ネットワークから見たスパム・マルウェアの研究とその舞台裏

ISSスクエア・ネットワーク分科会

2010/11/13

NTTサービスインテグレーショ基盤研究所

森　達哉

自己紹介

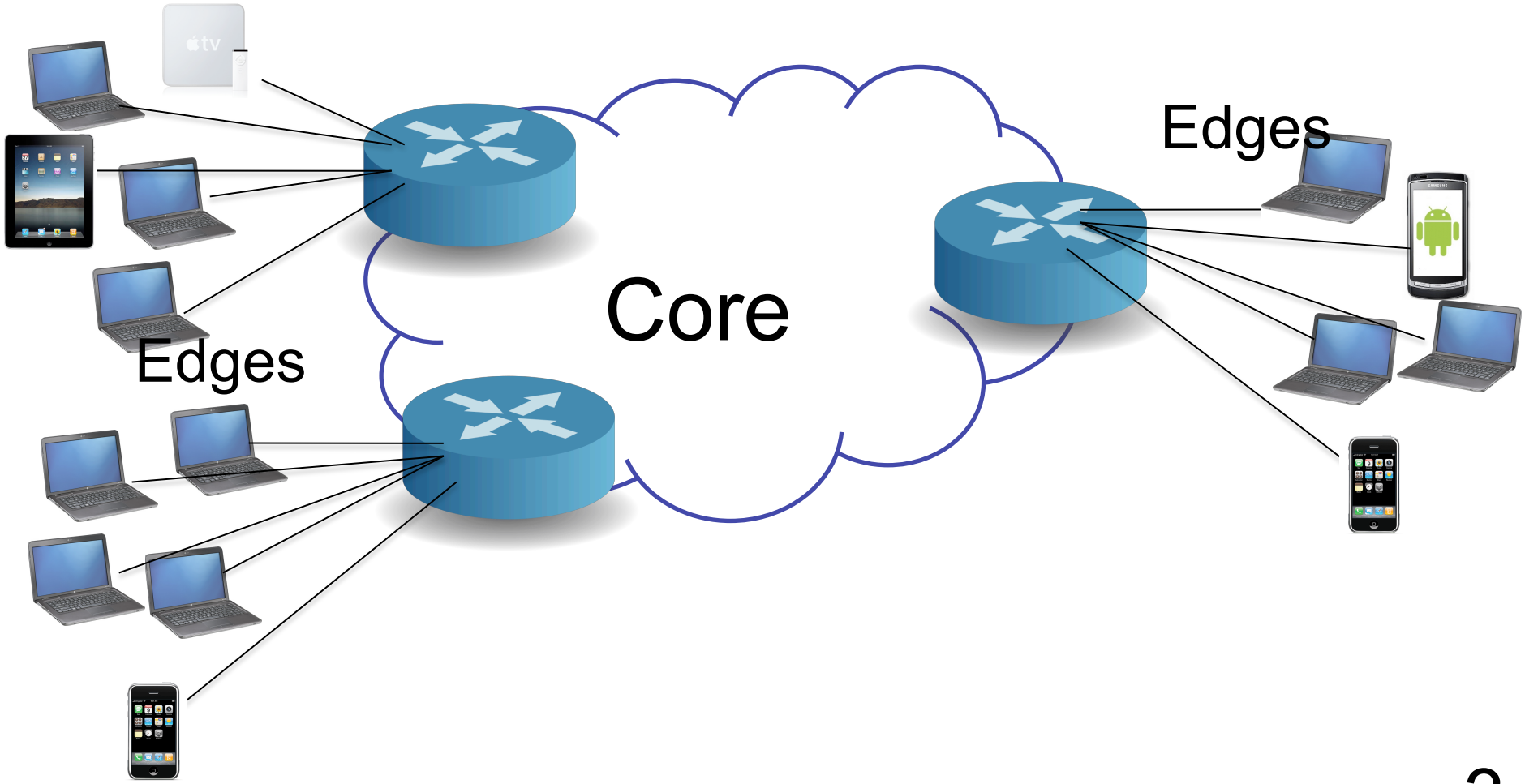
- 1999年よりNTT研究所
- 主にネットワークの計測・分析に関する研究
  - 「トラヒック」解析。性能品質評価。
  - P2Pがネットワークインフラに与える影響
- 2004年ごろよりセキュリティ的なテーマ
  - ネットワーク上の異常検出、ワーム検出
  - スパム・マルウェア (2007年～)
- 最近は大規模データ分析・クラウド等にも興味あり

アジェンダ

- イントロ
  - ネットワークから見るセキュリティ
- 表舞台の話
  - いくつかの研究事例紹介
- 舞台裏の話
  - データの収集
  - データの料理

ネットワークから見るセキュリティ

個々のエッジではなく、ネットワークのコアで見る



ネットワークで見るメリット

- 集約された情報・トレンドを把握出来る
  - Worm/Malware outbreak, DDoS attack
  - 事象の空間的広がり・波及の把握
  - 木でなく森を見る
  - １サンプルではなく、統計的アプローチが可能に
- 通信の大域的なパターンがわかる
  - いつ、誰が、どこから、どこへ
  - Network scan, Darknet monitoring
- 効果的かつ迅速な制御へのフィードバック
  - IPアドレス・ポートのフィルタリング

ネットワークで見るデメリットと課題

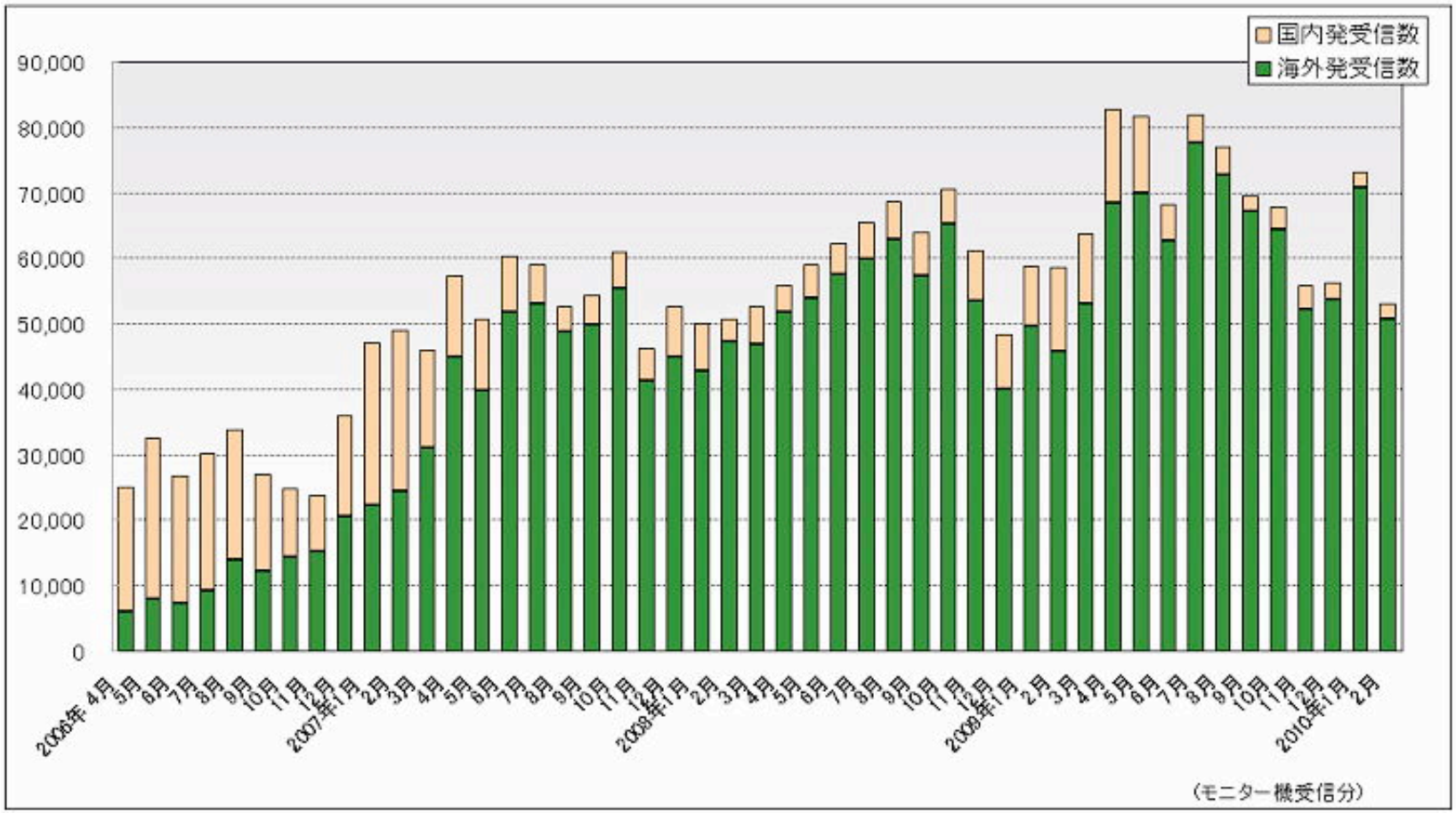
- ネットワーク層で得られる情報には限界あり
  - DPI出来ない暗号化・難読化
  - 攻撃を実行したシステムの状態
    - システムでの挙動や脆弱性についてはわからない
  - サーバの分析と組み合わせることが望ましい
- 技術的課題
  - Per-packet processing overhead
    - 100 Gbps 超の世界はどうするか:
      → Open problem
  - どこにでも監視ポイントをおけるわけではない
    - 簡単なしくみを

ネットワークから見る
セキュリティ分析

- 今回ご紹介するお話
  - スパム送信源の分析
  - マルウェアを送受信する通信の検出
- それぞれの研究テーマのモチベーションは何か。全体像の中での位置づけは何か
  - High-level picture
- この分野のおもしろさ
  - 様々な対象がある moving target
  - 大規模なデータ収集・分析→並列分散処理・統計数理の手法が有効 (学際的なアプローチ)

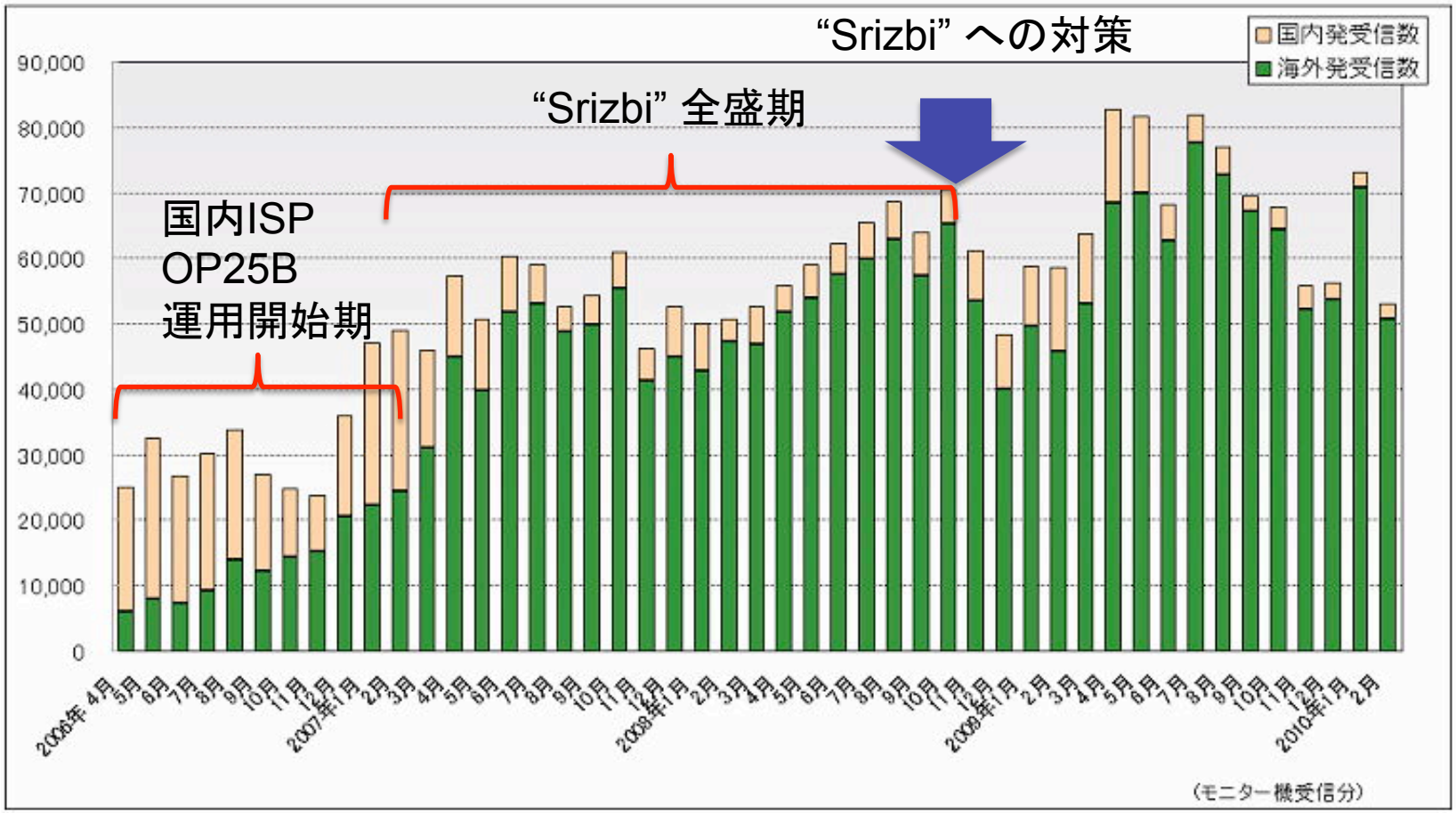
表舞台

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

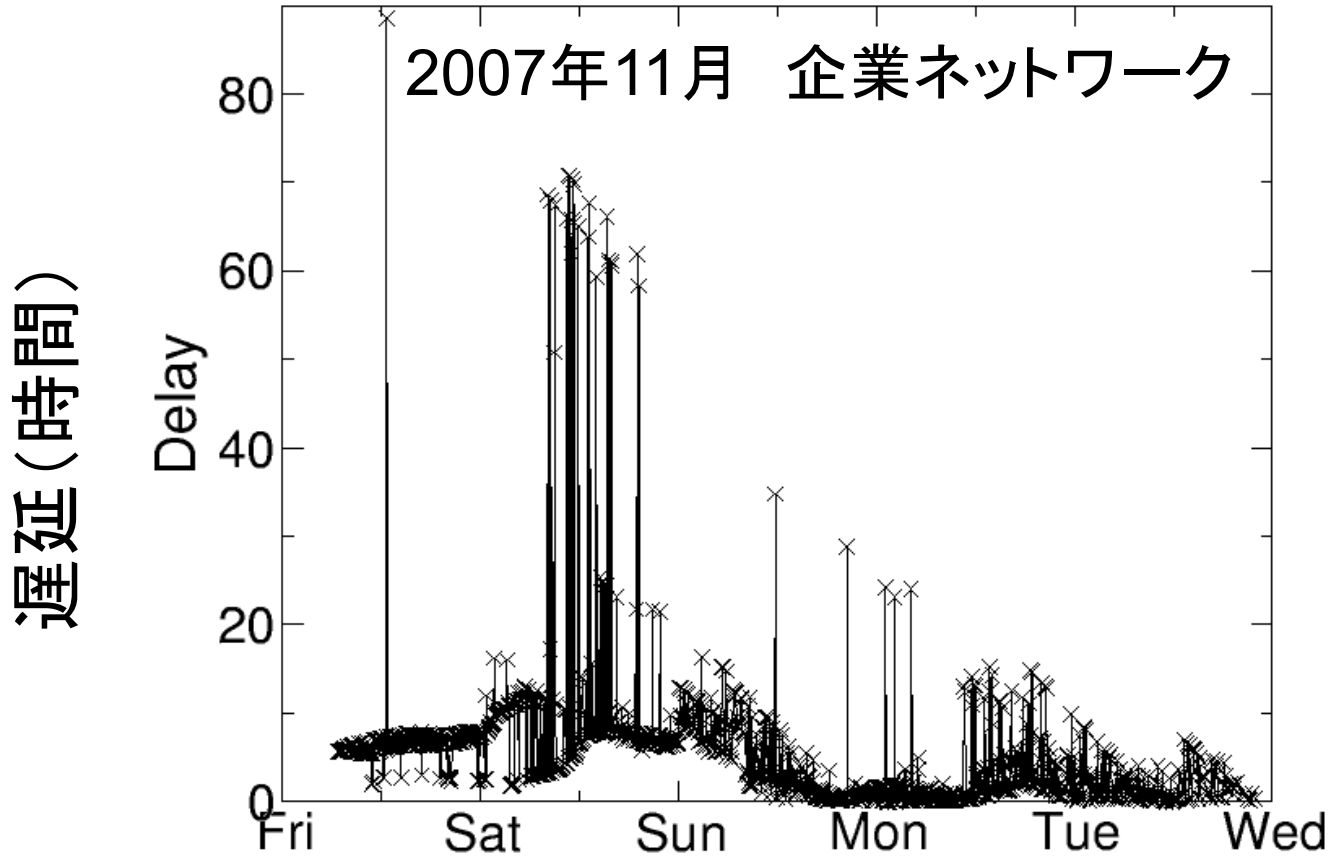
Lost Salary (yearly):	$6,635,417
Lost Productivity (yearly):	6337 days

