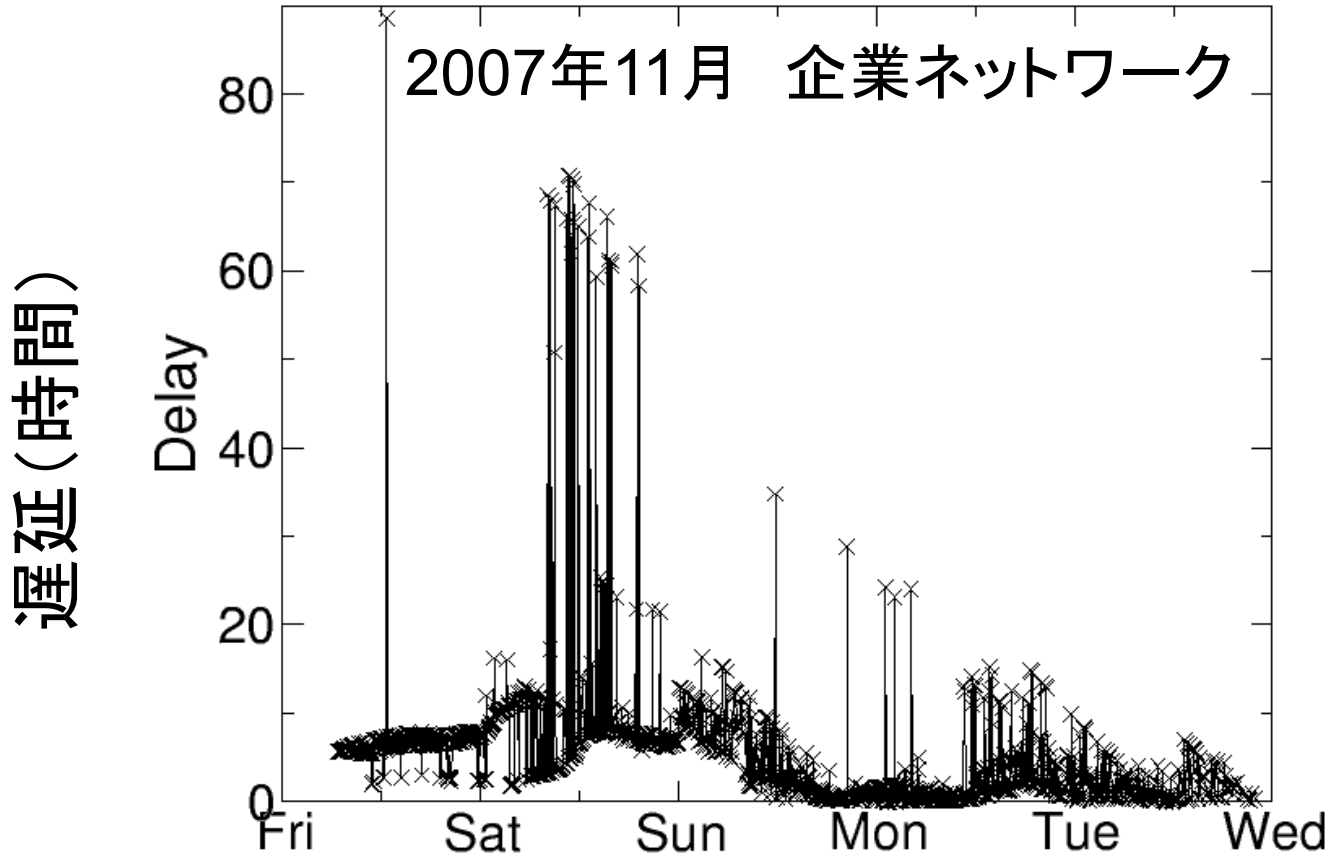
Lost Salary (yearly):	$6,635,417
Lost Productivity (yearly):	6337 days

従業員数
従業員毎の労働日数
従業員毎の平均時給
従業員毎のスパム受信数/日
スパム一通毎に消費する秒数

年間損失利益　約6億円

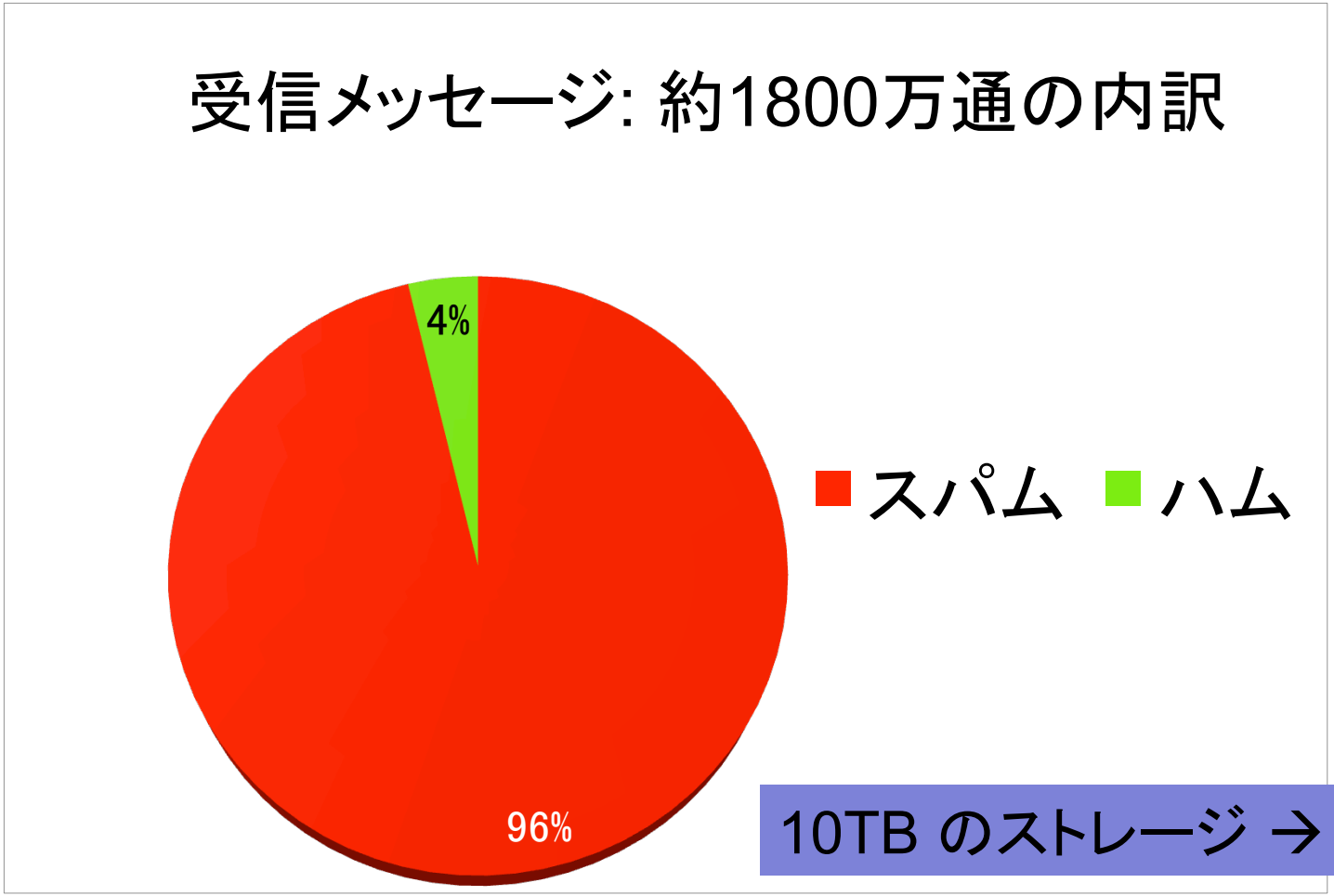
年間損失生産性　6337人日

スパム増加による，電子メールサービスの大規模遅延の例



スパムの実態と代表的な対策技術

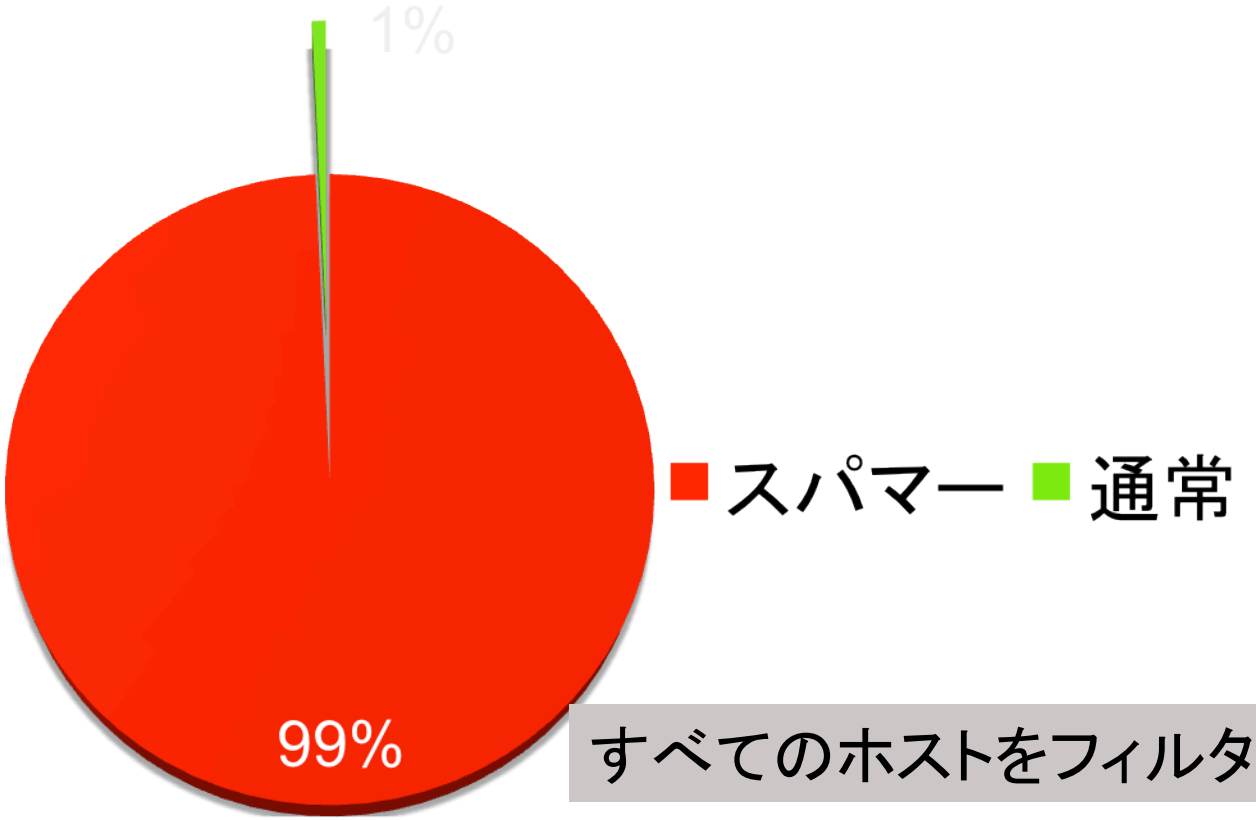
ある企業のメールサーバにおける 1ヶ月のメール受信状況



10TB のストレージ → 9.6TB が無駄!

ある企業におけるメールサーバの1ヶ月のメール受信状況

メール送信ホスト: 約200万ホストの内訳



すべてのホストをフィルタ → 99%正解!!