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

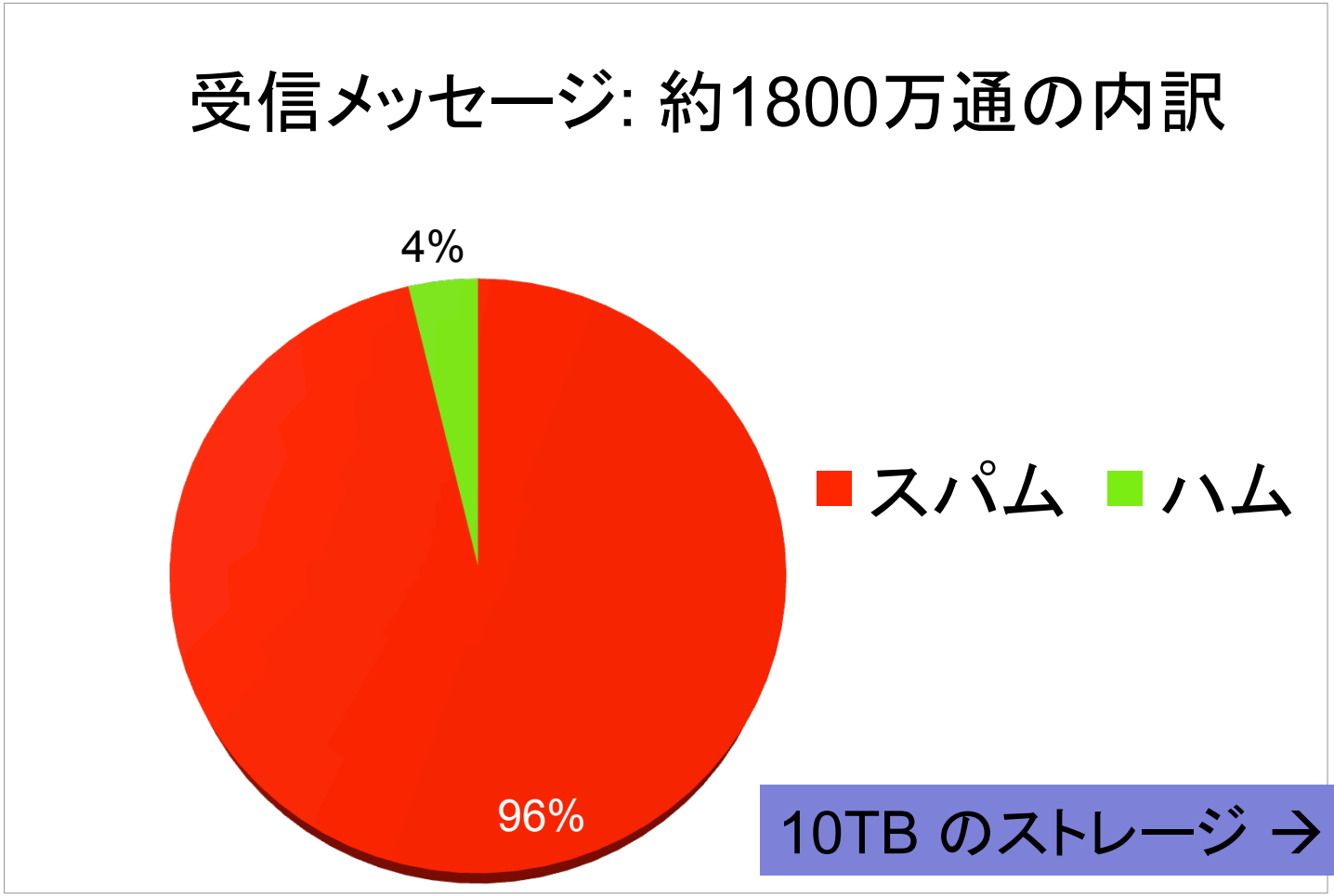
年間損失生産性　6337人日

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



スパム増大でメールが数日遅延あるいはロストという自体に

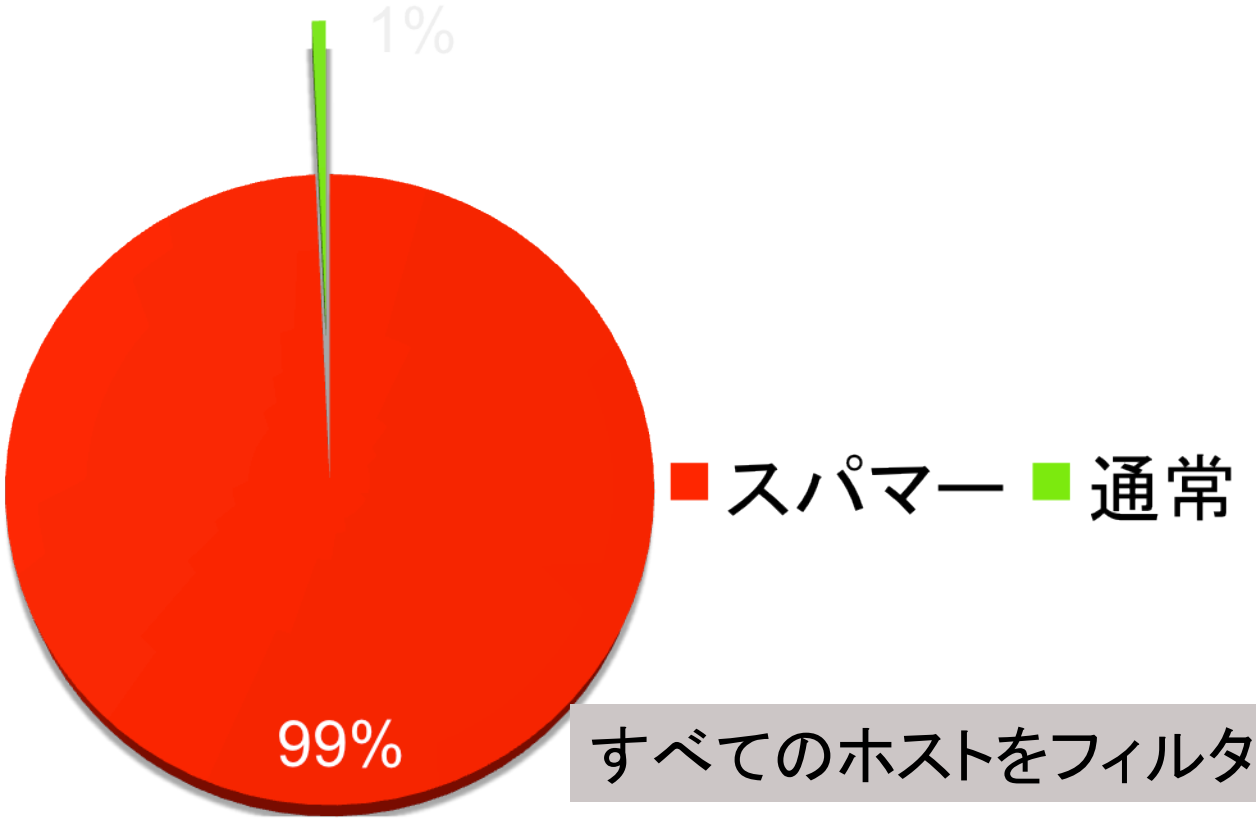
ある企業のメールサーバにおける 1ヶ月のメール受信状況



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

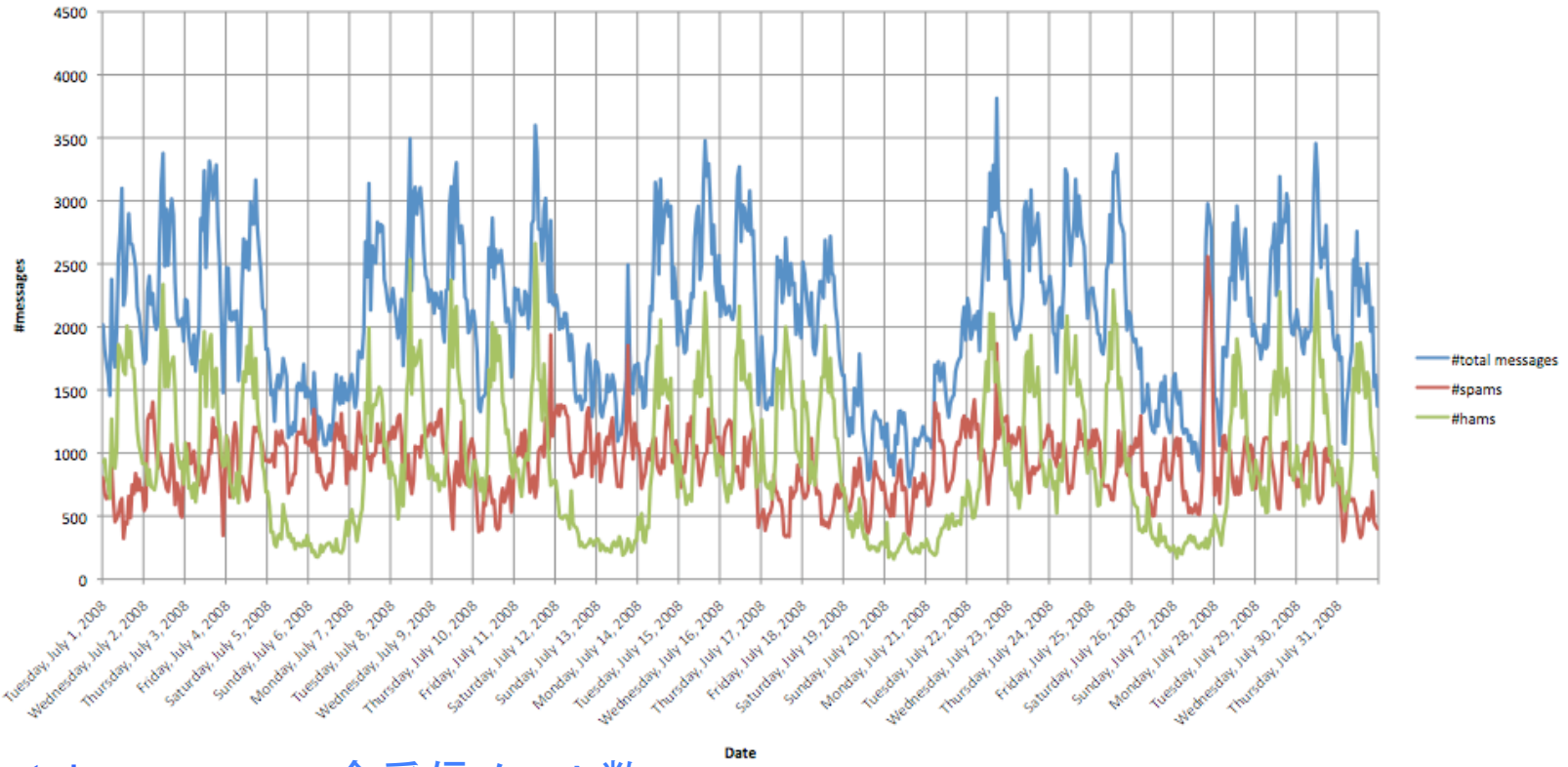
メールの9割は「迷惑メール」、そのうち2割弱は「詐欺メール」

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 >>

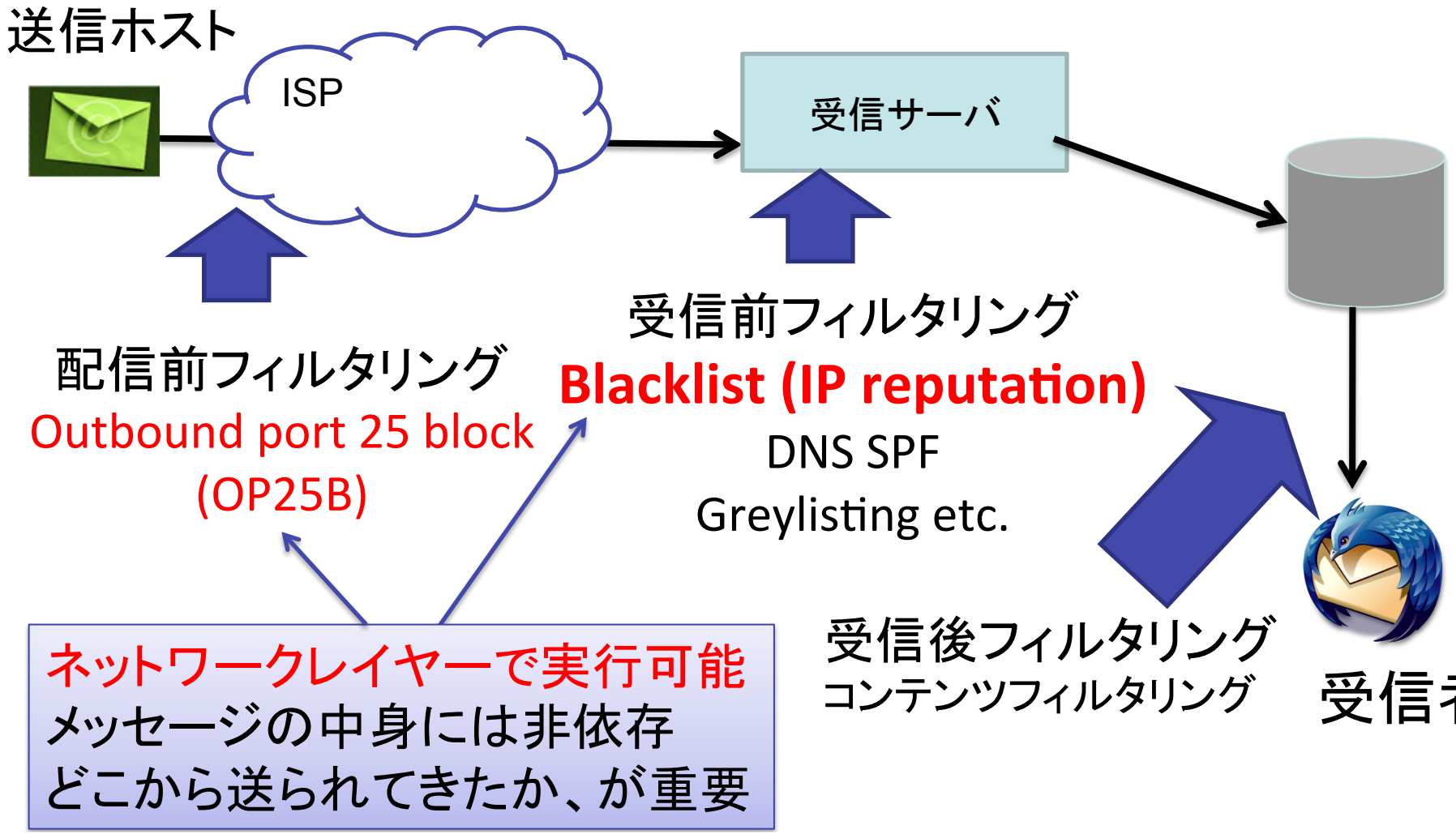
セキュリティ企業の米シマンテックは2010年4月16日、同社の観測データを基に、2010年3月の迷惑メール（スパム）動向を発表した。同社が観測したメールのおよそ9割が迷惑メールで、そのうちの17%が詐欺目的のメールだったという。

（余談）受信メッセージの時間変動パターン



#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。

今日の代表的なスパム対策技術



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

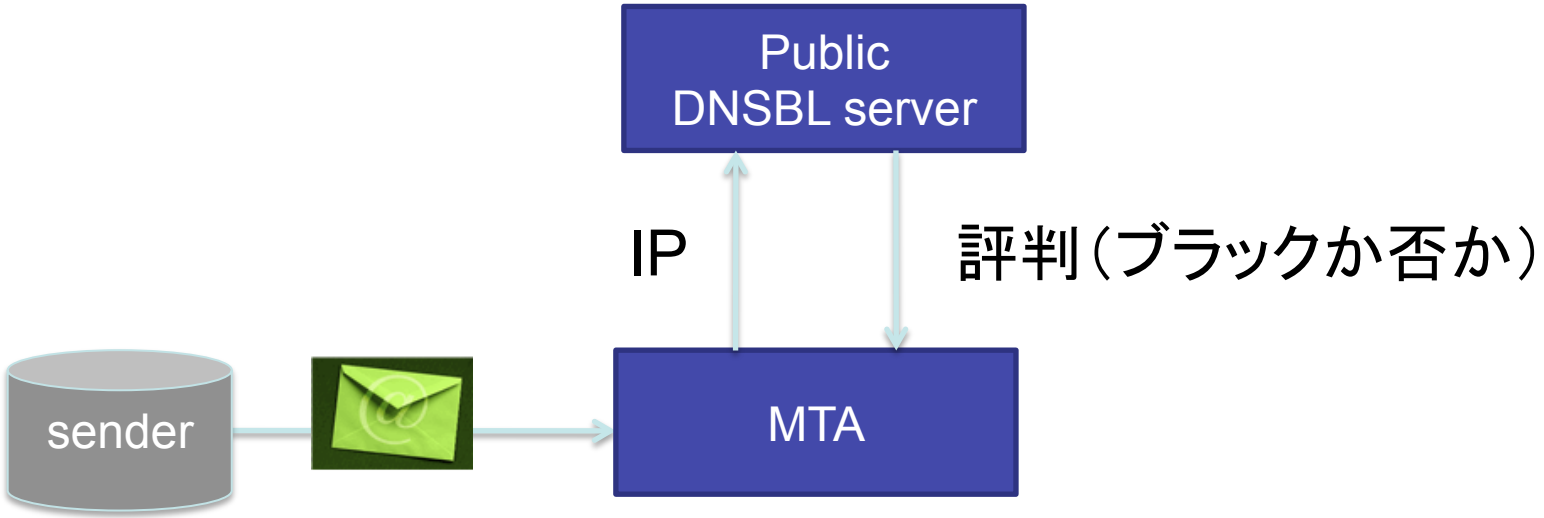
- 世界的にこのような機運が高まることで効果が期待できる（ただし抜け道もあるが）
- 通信の制御に対するポリシーは国によって様々

IP reputation

- IPアドレスあるいはブロックに対して格付けをするしくみ
- Black list, White list
- オープンなものとしては spamhaus が有名
  - http://www.spamhaus.org/
- スパムアプライアンスベンダーは各社自前のIP reputation DBを構築
  - 構築方法は一般に非公開
  - Honeypot, spamtrap などを利用と考えられる
- DNSBL(DNSWL)では DNS をIFとして使う