ITPro

（勝村　幸博＝日経パソコン）　[2010/04/19]

ニュース

コメントを読む/書く | ITproブックマーク | ソーシャルブックマーク | Twitter | 印刷 | ヘルプ

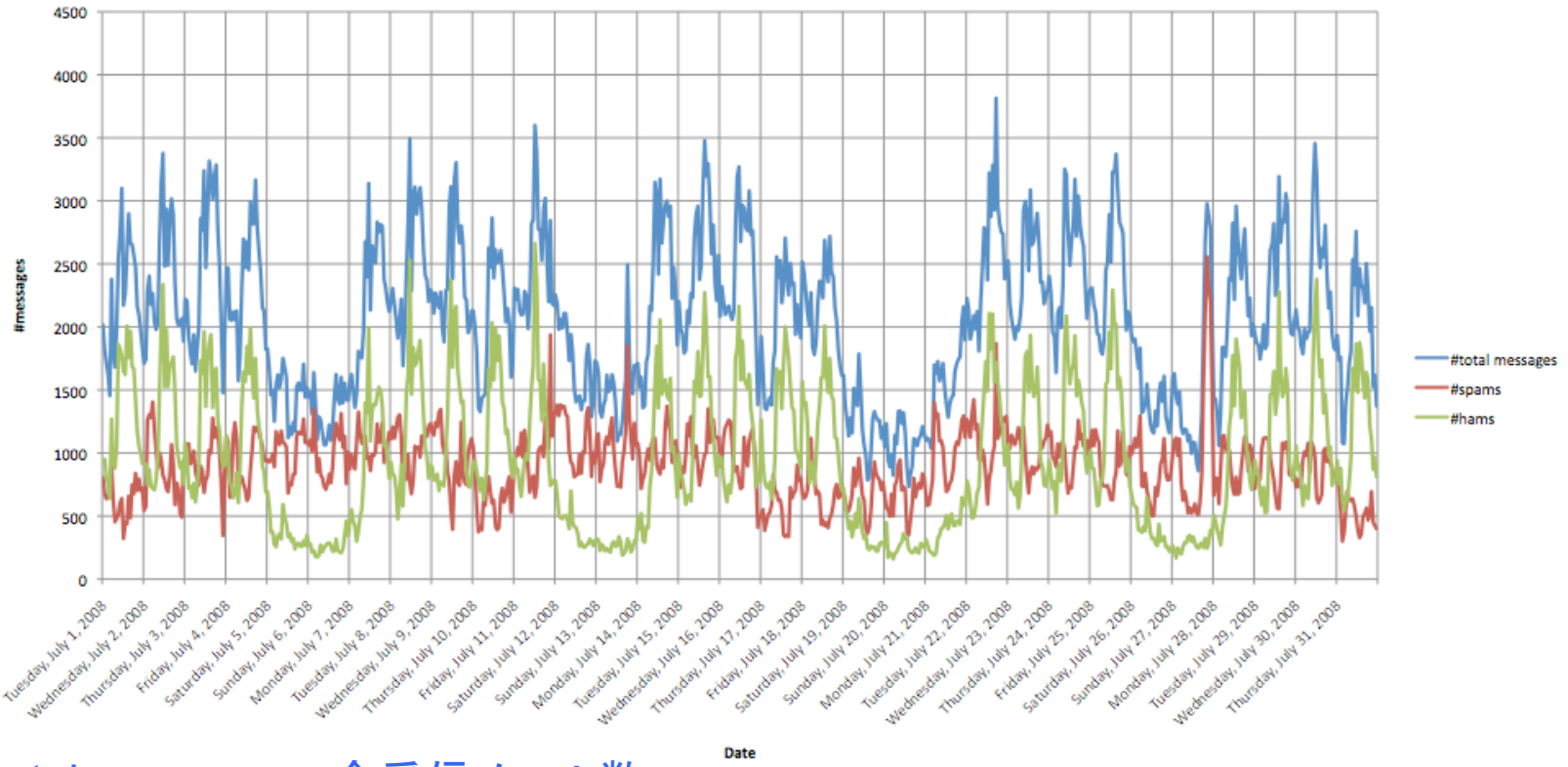
メールの9割は「迷惑メール」、そのうち2割弱は「詐欺メール」

米シマンテックが2010年3月の迷惑メール動向、「件名は『空白』が最多」

記事一覧へ >>

セキュリティ企業の米シマンテックは2010年4月16日、同社の観測データを基に、2010年3月の迷惑メール（スパム）動向を発表した。同社が観測したメールのおよそ9割が迷惑メールで、そのうちの17%が詐欺目的のメールだったという。