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
```

ネットワークレイヤーでの スパム対策の優位性

- メッセージを処理する必要がない
  - 文字列解析、自然言語処理、添付ファイルの解凍、スキャン、OCR等一切不要
- 情報の管理が簡便
  - 基本はIPアドレスリストのみ
- Router/Middle box での制御が簡便
  - ポートフィルタリング (OP25B)
  - IP フィルタリング　(IP reputation)
- 実際にかなりの有効性がある（後述）

なぜIPアドレスを元にした スパム検出がうまくいくのか？

- 送信元の（偽装不可能な）特徴に秘密があり
  → スパム送信源の分析に関する研究
- スパム送信システムの内訳
- スパム送信源の地理的分散

研究(1)
IP reputation の有効性評価

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)

主要なスパム送信システム

- 通常のサーバ
  - ISP，企業, 政府, Hotmail, Gmail, etc.
- ボットネット（マルウェアに感染したエンドホスト）
- 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

スパム送信システムの内訳

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 %

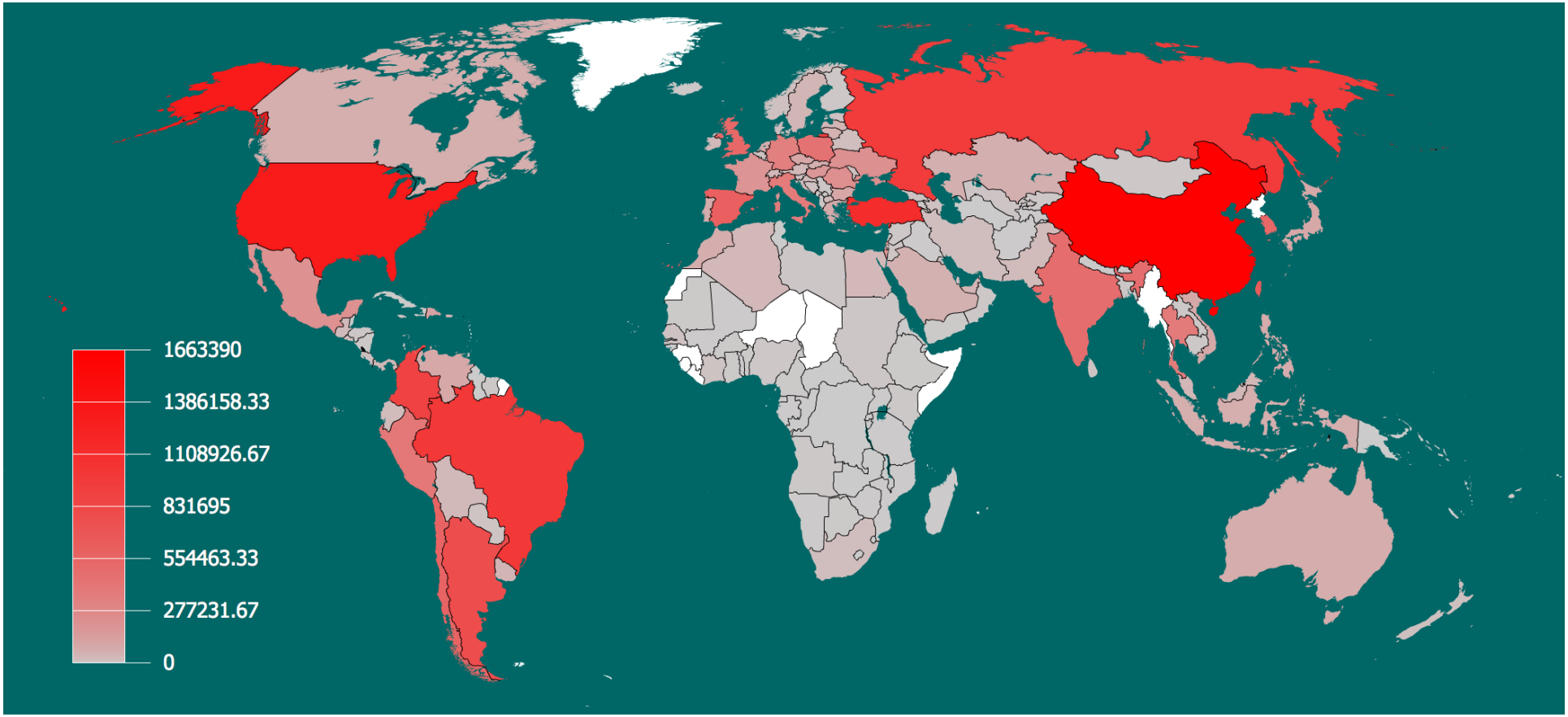
各種IP list, DNS heuristics, IP block analysis, hijacked BGP prefix などを使って分類

スパム送信システム

- ボット(End-hosts)が大半
- ついでホスティングサーバ系 (bullet-proof hosting)
  - 「悪の」ISP、ホスティング会社

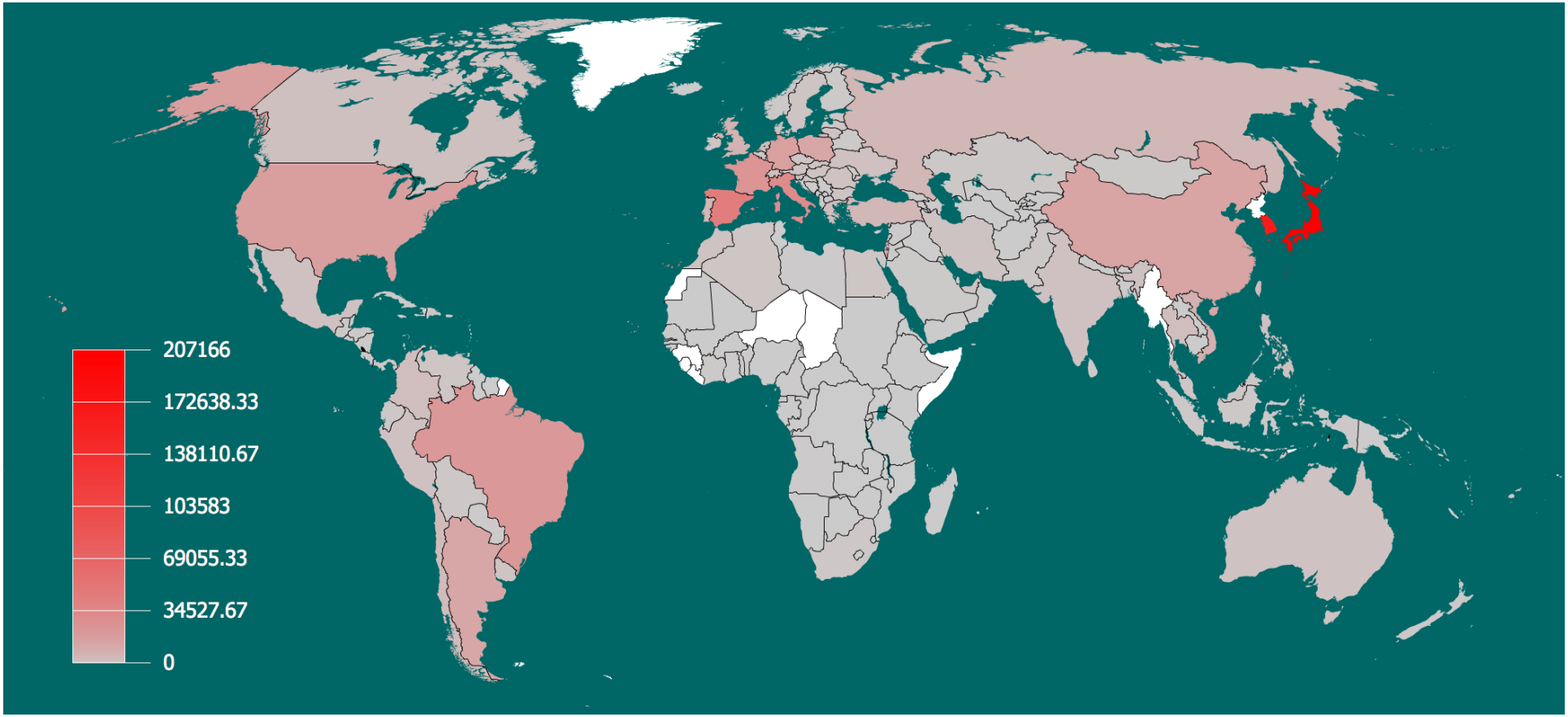
→これらのアドレスが突き止められればスパムの大部分（すべてではない）を抑えられるはず。

ボット発スパムの送信元



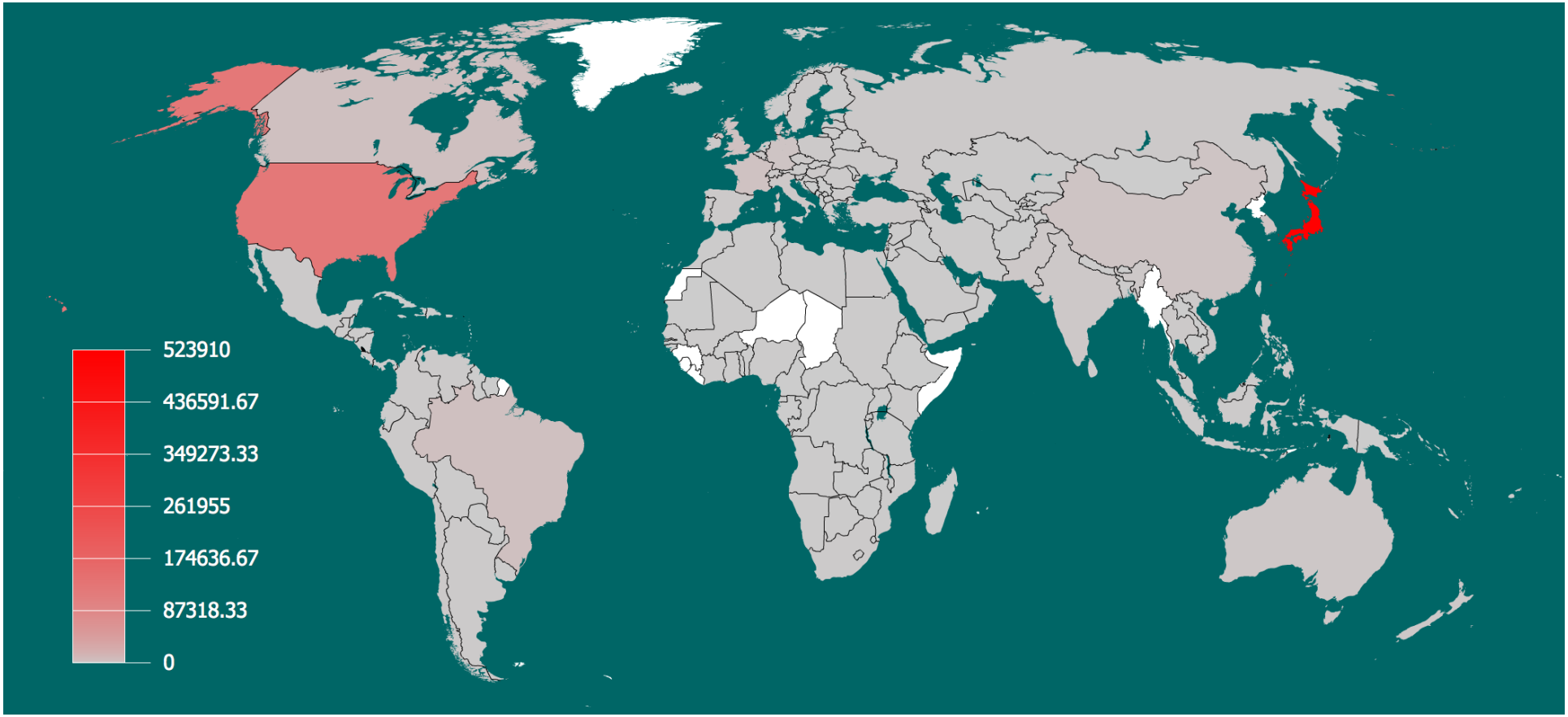
BRICs 諸国を中心とした一部の国に集中

ホスティングサーバ発
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

通常メールの送信元



日米に集中

スパム送信源

- 一部の国・ISPに集中する傾向あり
- システム毎に異なる傾向がある

→この特徴を利用したスパム検出が可能では？

研究(2)
スパム送信ホストの特徴を利用したスパム検出

森
“PrBL:スパムメールのための確率的なブラックリストの提案”
IEICE NS 2009-03 研究会

送信源情報を元にしたスパム検出

- メール送信ホストの特徴としてIPアドレスの所属, DNS情報, OS等のメッセージの中身に依存しない量を採用
- 機械学習により、観測したホストの特徴からそのホストのクラスを確率的に判定する
  →柔軟な判定が可能