受信メッセージの変動パターン



#total messages: 全受信メール数

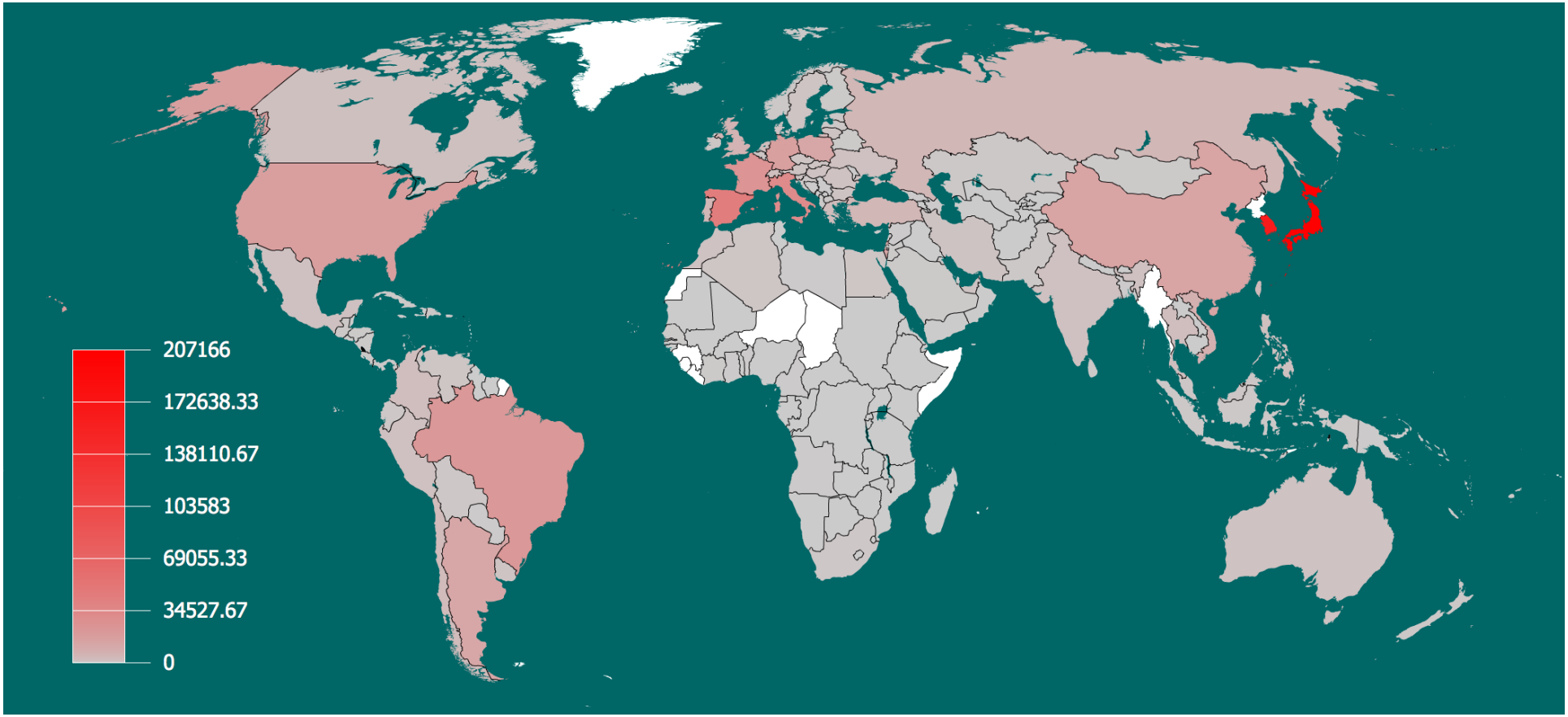
#spams: スパムメール数

#hams: ハムメール数

ハムの配信数は人間活動と相関のあると思われる日変動を示す。

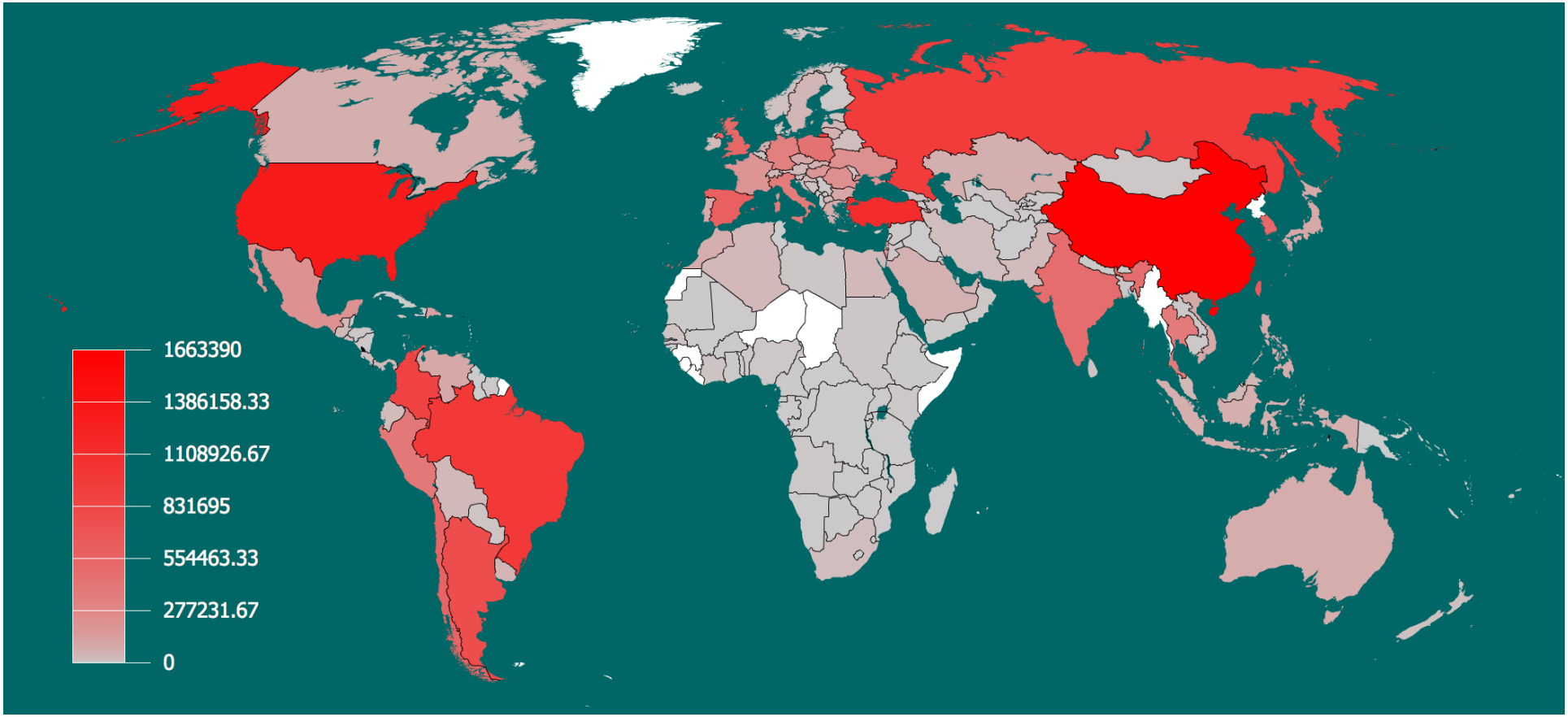
スパムの配信数もやや日変動傾向あり。タイムゾーンが7-8時間ほどずれている。

ネットワークフィルタ
されなかったスパムの送信元



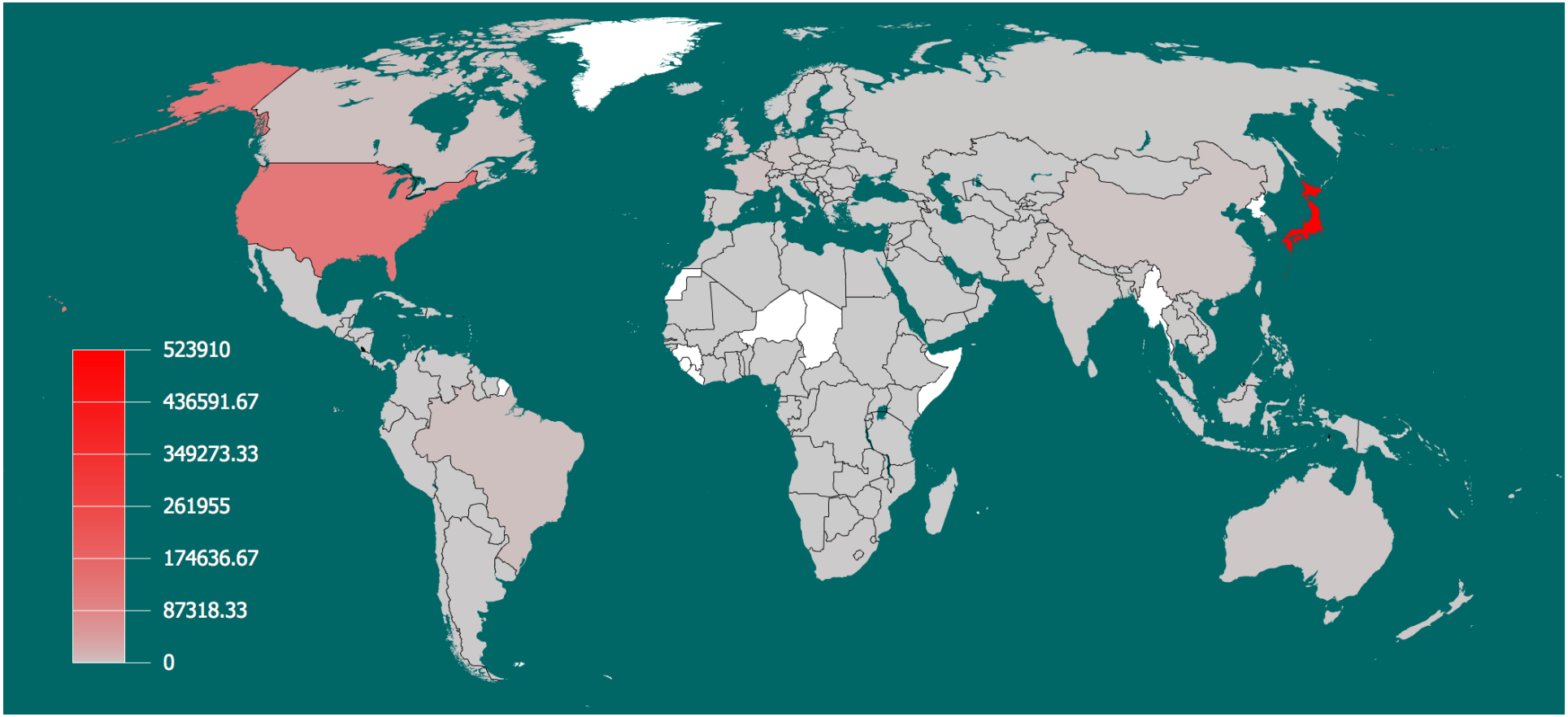
実際に配送されたスパムは国内・韓国発が多かった
※これらのスパムは greylisting で落ちていない

ネットワークフィルターされた スパムの送信元



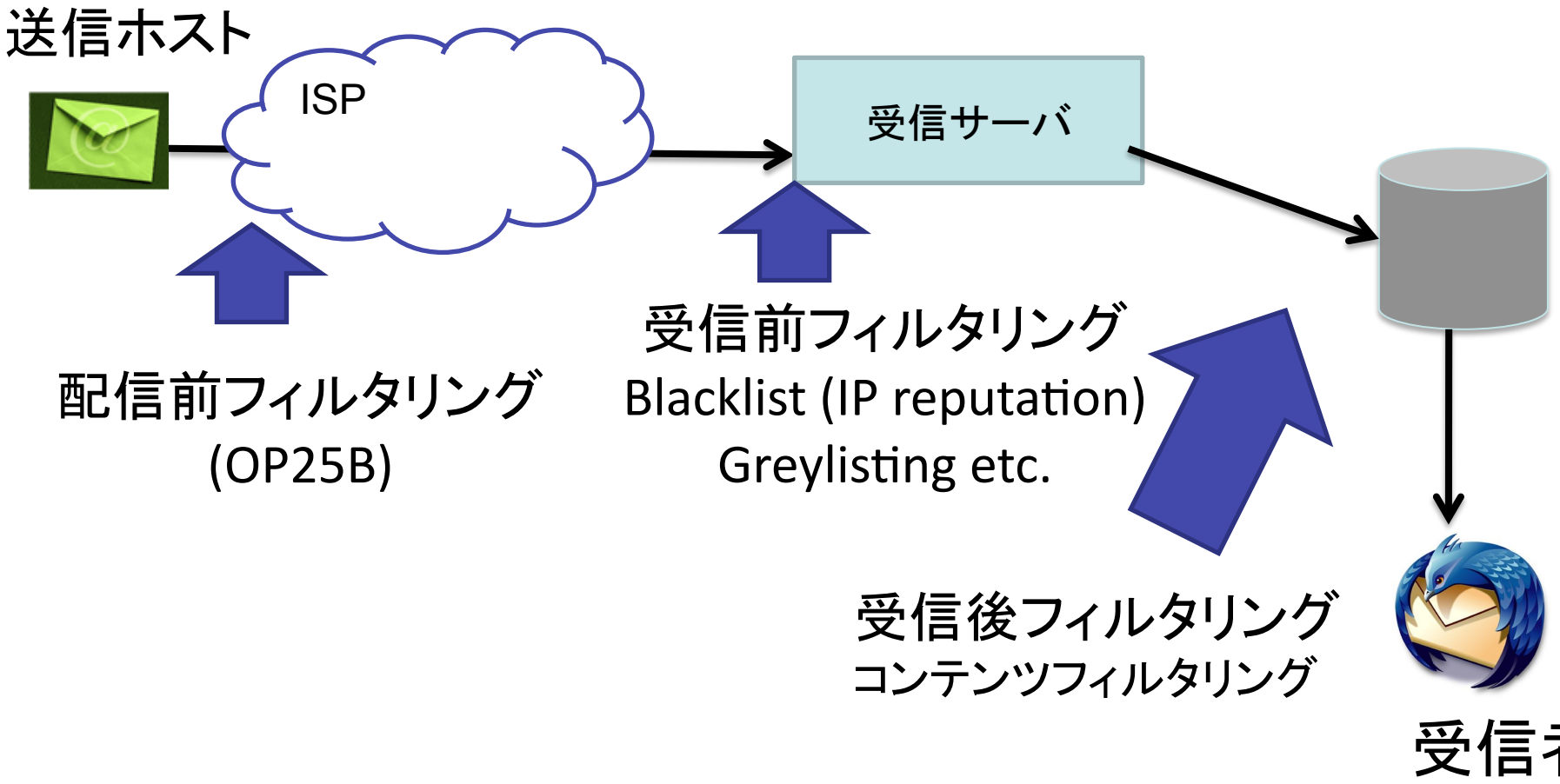
Greylisting でフィルタされたメッセージ(非受信スパム)は BRICs 諸国を中心とした一部の国に集中

受信したハムの送信元



通常のメッセージの送信元は日米に集中

代表的な迷惑メール対策技術



OP25B

- **Outbound Port 25 Blocking**
- **エンドユーザ（ホスト・ボット）から外部に直接メールを送信させないしくみ**
- 国内の主要なISPが2006年～2007年にかけて一斉に運用開始
- 国内の業者・ボット発のスパムが激減した

- 世界的にこのような機運が高まることで効果が期待できる（ただし抜け道もあるが）
- 通信の制御に対するポリシーは国によって様々

スパムが増大し続ける主要因

スパム送信のインセンティブ =マーケット

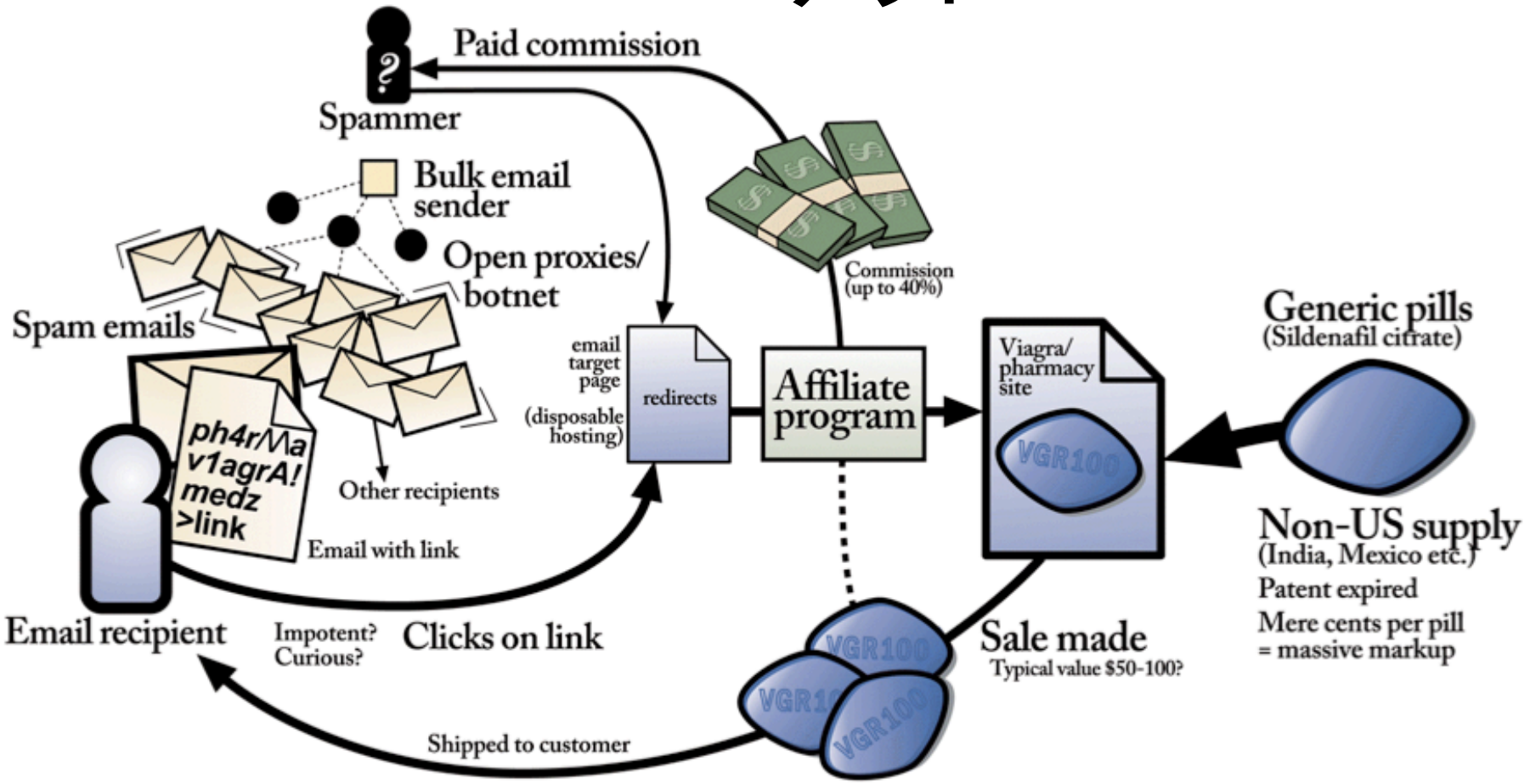
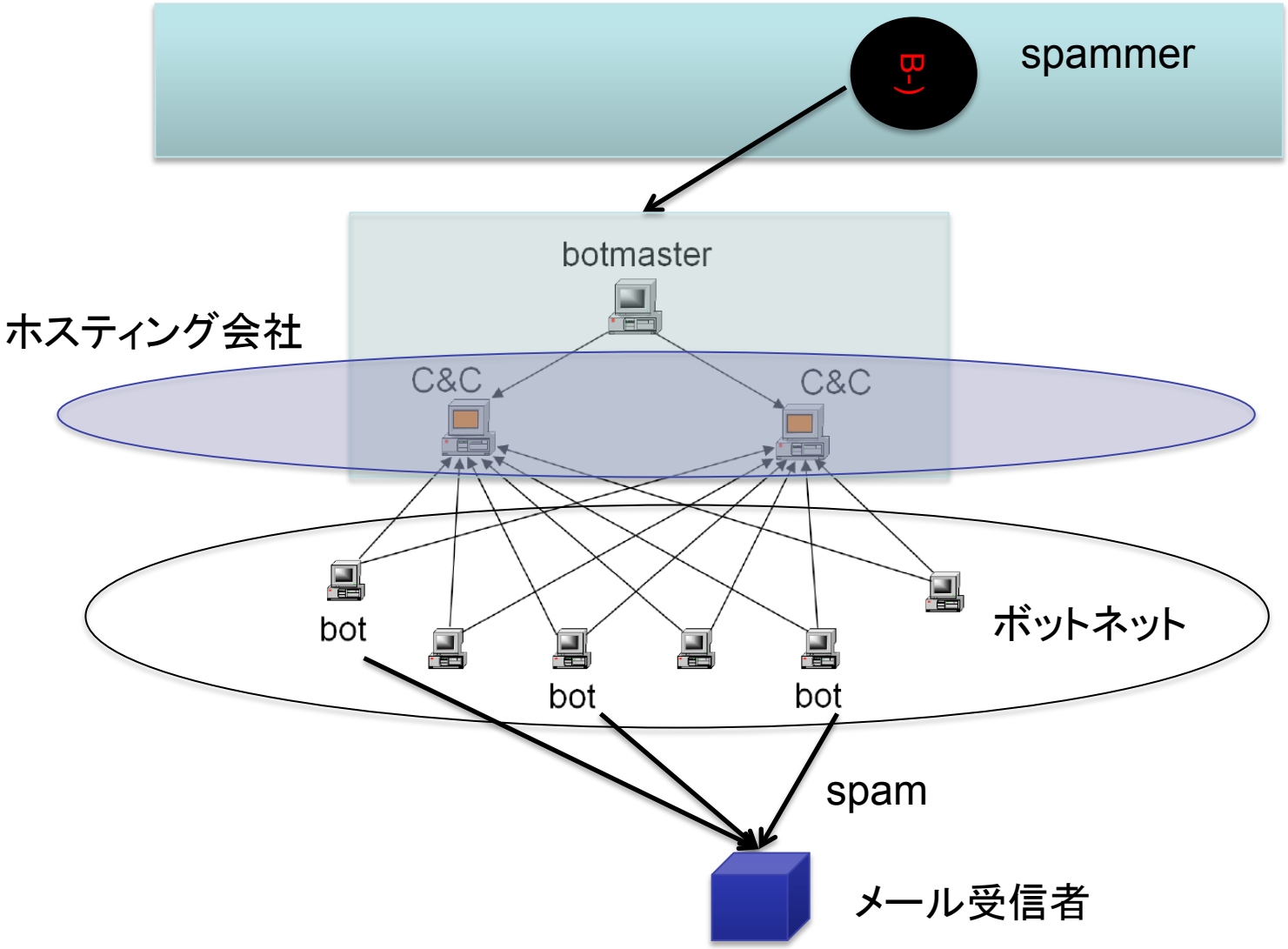


Diagram by Stuart Brown
modernlifeisrubbish.co.uk

ボットによるスパム送信



主要なスパム送信源

- 通常のサーバ
  - Hotmail, Gmail, etc.
- ボットネット
- スパムギャング
  - ホスティングサーバ等の安定的なインフラを利用
- Open Proxy / Open Relay
  - 古くからある手法
- Hijacked Prefix
  - 経路の乗っ取り

スパム送信源の内訳

CONTRIBUTION OF EACH CATEGORY

List	#IPs	#Spam	#Ham
Total	100 %	100 %	100 %
Legit Servers	1.0 %	1.7 %	87.9 %
End-hosts	85.0 %	55.0 %	0.5 %
Spam gang	1.6 %	28.6 %	0.6 %
Hijacked prefix	0.4 %	0.4 %	0.2 %
Open Relays/Proxies	0.9 %	2.6 %	0.1 %
Unclassified	11.1 %	11.7 %	10.7 %

H. Esquivel, T. Mori, and A. Akella
``**On the Effectiveness of IP reputation for Spam Filtering**,''
IEEE/ACM COMSNETS 2010, Jan 2010 (Best Paper Award)

スパムボットの実態と対策

代表的なスパムボットの歴史

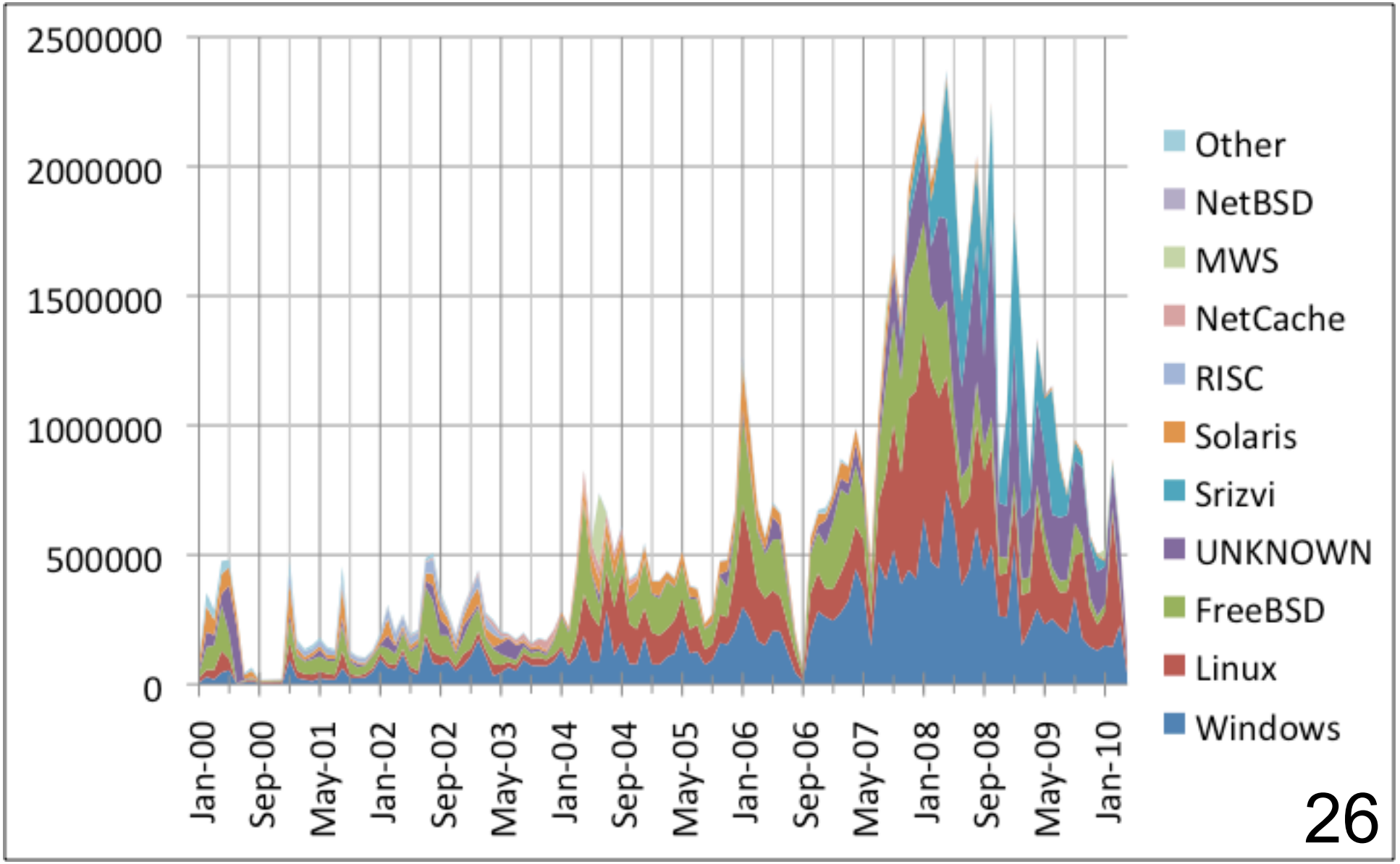
- 1996/8: SilverNet
- 2004頃～　スパム送信手段として定着し始める
- 2005～: SD-bot
- 2006?～: Mega-D　3.5万ホスト 100億通/日
- 2007～: Storm　　100万ホスト　30億通/日
- 2007～: Srizbi　　200万ホスト　600億通/日
- 2008～: Confiker　1000万ホスト 100億通/日

http://en.wikipedia.org/wiki/Botnet および独自調査

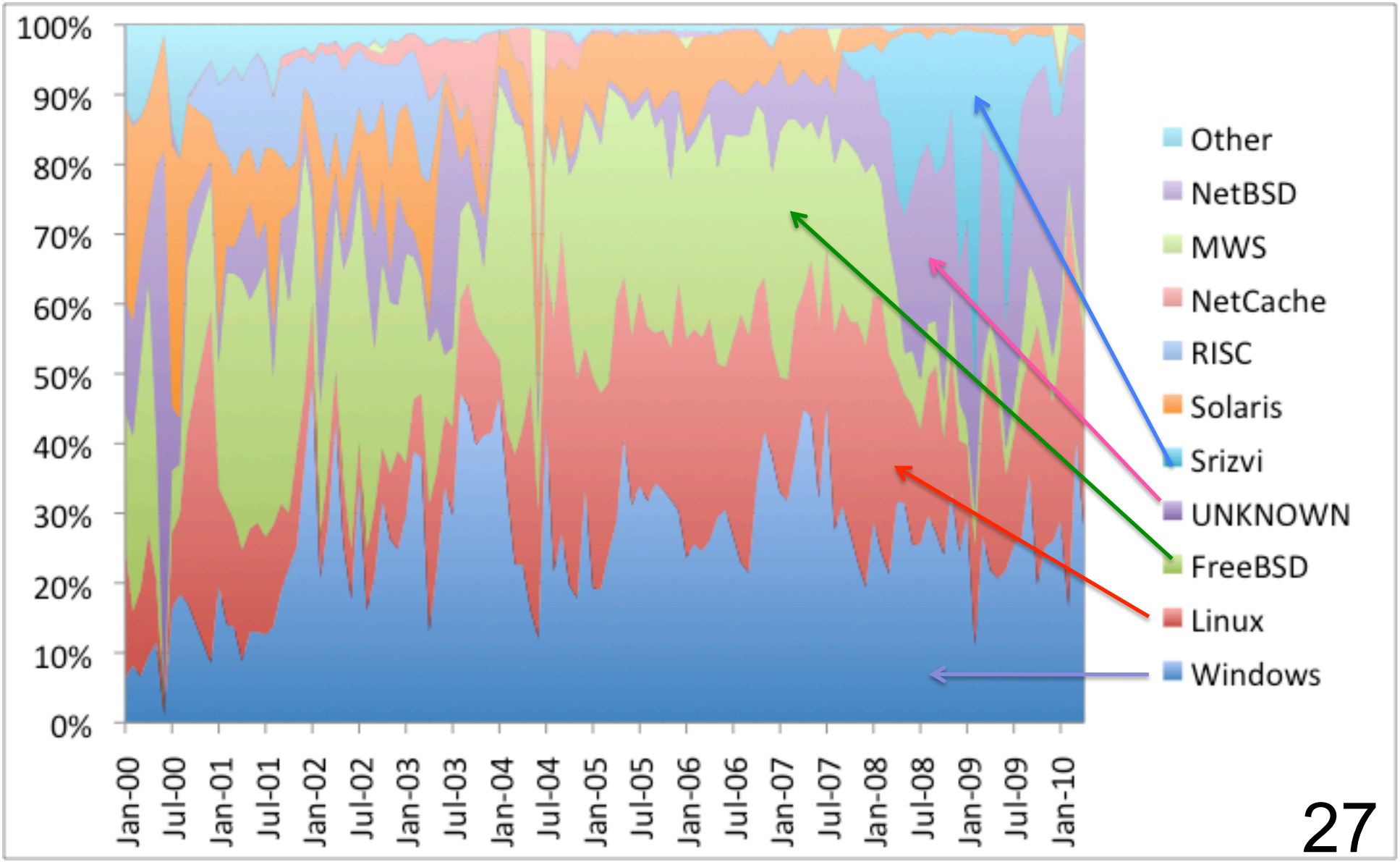
長期定点観測で見る
電子メール送信形態の変遷

- WIDEプロジェクト MAWI Working Group 提供の公開データを活用
  - http://mawi.wide.ad.jp
- 日米国際回線上のメールトラヒックを観測
- 2000年1月～2010年4月を分析
- パケットのヘッダ情報より，送信ホストのOS (オペレーティングシステム)を推定する技術を利用