- 機械学習手法として、ナイーブベイズを利用
  - 計算量が少ない割に精度がわりと高いのがメリット

利用するホスト毎の特徴量

- ネットワークロケーション
  - 地理: Country Code,
  - 論理: BGP Prefix, ASN
- DNS
  - RDNS（逆引き）の有無
- Host (OS)
  - Passive fingerprint

- それぞれスパマー，通常ホストで傾向が大きく異なるものを採用
  - それぞれ単一ではエラーが多いが，複数の証拠を組み合わせることで精度をあげることが狙い
  - オペレータの rule-of-thumb を定量化・自動化

メール送信ホストのクラス分類

- C1: spammer
  - 送信したメールの9割以上がspamメールであるあるいは、メッセージ送信0かつ10以上 greylisting でフィルタされたホスト
- C2: legit
  - 送信したメールの9割以上がhamメールである
- unknown
  - 上記以外（クラスを判定するのに十分な数がない）

Naïve Bayesian Classifier

- **学習**
  - **あるホストのクラスが** Ci **であるとき、その ホストの特徴が A である確率(尤度)を算出**
  - **同時に事前確率** P(Ci) **を保持**

$$P(\mathbf{A}|C_i) = P(A_1, A_2, ...|C_i)$$

Naïve Bayesian Classifier

- **判定**
  - 観測したホストの特徴 A より、そのホストのクラスが Ci である確率(事後確率)を算出
  - ベイズの定理 + 独立性仮定

→Ci を最大事後確率(MAP)により判定

$$P(C_i|\mathbf{A}) = \frac{P(C_i)}{P(\mathbf{A})} \prod_j P(A_j = a_{jk}|C_i)$$

クラスが2値の場合のスコア(確率)

- C_1: spammer, C_2: legit
- p = Pr[C_1|A], q = 1- p = Pr[C_2|A]
- 対数オッズ比をとることで、下記を得る (0 <= p <= 1)

$$p = \frac{1}{1 + e^{-\left(\sum_j w_j\right) - b}}$$

$$w_j = \log P(A_j = a_{jk}|C_1) - \log P(A_j = a_{jk}|C_2)$$

$$b = \log P(C_1) - \log P(C_2)$$

$p > p_\theta$ → spammer 判定
$q < q_\theta$ → legit 判定

分析したデータ

- 対象
  - 企業網メール、約3000名が利用
  - 計測期間: 2008年4月～2008年7月

- 運用
  - White list のみを無条件で通過させる Selective greylisting を運用中
    - それ以外のコネクションはすべて1度目は greylisting で弾かれる
  - 商用迷惑メールフィルタソフトウェアにより、すべてのメッセージにスコアがつく

分類した例