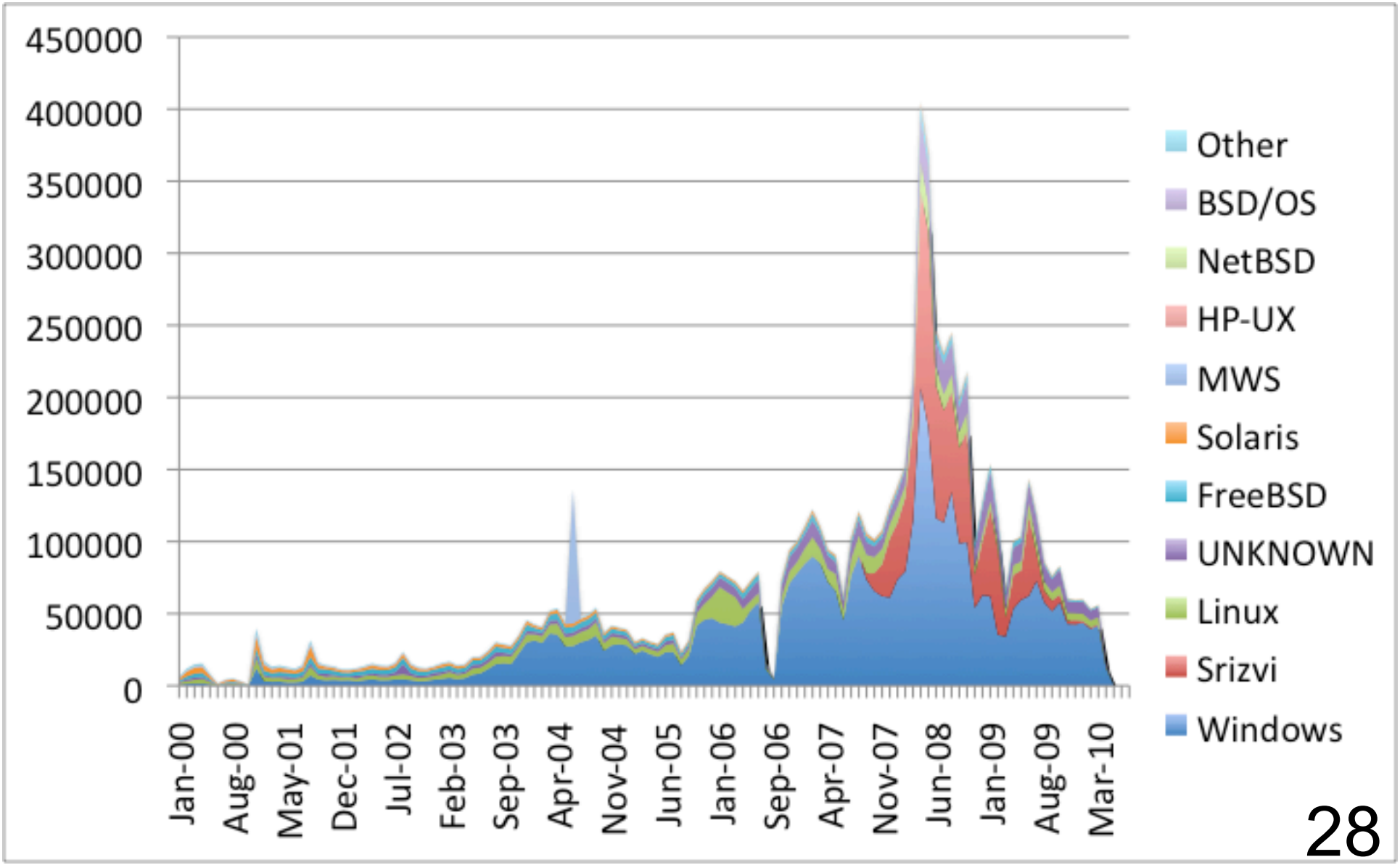
OS別SMTPコネクション数



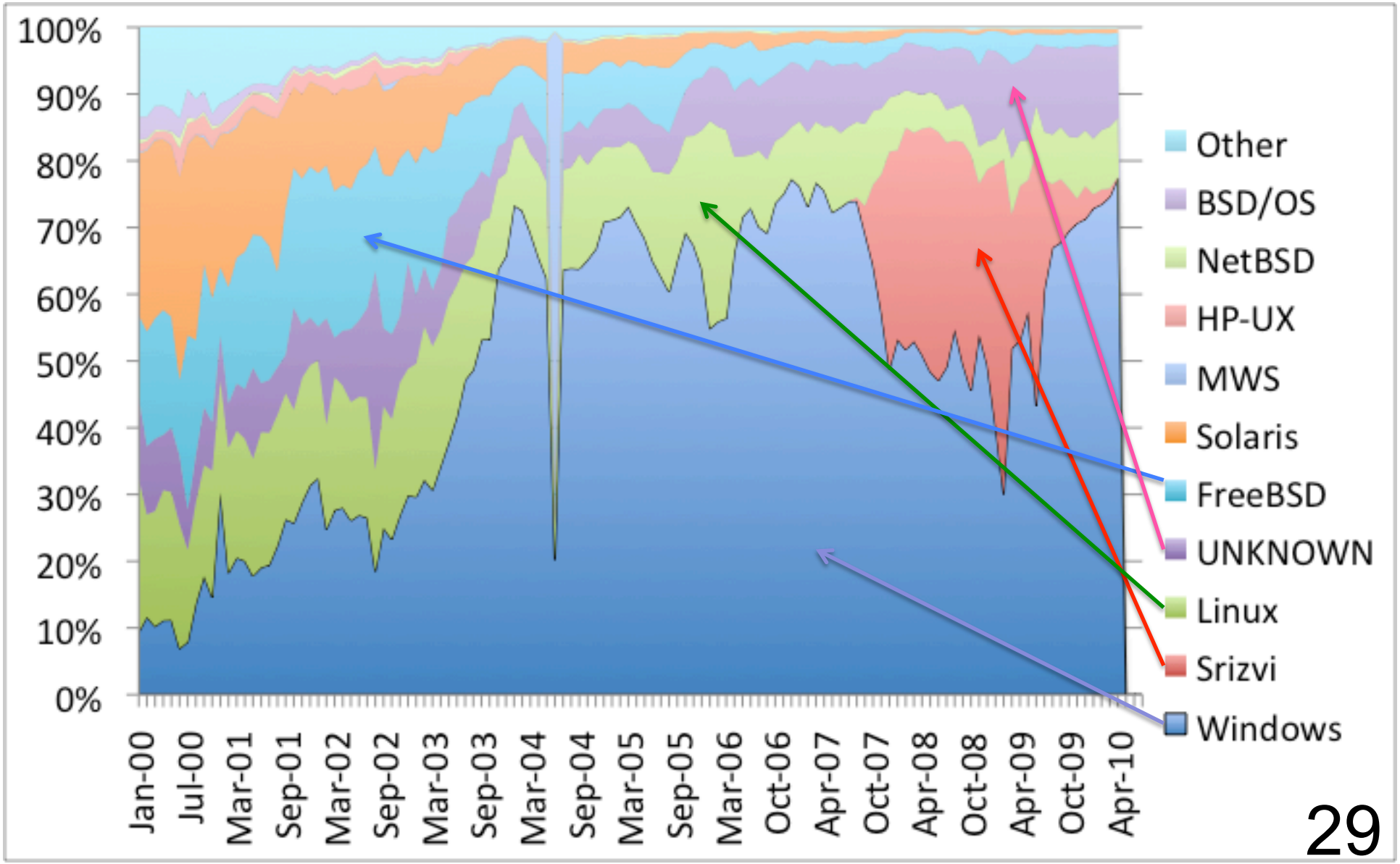
OS別SMTPコネクション数（割合）



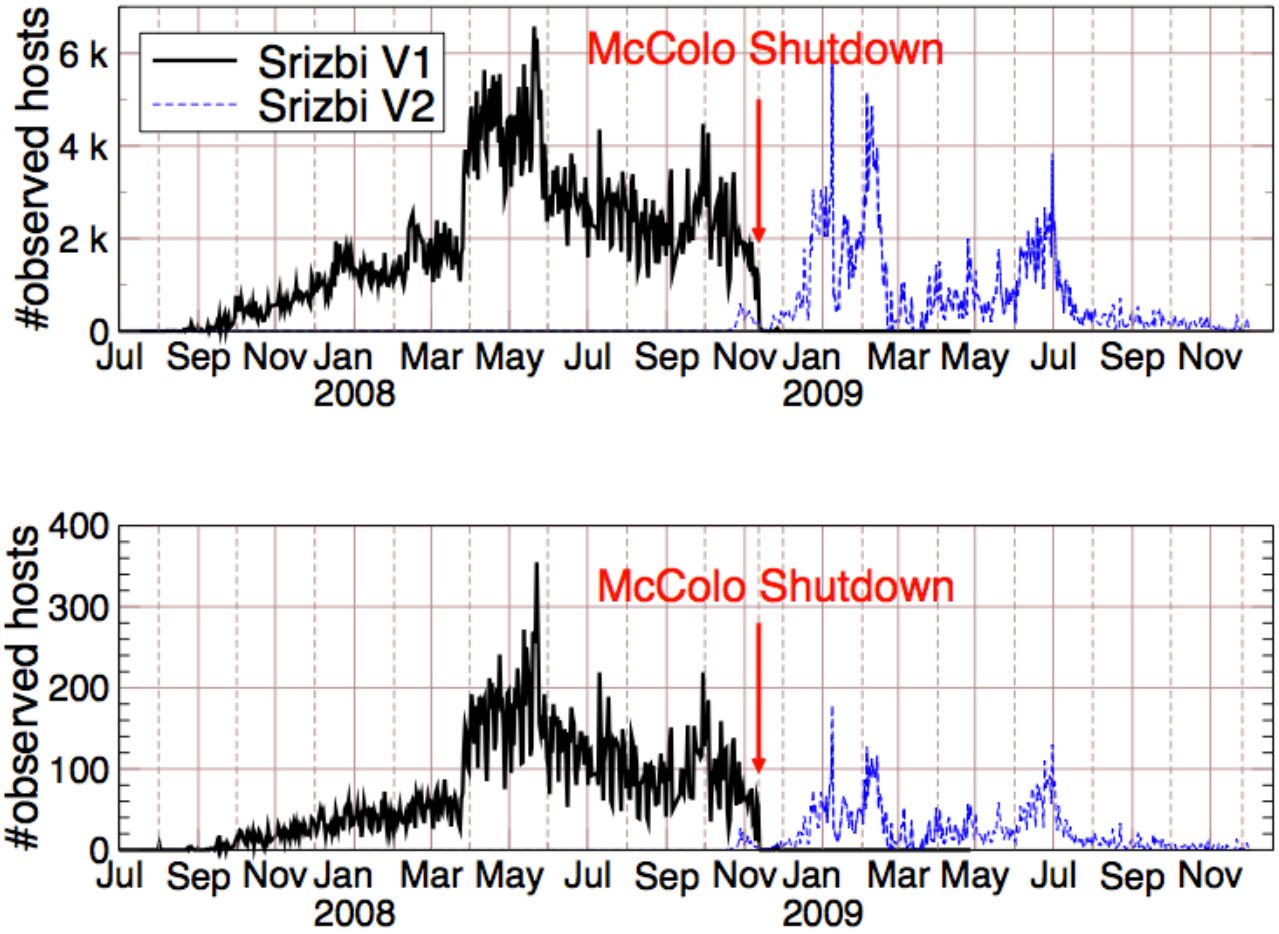
OS別送信元IPアドレス数



OS別送信元IPアドレス数（割合）

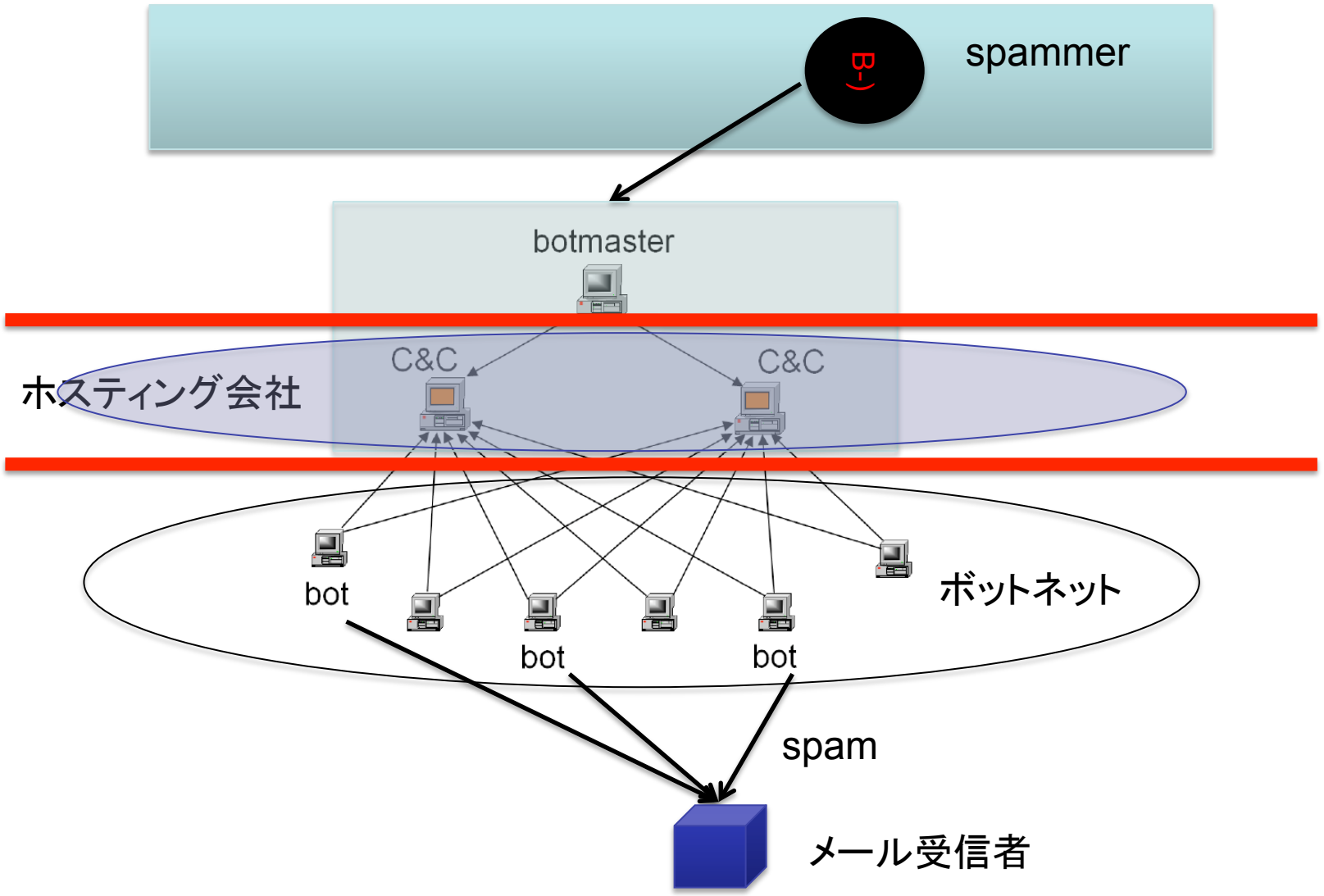


Srizbi ボットネットの勃興と衰退



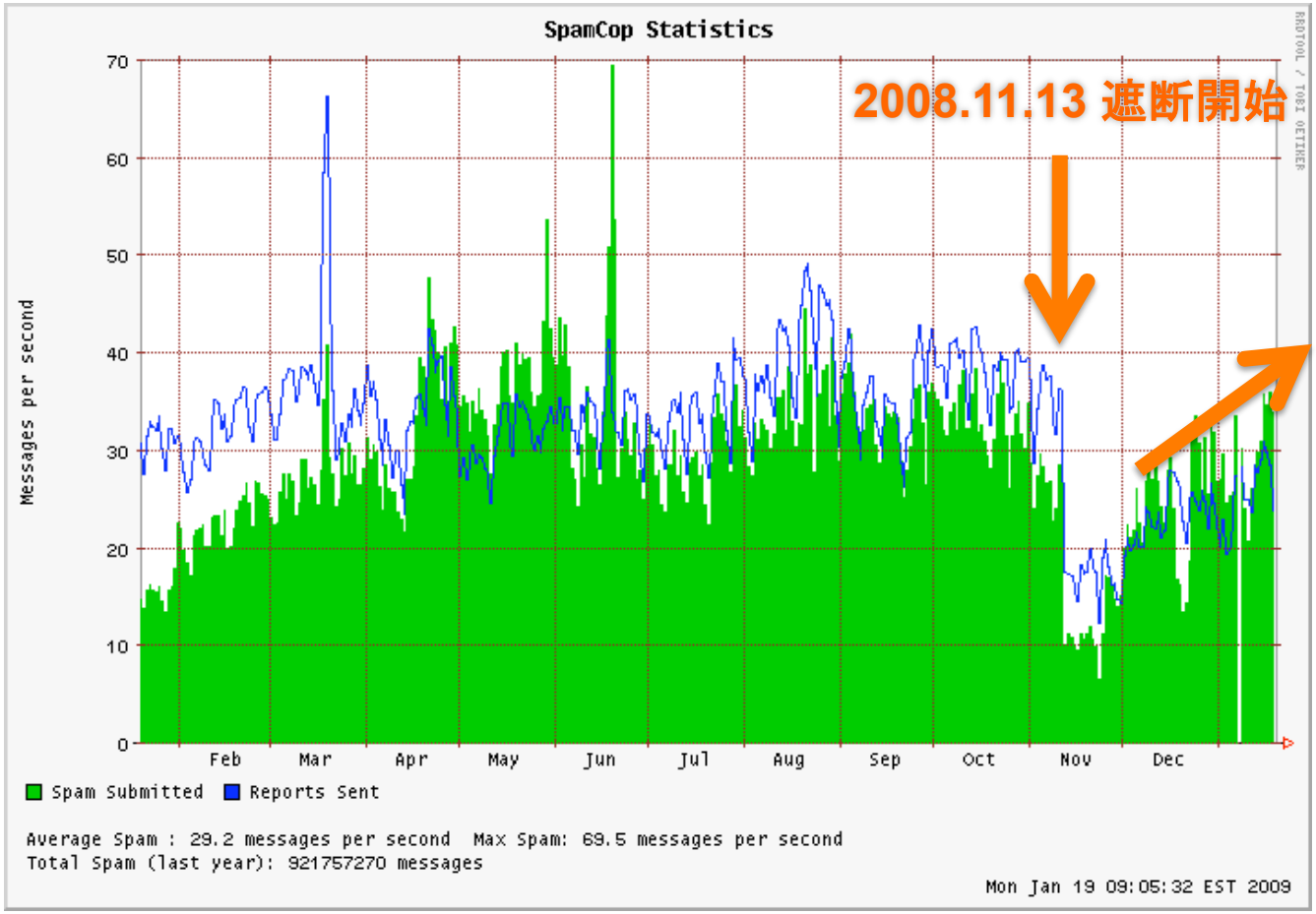
Tatsuya Mori et al.,
``Understanding the World's Worst Spamming Botnet,''
The University of Wisconsin-Madison Computer Sciences Tech Reports TR1660,

C&Cサーバを