ホストの分類

分類したクラス

	spammer	legit	unknown	total
spammer	46702	9	14905	61616
legit	2	273	84	359
unknown	169849	845	41335	212029

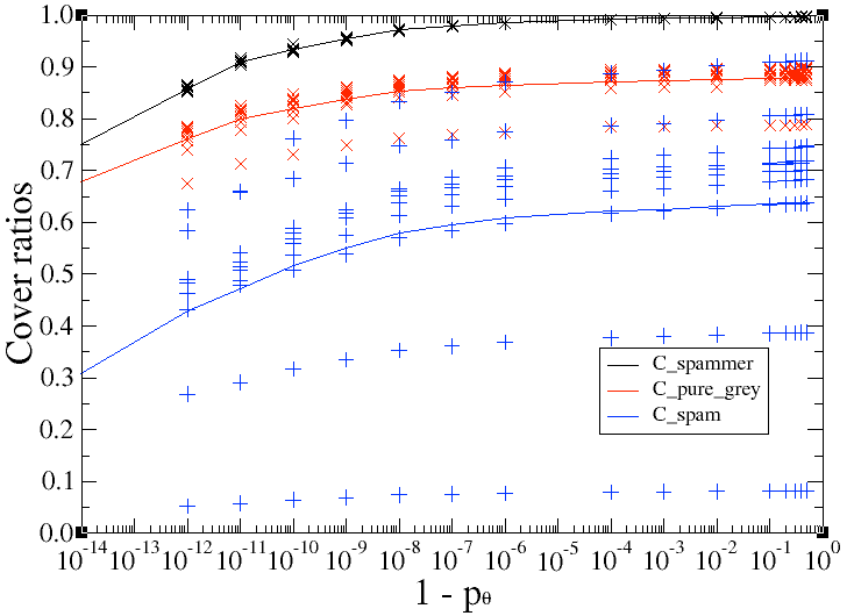
メッセージの分類

分類したクラス

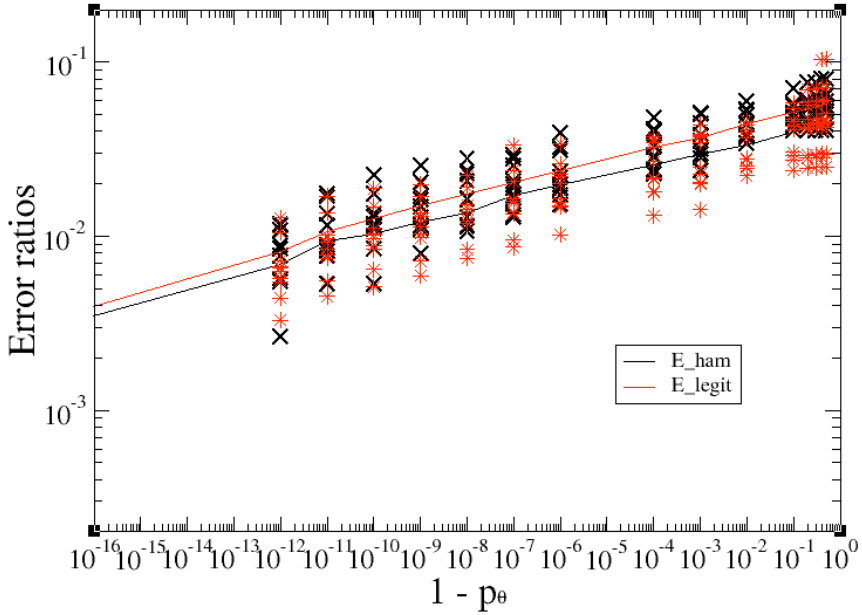
	#delivered	#spams	#hams	#undelivered spam
spammer	14479	13439	155	1877822
legit	99918	26204	63306	335
unknown	64022	34150	19503	563018
total	178419	73793	82964	2441175

カバー率と精度のトレードオフ

カバー率



精度(false positive rate)



2008/4 のデータに対し、10-fold cross validation を適用
実線は10回の試行の平均値

スパム送信元の大半はボット

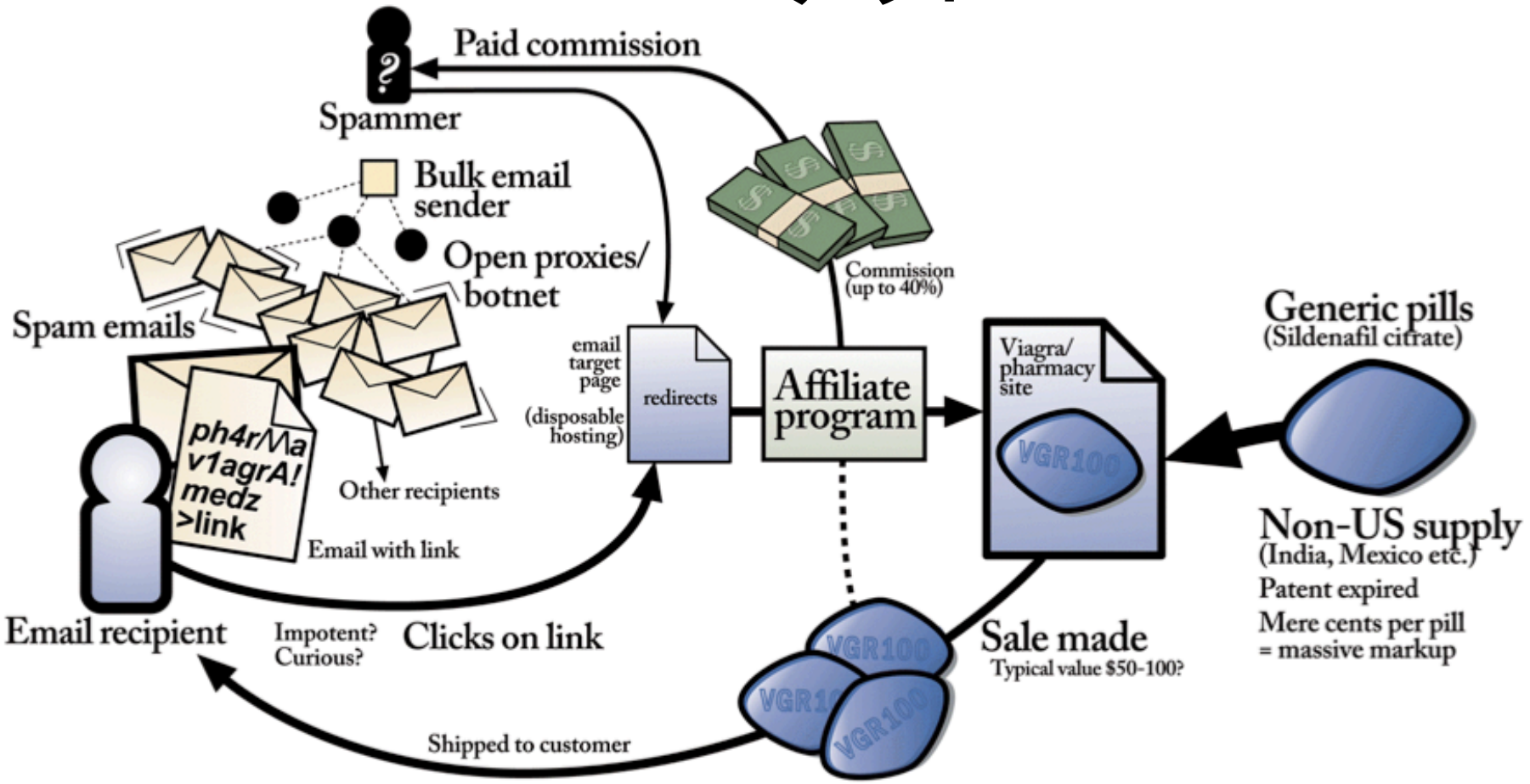
→スパムボットに関して
調べてみよう

代表的なスパムボットの歴史

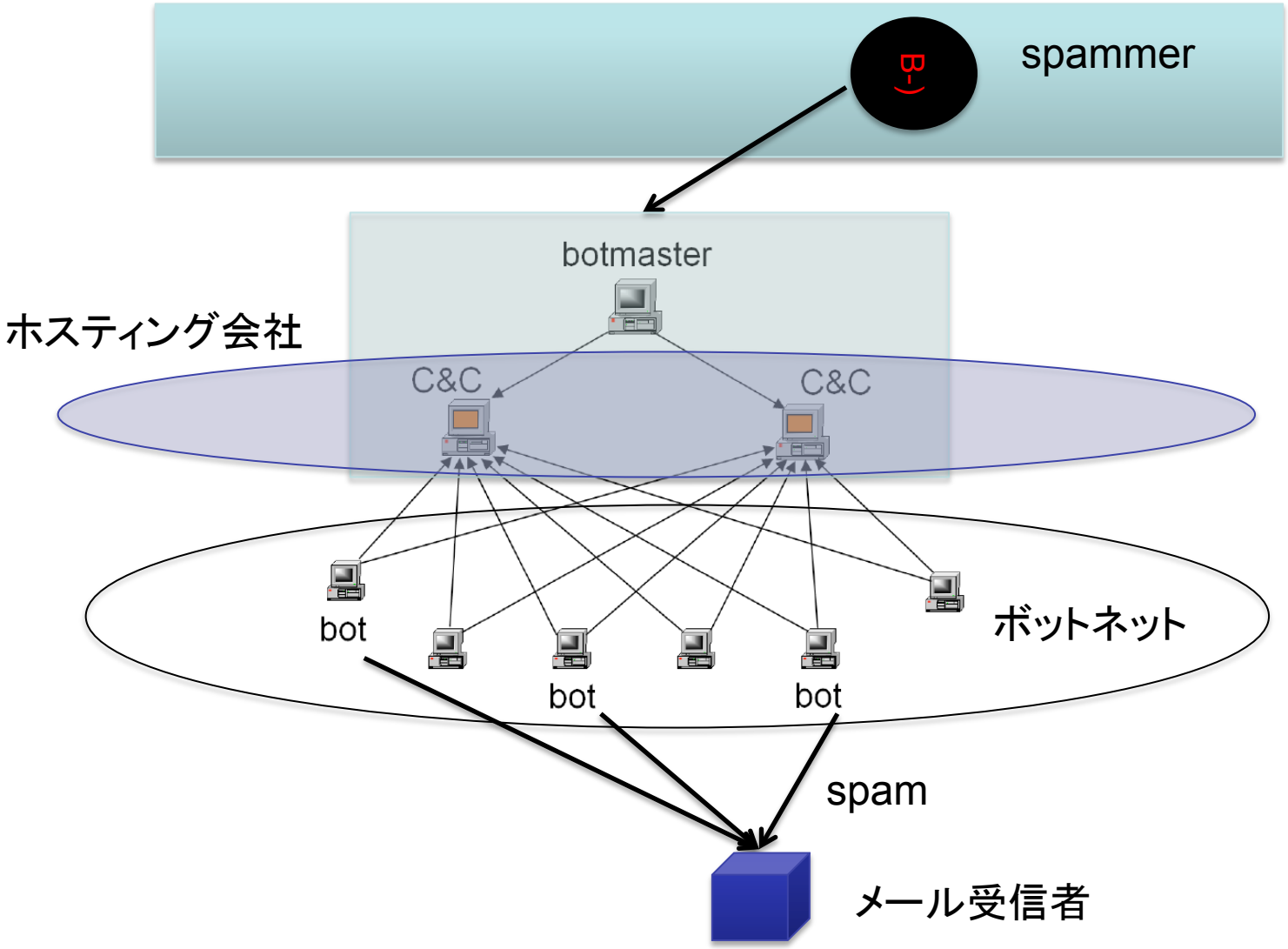
- 1996/8: SilverNet
- 2004頃～　スパム送信手段として定着し始める
- 2005～: SD-bot
- 2006?～: Mega-D　3.5万ホスト 100億通/日
- 2007～: Storm　　100万ホスト　30億通/日
- 2007～: Srizbi　　200万ホスト　600億通/日
- 2008～: Confiker　1000万ホスト 100億通/日

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

スパム送信のインセンティブ =マーケット



ボットによるスパム送信



スパムボットを検出するための
ネットワークレイヤーでの
特徴はないか？

→ある（あった・過去形）

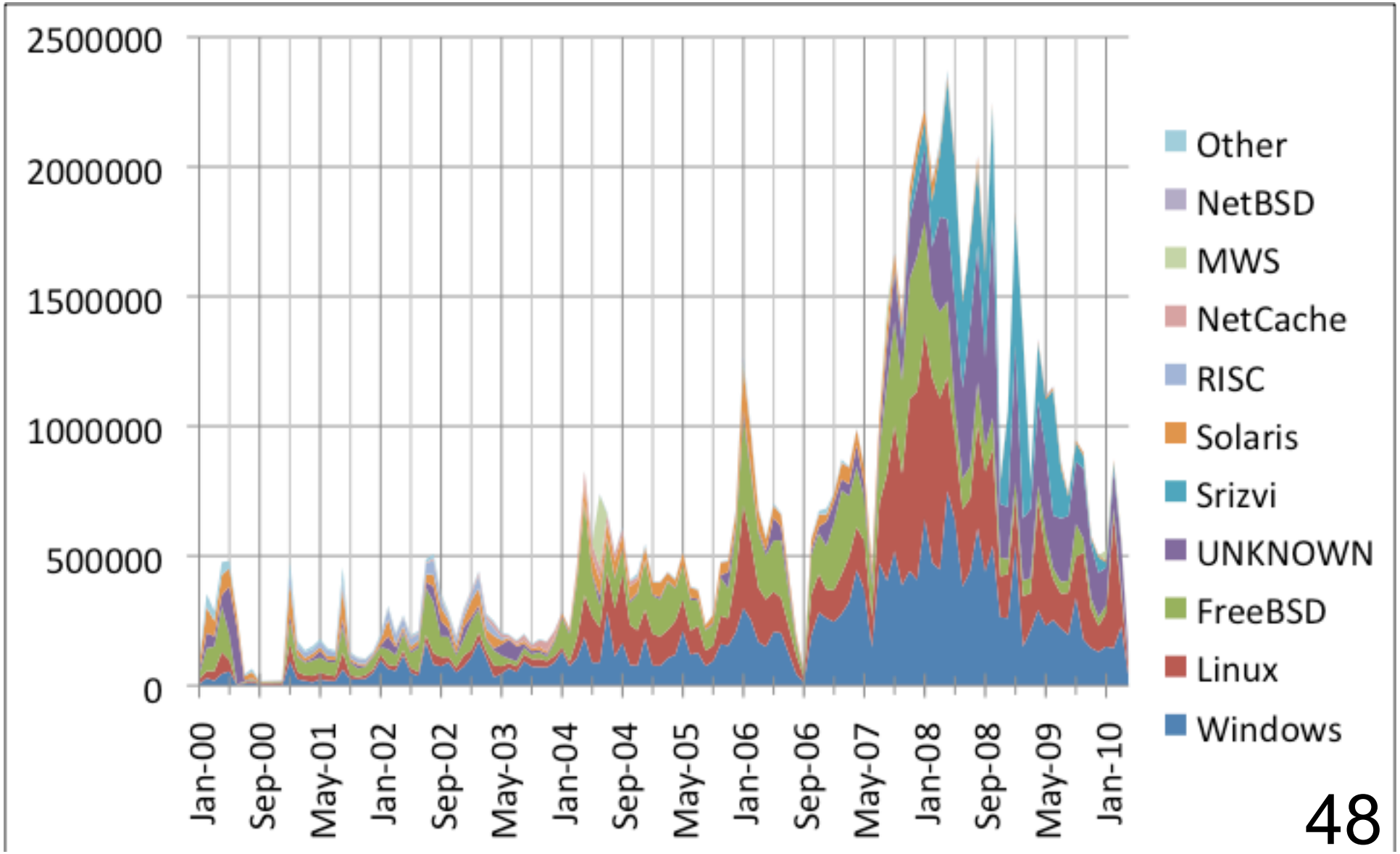
研究(3)
スパム送信ホストの
TCP/IPスタックの分析と
スパム検出への応用

Holly Esquivel, Tatsuya Mori and Aditya Akella
Router-Level Spam Filtering Using TCP Fingerprints: Architecture and Measurement-Based Evaluation, CEAS 2009

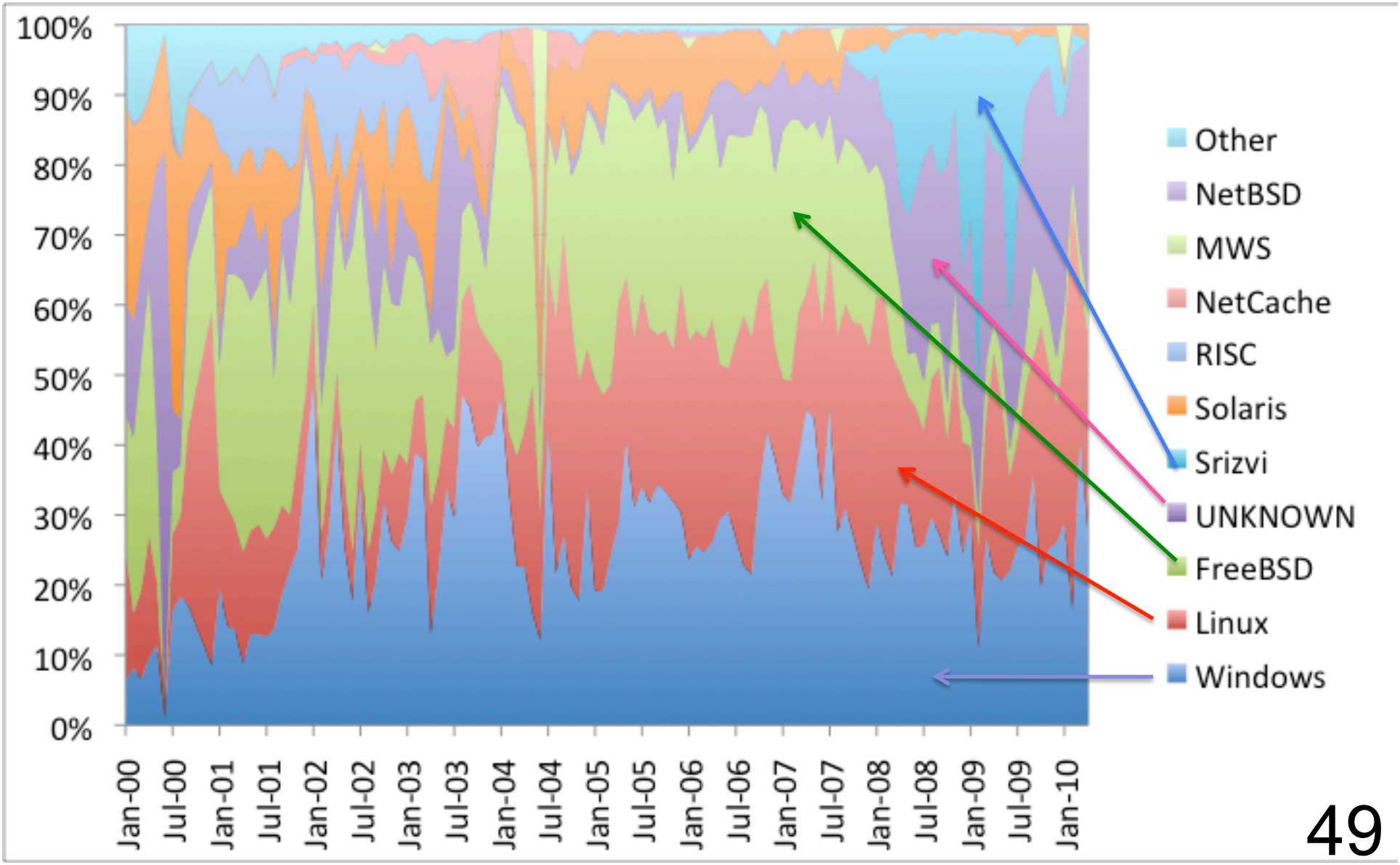
長期定点観測で見る
電子メール送信システムの変遷

- 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

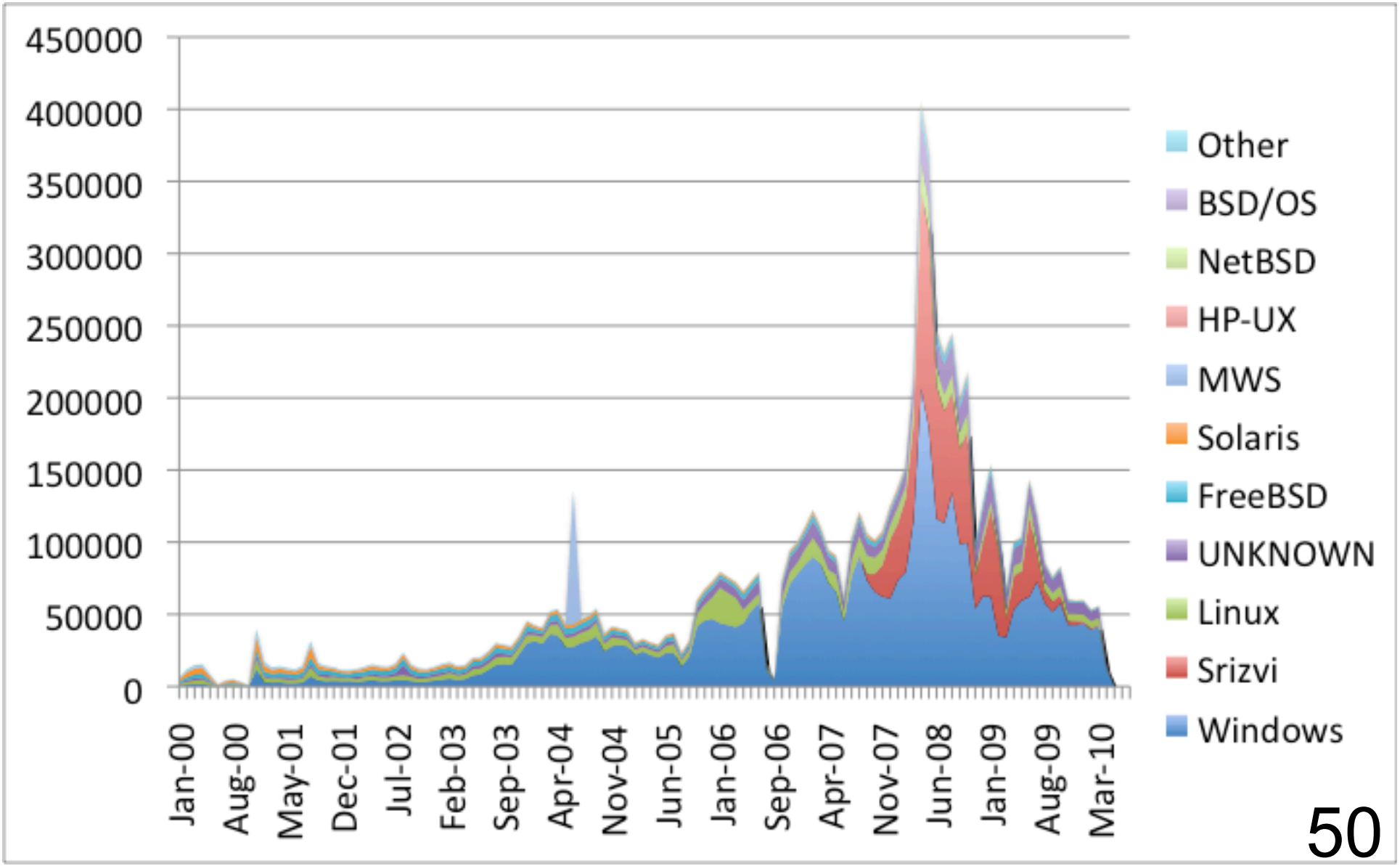
OS別SMTPコネクション数