インターネットから遮断

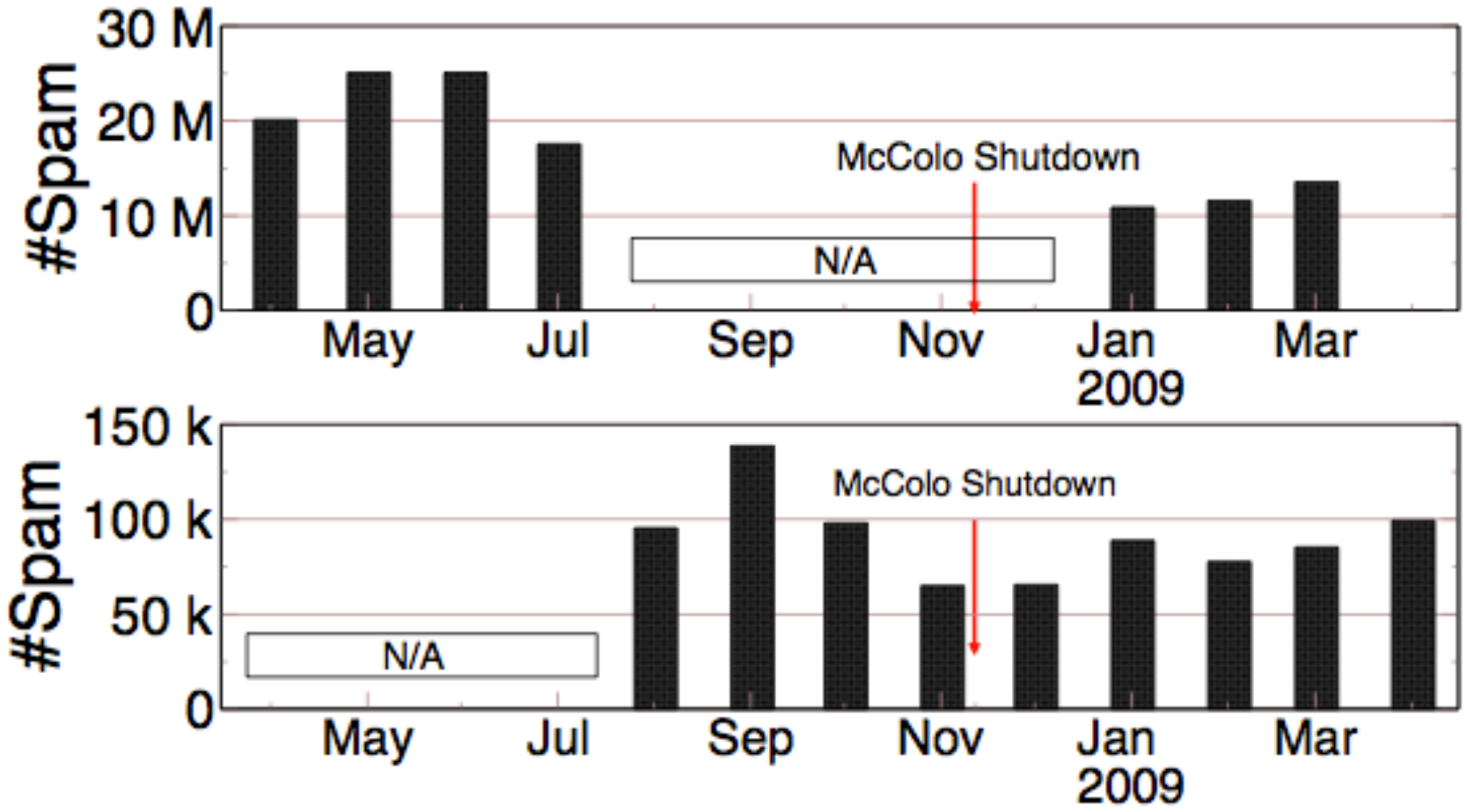


Srizbi C&Cサーバホスティング会社の遮断とその後の経過

- 2週間ほどは効果があったがその後徐々に復活した



国内企業・学術ネットワーク (GEMnet2)で観測された遮断の効果



Tatsuya Mori et al.,
``Understanding the World's Worst Spamming Botnet,''
The University of Wisconsin-Madison Computer Sciences Tech Reports TR1660,

McColo 遮断後のアクション と効果

Spammers survive botnet shutdowns

Spam levels have not been dented by a series of strikes against controllers of networks of hijacked computers.

Early 2010 has seen four such networks, or botnets, tackled via arrests, net access cutoffs and by infiltrating command systems.

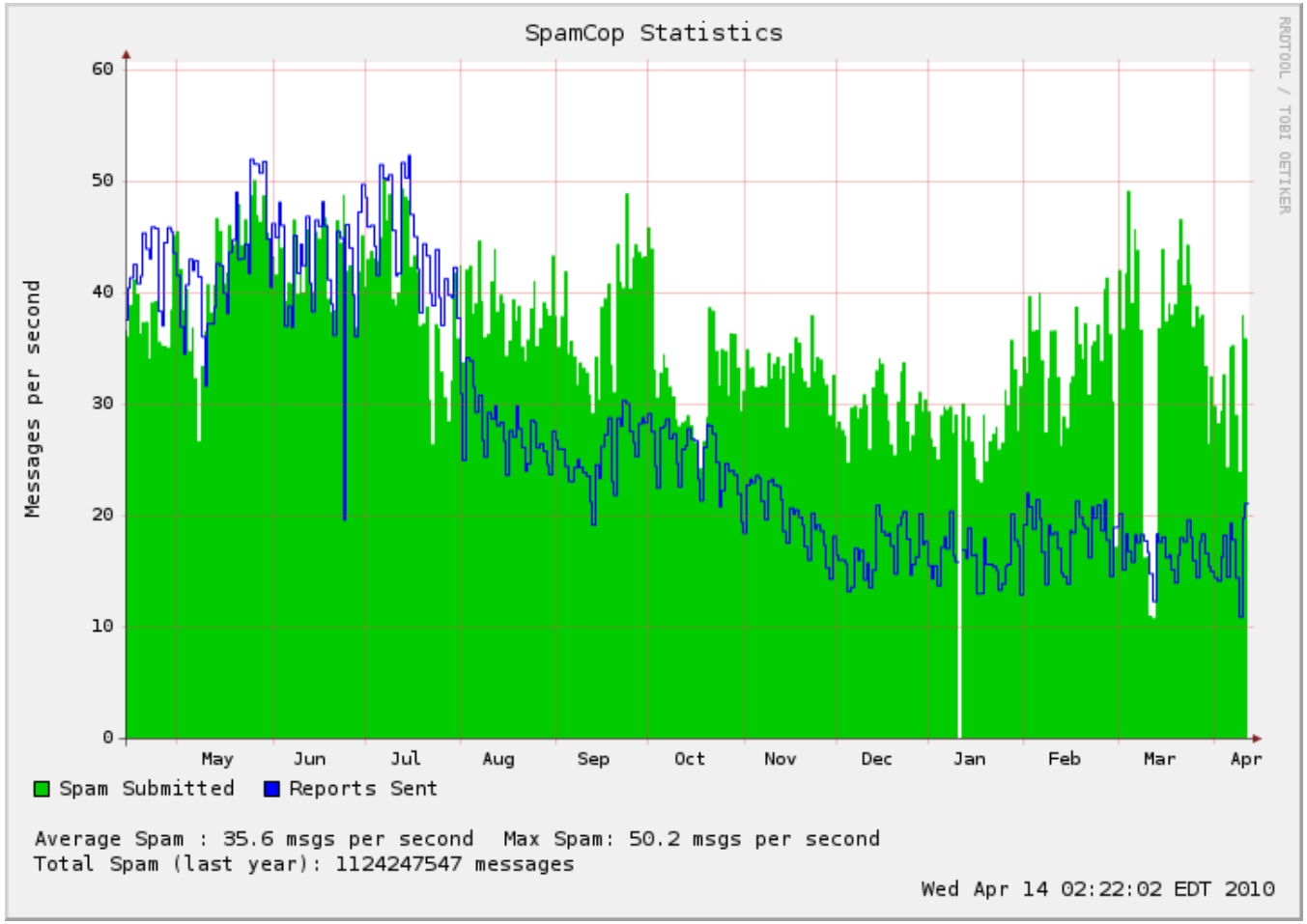
The successes have not inconvenienced hi-tech criminals who found other routes to send spam, say experts.

Most spam now travels via a botnet of hijacked PCs.

SEE A
Hacl
10 F
US
05 J
Gam
30 N
How
02 D
Botr
21 A
Spa

BBC Thursday, 18 March 2010

現在のスパム流量



http://www.spamcop.net/spamgraph.shtml?spamyear

C&C 遮断では不十分である理由

- 分業化されたマーケットとプレーヤー
  - スパマーとC&Cマスターは独立
  - C&Cが遮断されたらスパマーは別の使えるC&Cを探す
  - マルウェアも別の組織が開発・販売・サポート

ボットネット対策の根本的な難しさ

ブラックマーケットの例

allBots Inc.

Social Networking Bots

GOOD News!!! We have something more for you! Yes, we have just integrated **CAPTCHA Bypasser*** in all of our bots.

Winsock (Multi-threaded) Bots

Become an Affiliate and Start Earning Now

Click here for 30+ MySpace Bots

Accounts Creator

(You Just Need To Type In The CAPTCHAs To Create Accounts)

Social Networks			
MySpace Accounts Creator with Picture Uploader, Profile & Layout Manager	PayPal Buy Now	~~$180.95~~	$140.00
MySpace Accounts Creator with Picture Uploader, Profile & Layout Manager (Winsock)	PayPal Buy Now	~~$360.95~~	$320.00
YouTube Accounts Creator	PayPal Buy Now	~~$120.95~~	$95.00
Friendster Accounts Creator	PayPal Buy Now	~~$120.95~~	$95.00
Hi5 Accounts Creator	PayPal Buy Now	~~$120.95~~	$95.00
TagWorld Accounts Creator	PayPal		

Friend Adders, Message Senders, Comment Posters & Others

(All Bots Work In A Conventional Manner, They Gather Friend IDs/Names And Send Friend Requests, Messages, Comments Automatically)

Chaining Feature Is Available On All Bots for All Networks Except Facebook

V. Paxson, How The Pursuit of Truth Led Me To Selling Viagra, 18th USENIX Security Symposium, August 2009

ブラックマーケットの例

V. Paxson, How The Pursuit of Truth Led Me To Selling Viagra, 18th USENIX Security Symposium, August 2009

スパム対策の根源的な課題

- スパム送信のインセンティブを断絶できない
  - 送信コストがゼロに近い
  - 負のチープ革命
  - 高度に分業化されたマーケット
  - スパムが手がけるマーケットにおける需要の普遍性
- 世界的に普及してしまった電子メールサービスを止めたり変更することができない
  - プロトコル上の弱点（認証機構の欠如）＝普及上の長所（利便性）

技術的課題(1)

- スパム送信にディスインセンティブを与えるしくみ
  - ネットワークアーキテクチャが抜本的に変わるタイミングを利用
    - 新世代ネットワークアーキテクチャ

技術的課題(2)

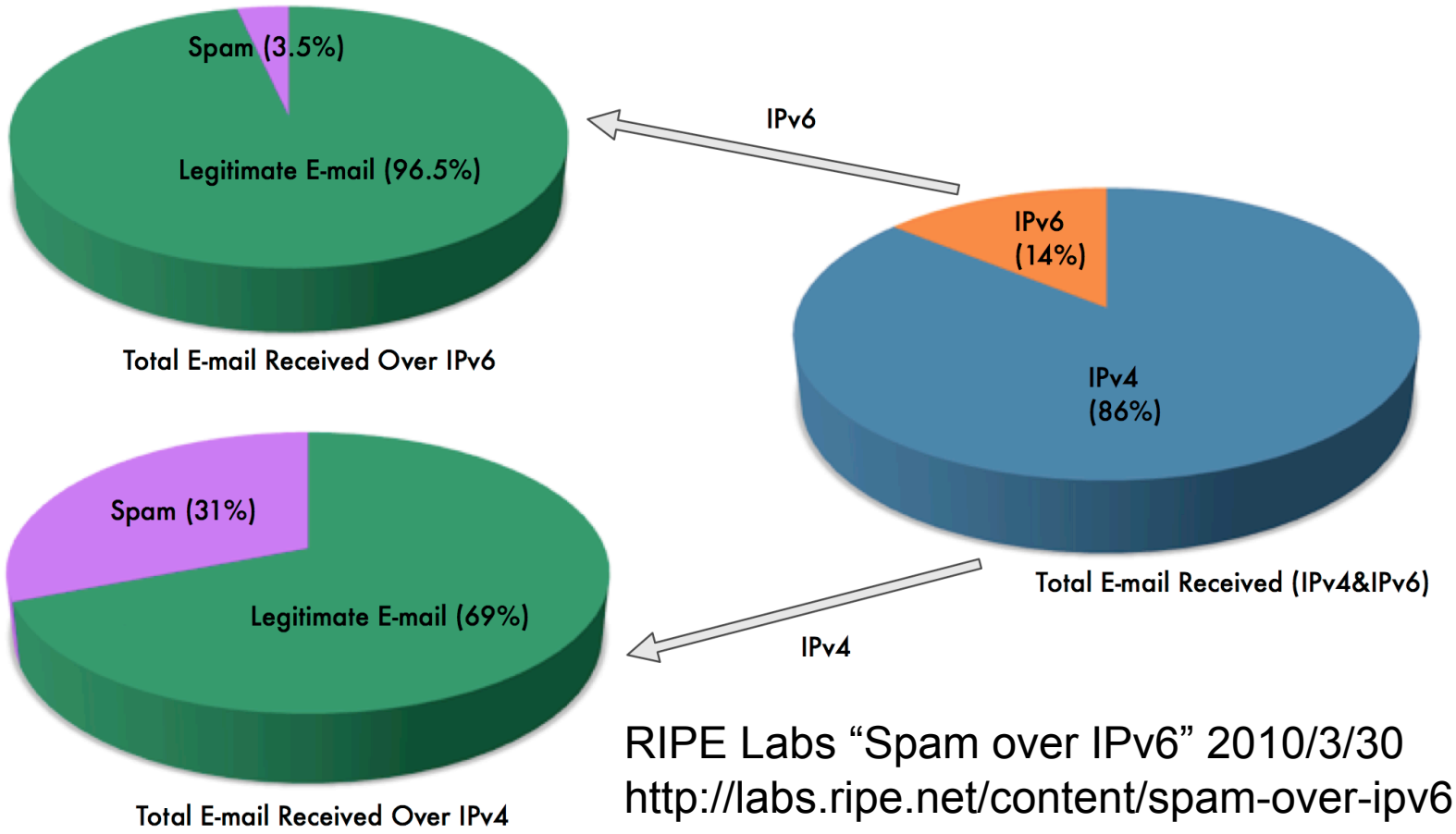
- スパム被害を受ける他の領域の分析
  - Spam over Social Networking Sites
  - Spam on YouTube
  - Spam on blog comments
  - Spam over IP Telephony (SPIT)
  - Spam over Internet Message (SPIM)

技術的課題(3)

- 従来手法の高精度・高効率化
  - スケーラブルなフィルタリング技術
    - 大規模データ
    - 超高速回線
  - フィードバックを活用したフィルタリング
    - 汎用的な ”This is a spam button”

技術的課題(4)

- IPv6 の普及とスパム（ボット）



RIPE Labs “Spam over IPv6” 2010/3/30
http://labs.ripe.net/content/spam-over-ipv6

今後の展開

- 非技術的解決手段
  - 法律の整備
  - 国際協調
    - OP25B の世界的普及
  - リテラシー向上（マルウェア感染の成功率をある程度まで下げる）

まとめ

- スパム増大に伴なうコストは無視できない
  - メールはお金にならないが重要なインフラ
- スパムの実態と代表的な対策技術
- スパムが増大し続ける主要因
  - マーケットの存在と入り組んだプレーヤー
- スパムボットの実態と対策
  - C&Cサーバ遮断をケーススタディとして
- ボットネット対策の根本的な難しさと考えうる技術的・非技術的方向性