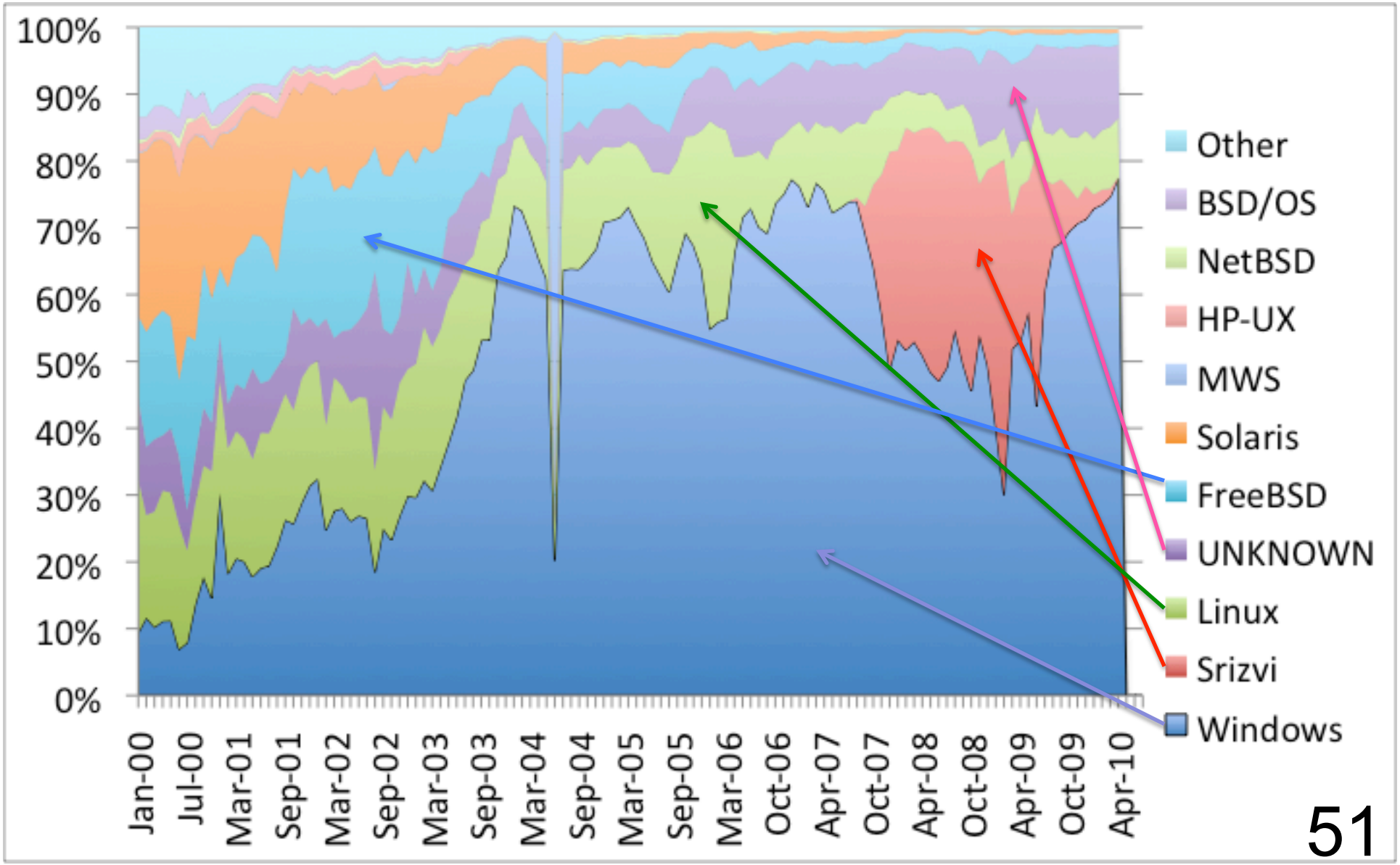
OS別SMTPコネクション数（割合）



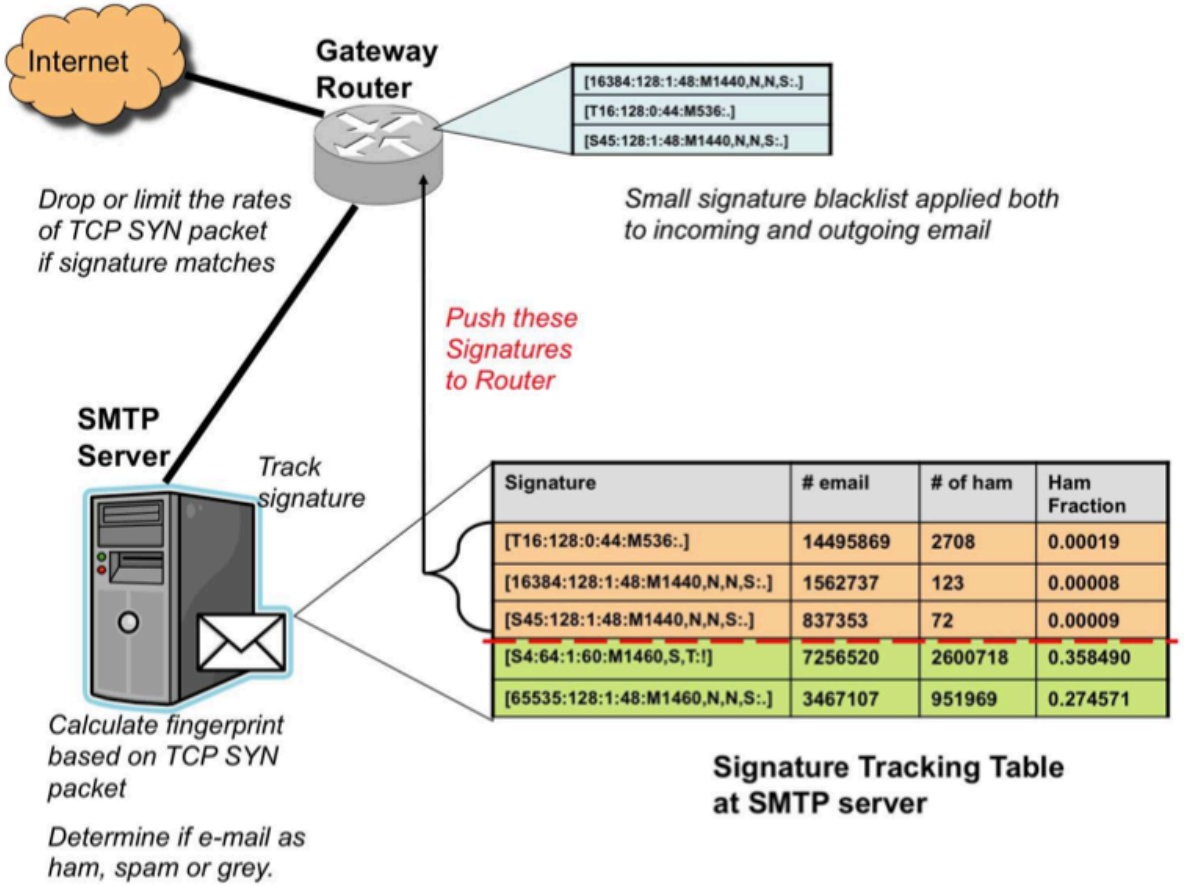
OS別送信元IPアドレス数



OS別送信元IPアドレス数（割合）



TCP fingerprint を利用したスパムフィルタ



精度評価結果

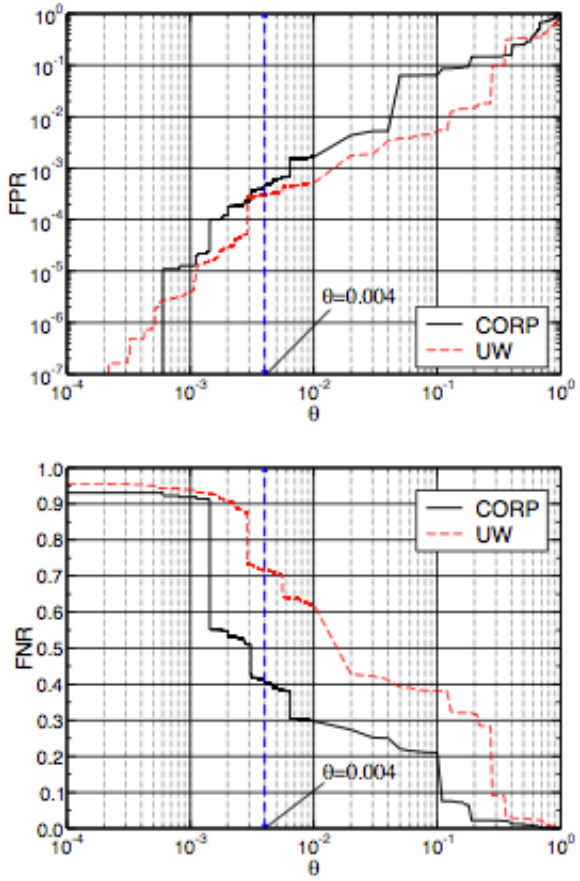


Figure 4: Performance of extracted signatures under the various thresholds (the first stage): False positive ratio (top) and False negative ratio (bottom).

閾値をうまく選ぶことで、TCP fingerprint単一でも高い精度が達成できる

研究(4)
スパム以外の悪意のある通信に関してTCP Fingeprintを分析

木佐森幸太, 下田晃弘, 森達哉, 後藤滋樹,
TCPフィンガープリントによる悪意のある通信の分析
マルウェア研究人材育成ワークショップ 2009

カーネルマルウェアの分析

- ハニーポットでも特徴的な TCP fingerprint を発見。攻撃通信のトリガーとして分析に利用。

表 3.1: MWS シグネチャの通信内容

シグネチャ	ftp	http	irc	shell	smb	sql
MWS 60352_6	232	0	0	558	0	0
MWS 53760_4	50	1	0	307	0	0
MWS 60352_3	38	0	0	66	0	0
MWS 65535_7	12	0	0	21	0	0
MWS 60352_2	0	0	0	18	0	0
MWS 60352_1	0	0	0	6	0	0
すべての通信	694	563	202	1,660	9,234	723

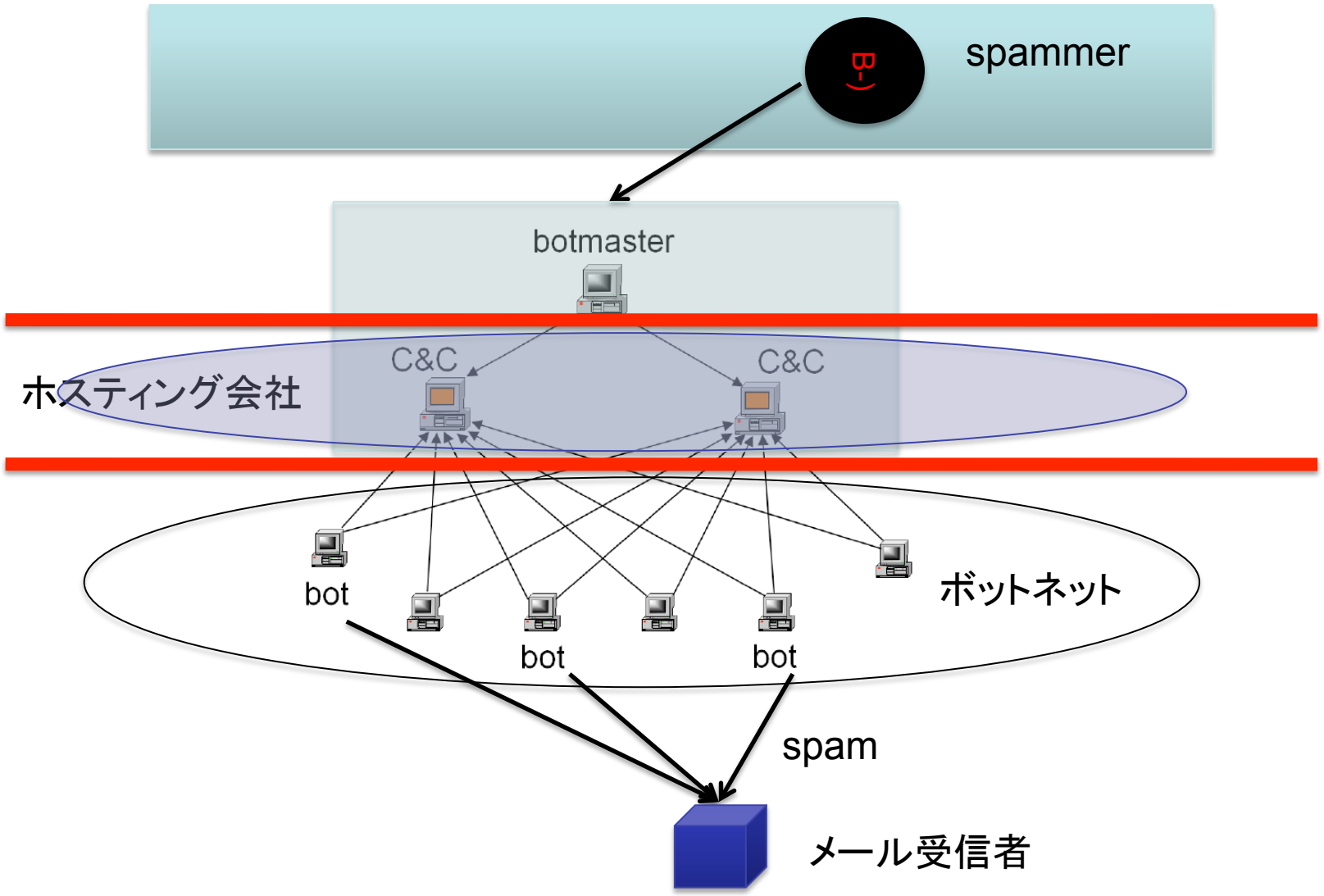
スパムボットの検出はできても
根本的に受信する
SMTPセッション数は減らない

→スパムボットを根本的に
シャットダウンする方法の
有効性は？

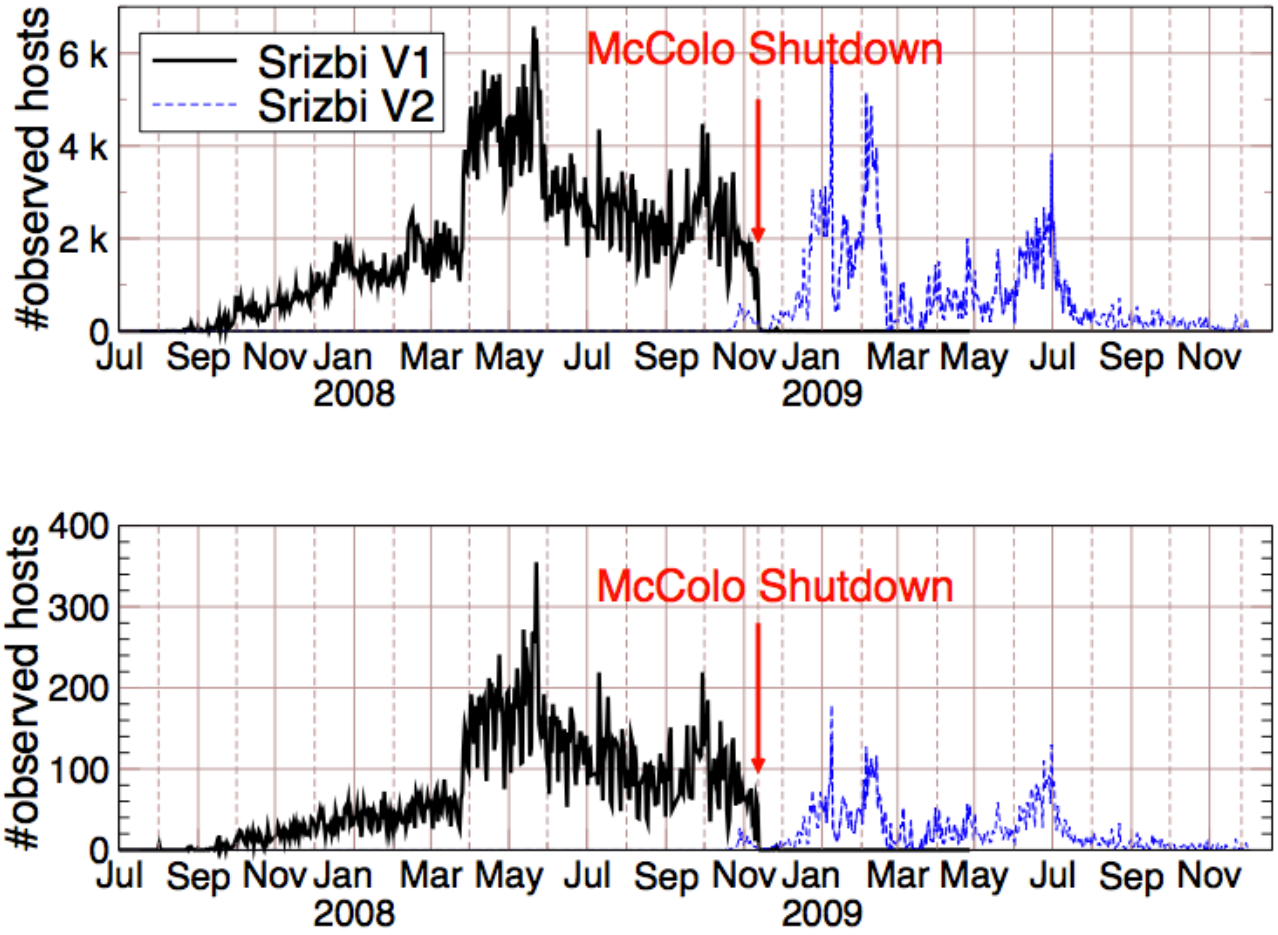
研究(5)
大規模スパムボット(Srizbi)の分析

T. Mori, H. Esquivel, A. Akella, A. Shimoda, and S. Goto
``**Understanding Large-Scale Spamming Botnets From Internet Edge Sites**,"
Proc. Seventh Conference on Email and Anti-spam (CEAS 2010),

C&Cサーバを
インターネットから遮断

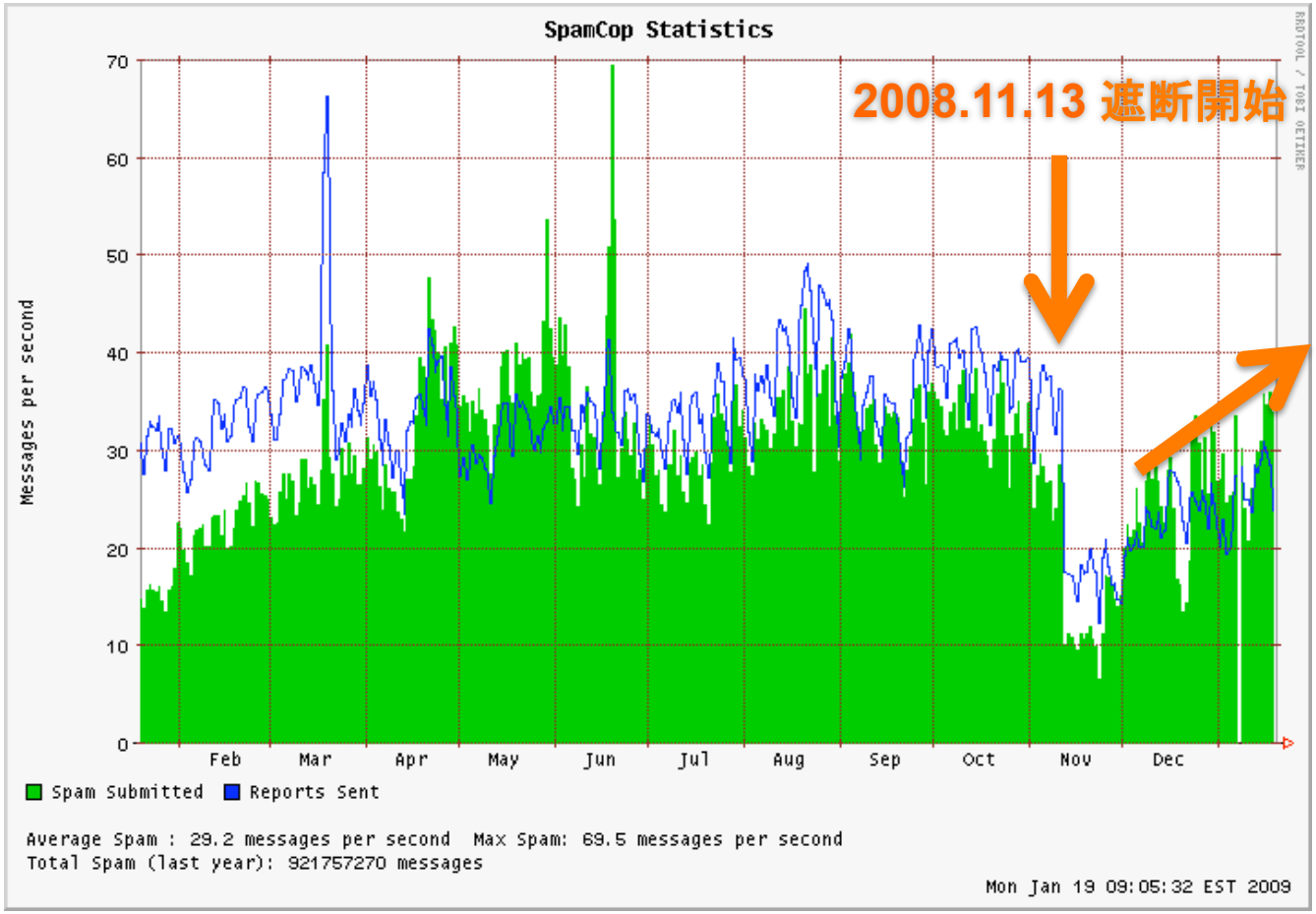


Srizbi ボットネットの勃興と衰退

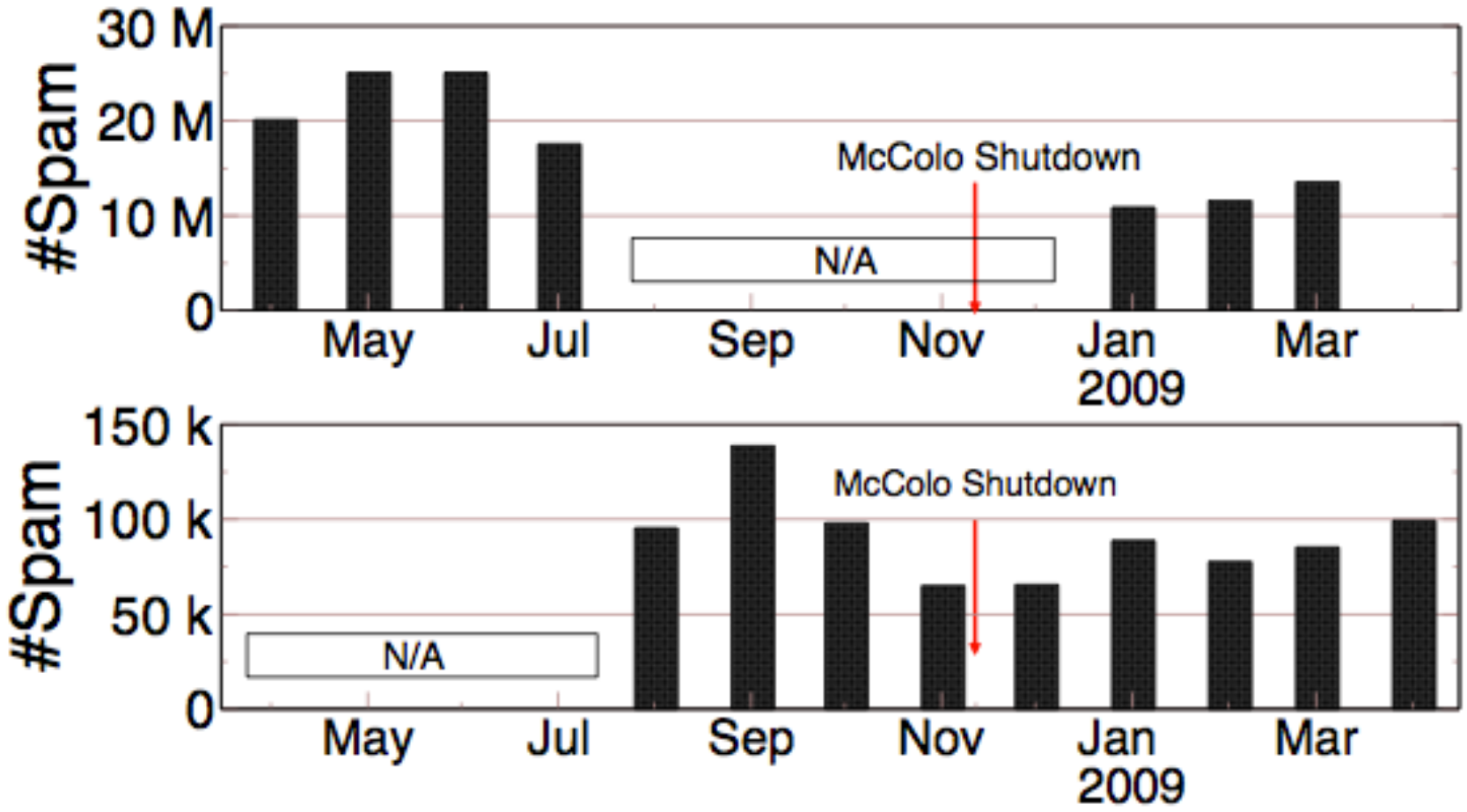


Srizbi C&Cサーバホスティング会社の遮断とその後の経過

- 2週間ほどは効果があったがその後徐々に復活した