参考情報

Greylisting

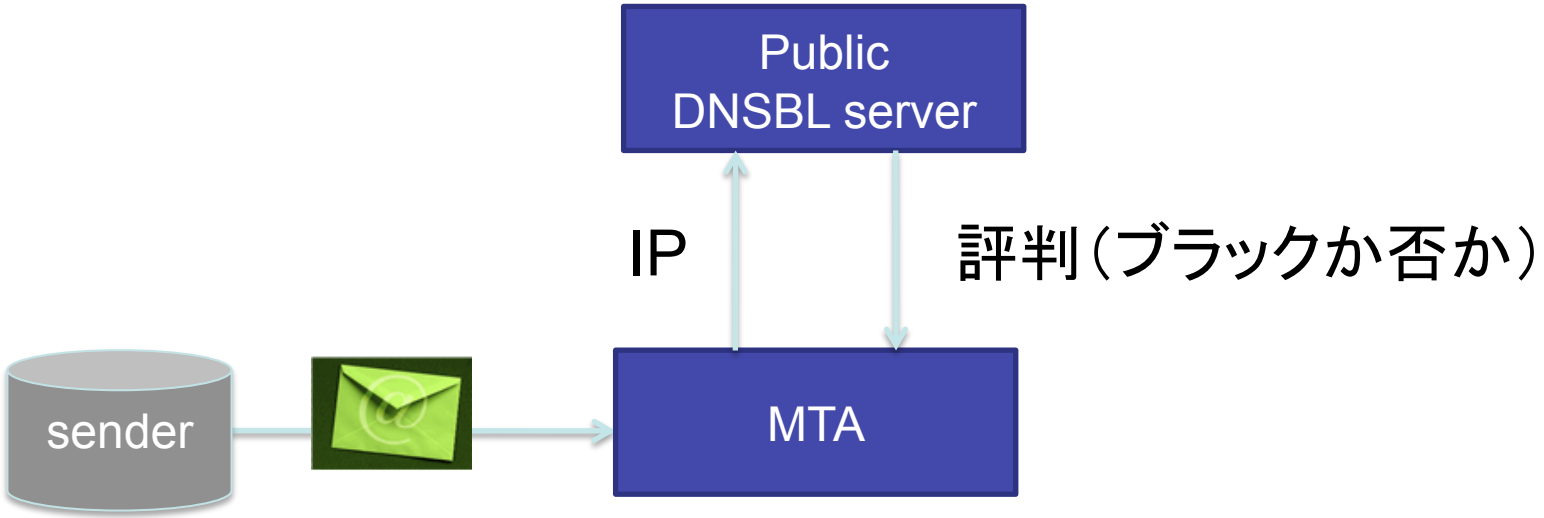
{ip, from, to}

初見の組み合わせ→ 拒否
二度目以降→受信

botnet のようなスパム送信ホストは再送しないというのが前提
IPアドレスやメッセージの中身に依存しないホストの挙動を利用した手法

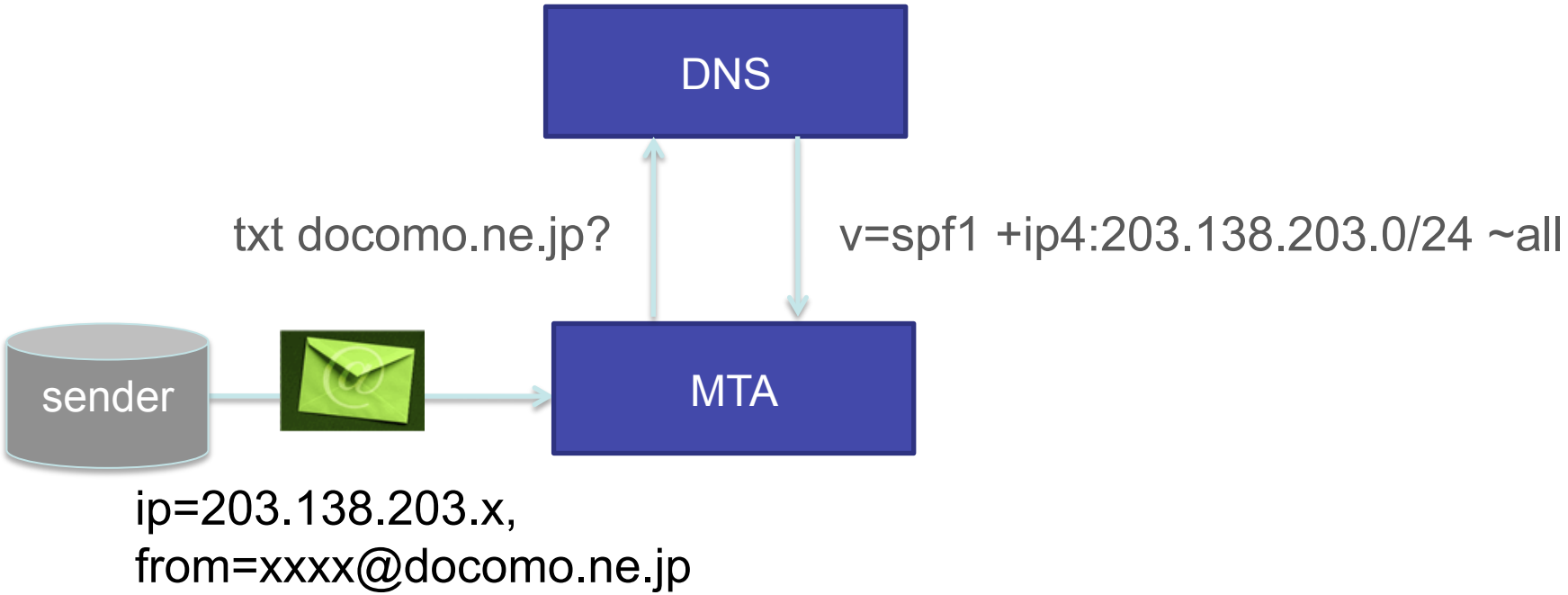
DNSBL (DNS Black list)

IPアドレスの評判(black list)をDNS インタフェースで提供



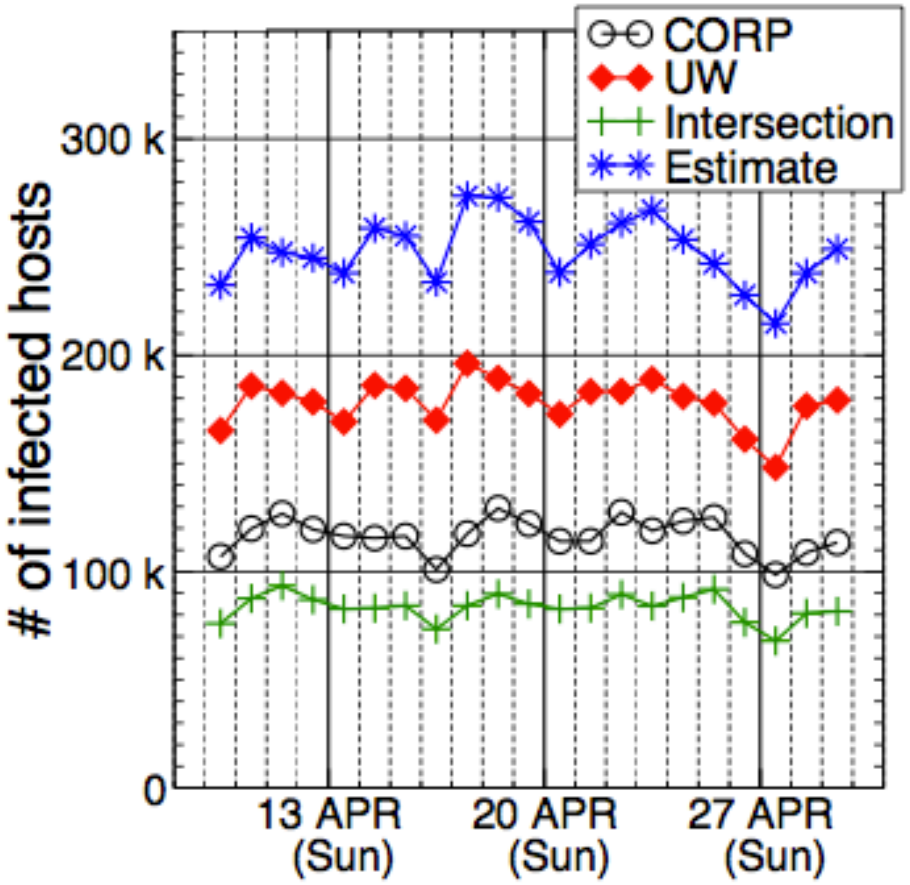

```
% nslookup 90.57.60.129.sbl.spamhaus.org
** server can't find 90.57.60.129.sbl.spamhaus.org: NXDOMAIN

% nslookup 93.12.186.222.sbl.spamhaus.org
Non-authoritative answer:
Name:   93.12.186.222.sbl.spamhaus.org
Address: 127.0.0.2
```

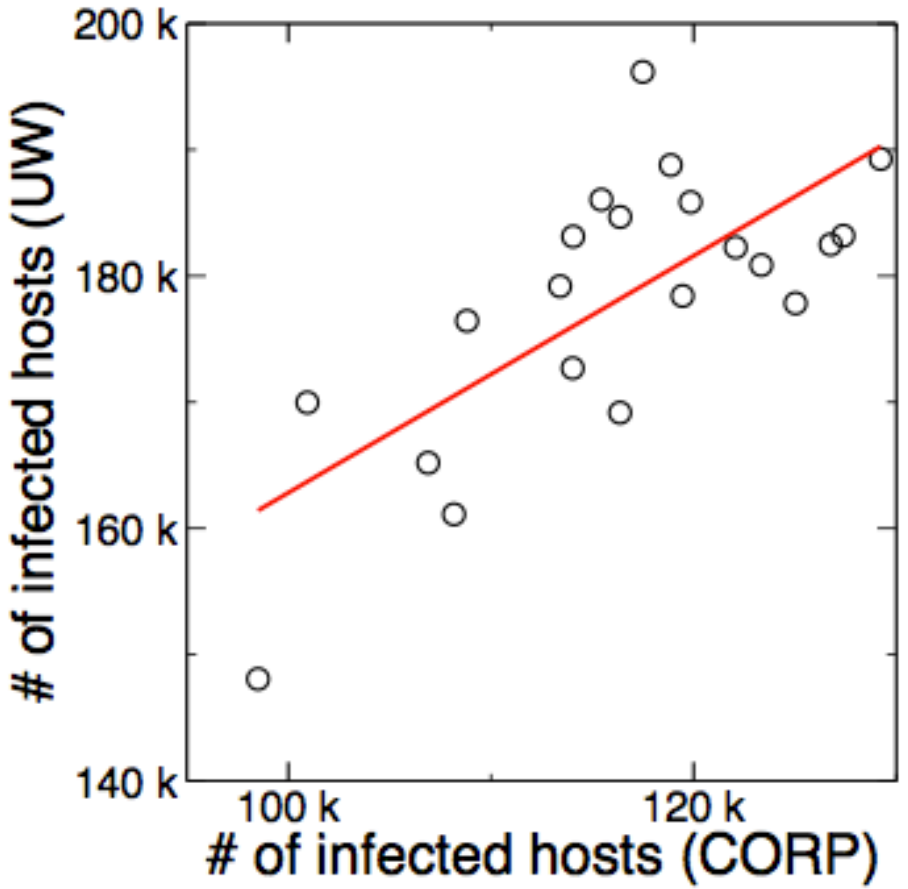
SPF (Sender Policy Framework)



送信してきたホストのIP が該当ドメインのSPFに記載されている
アドレスにマッチするか否かを調べる。
※マッチしない → 詐称というわけでは必ずしもない（移動先での
メール送信など）。

Srizbiの母集団推定分析





Tatsuya Mori et al.,
``Understanding the World's Worst Spamming Botnet,''
The University of Wisconsin-Madison Computer Sciences Tech Reports TR1660,