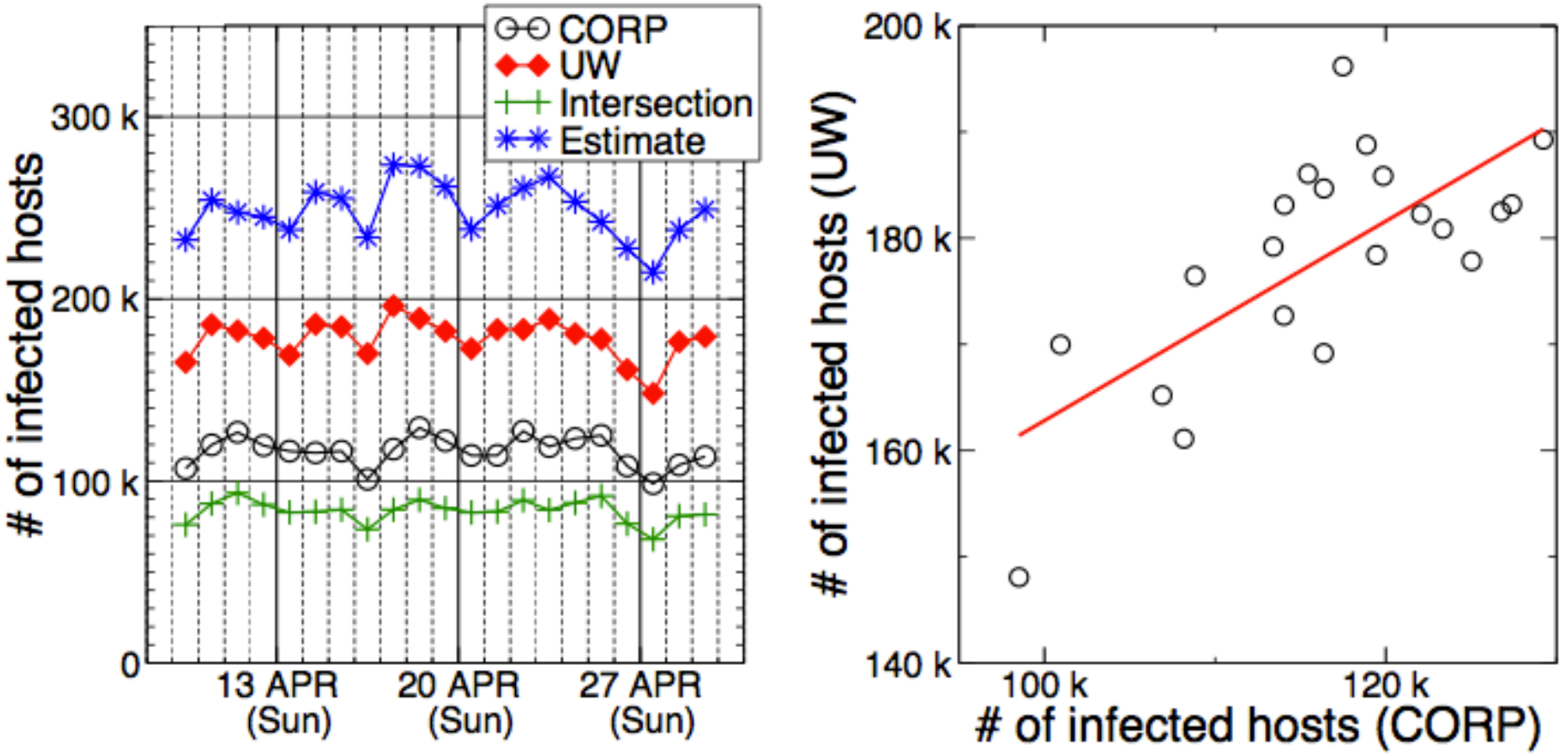


国内企業・学術ネットワーク (GEMnet2)で観測された遮断の効果



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

Srizbiの母集団推定分析



Mark and Recapture による母集団推定

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.

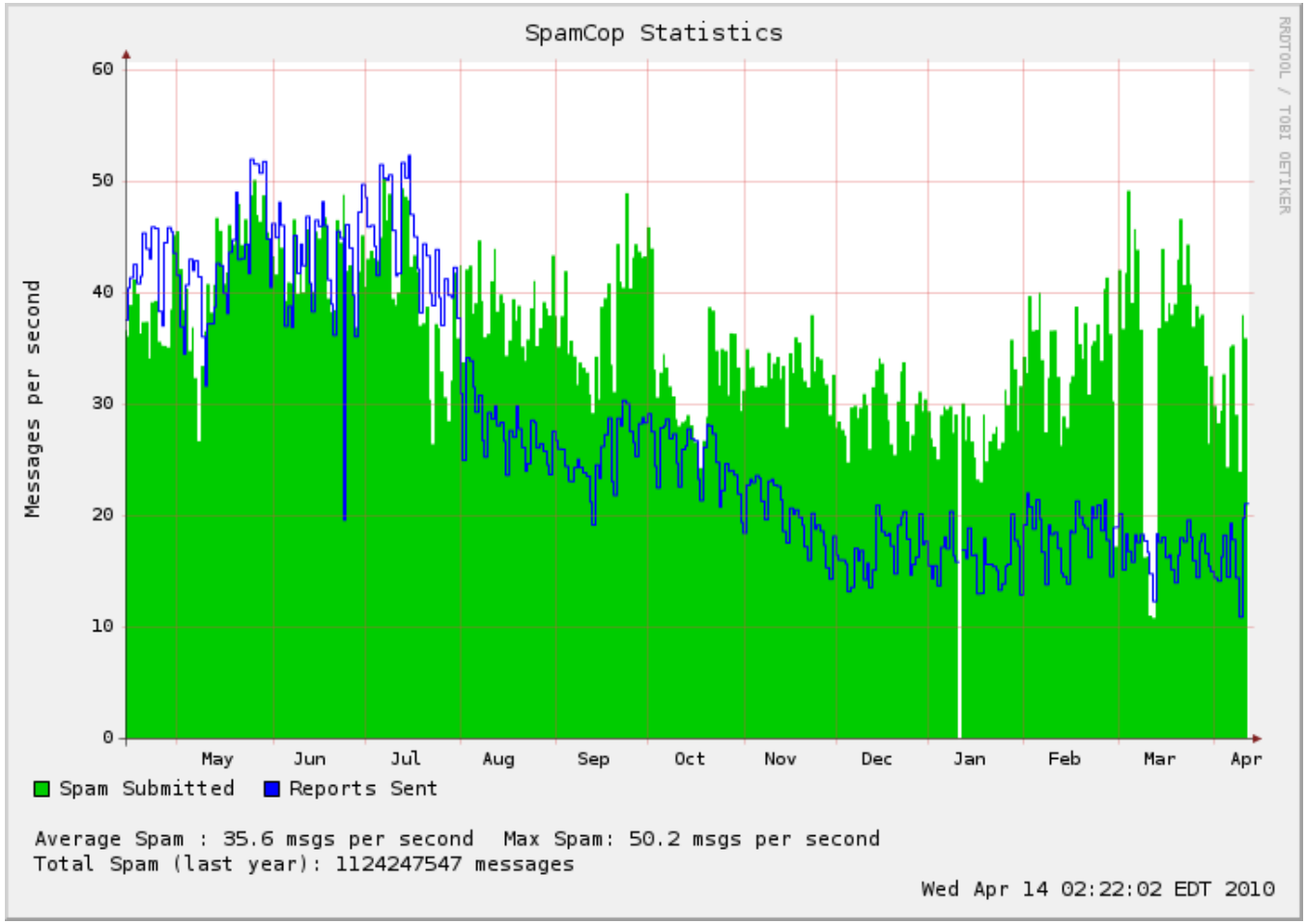
The successes have not inconvenienced hi-tech criminals who found other routes to send spam, say experts.

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

ボットネット自体の壊滅は難しい。
ボットに感染する水際で防げば
よいのでは？

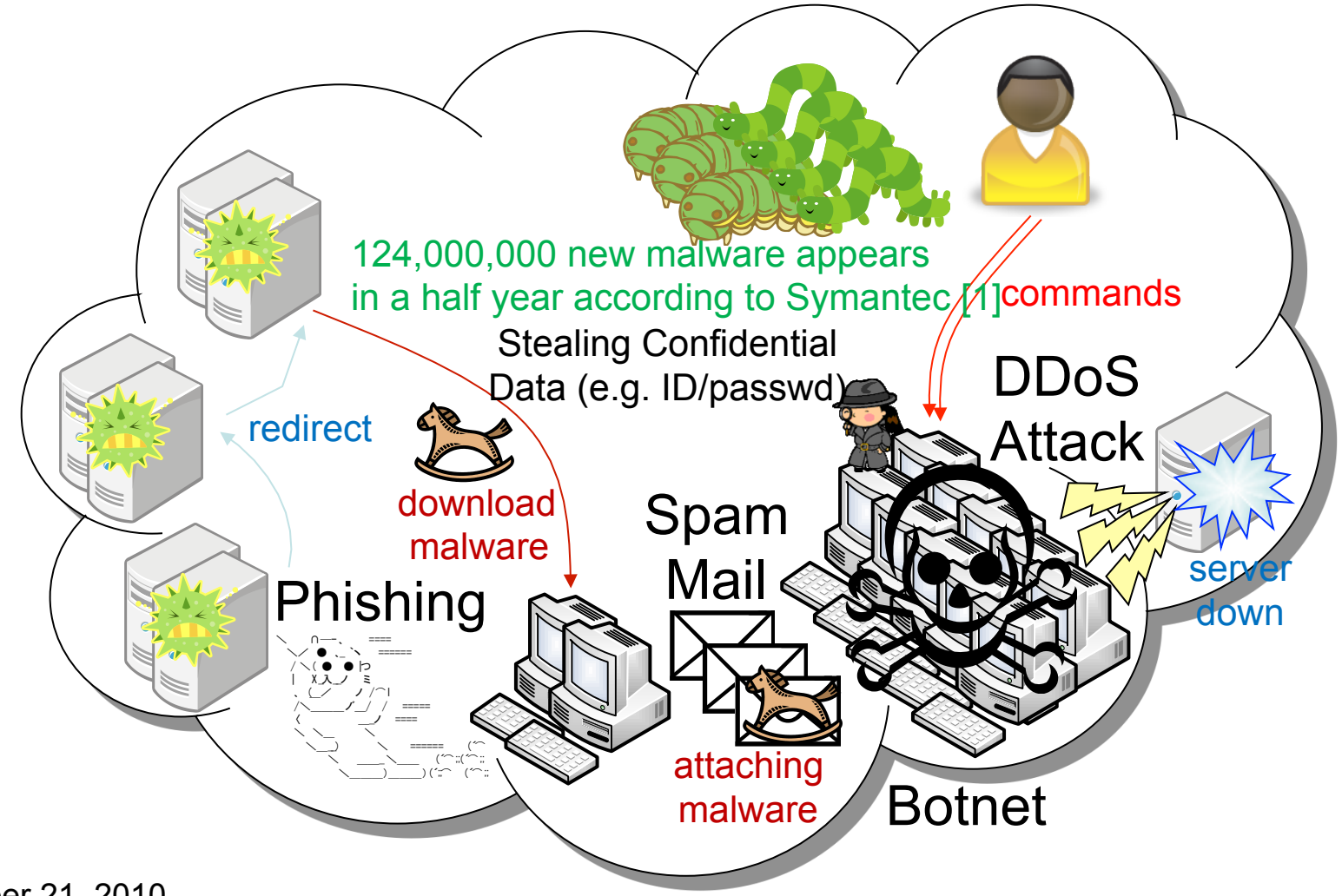
→

マルウエアそのものを送受信
する通信を検出し、フィルタしたい

研究(7)
軽量で高精度なマルウェア検出方法

戸部 和洋†, 森 達哉††, 千葉 大紀††,下田 晃弘†, 後藤 滋樹,
実行ファイルに含まれる文字列の学習に基づくマルウェア検出方法
マルウェア研究人材育成ワークショップ 2010

研究背景


124,000,000 new malware appears
in a half year according to Symantec [1]
commands
Stealing Confidential
Data (e.g. ID/passwd)
redirect
download
malware
Phishing
Spam
Mail
attaching
malware
DDoS
Attack
server
down
Botnet

研究背景 (cont.)

半年で1億2400万の新種マルウェアが出現 [1]

- 68万検体/日、2万8千検体/時、470検体/分
- 「ウイルス定義ファイル」の生成が間に合わない
  - 平均的なアナリスト：1時間/検体、優秀：5分/検体 [2]

攻撃者はパッカー*によって手軽に、
大量の亜種を作り出すことができる。

*パッカー：実行ファイルを実行可能形式のまま圧縮・暗号化（パッキング）するSW

従来のパターンマッチング方式は限界

- ふるまい検知（動的解析）では検知できない
  マルウェアが存在する… Anti-Anti-Virus機能

研究目標

解析に専門知識・技術を必要としない

e.g. ファイル構造、Win32 API、x86アーキテクチャ

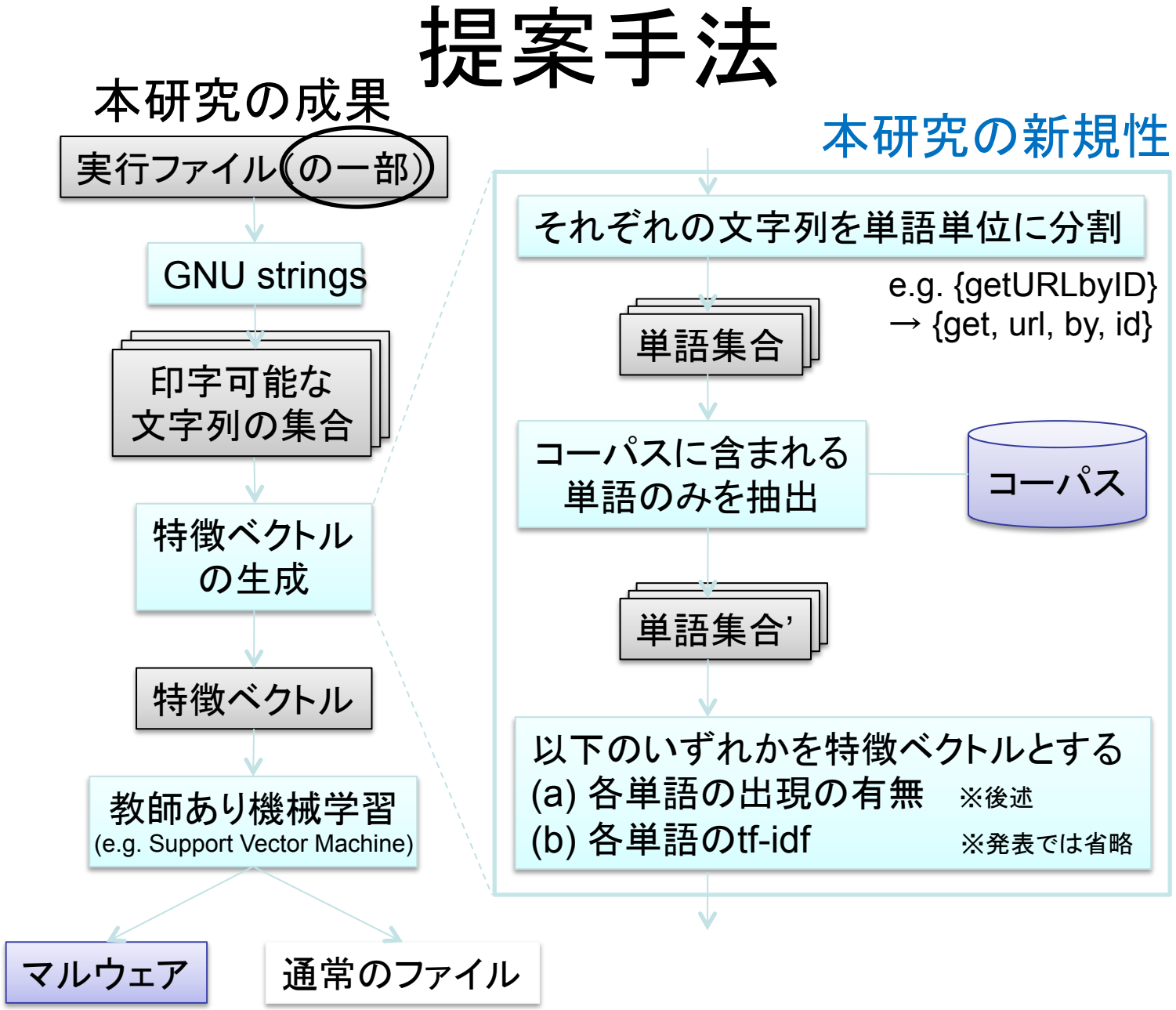
cf. ウイルス対策ソフトベンダの「職人」による解析

新種・亜種のマルウェアも高精度で検出可能

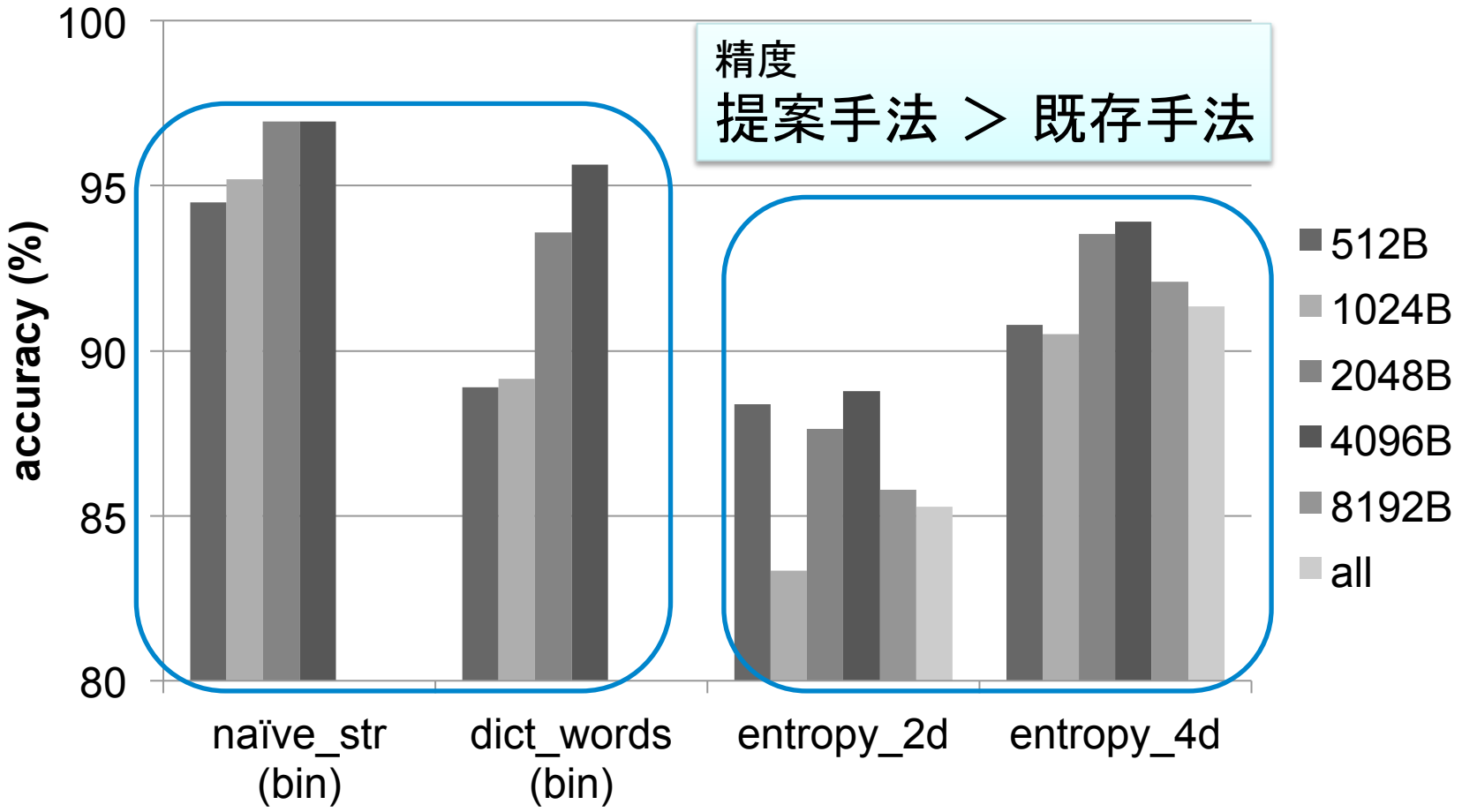
cf. 従来のパターンマッチング方式

高速・軽量でネットワークレイヤで適応可能

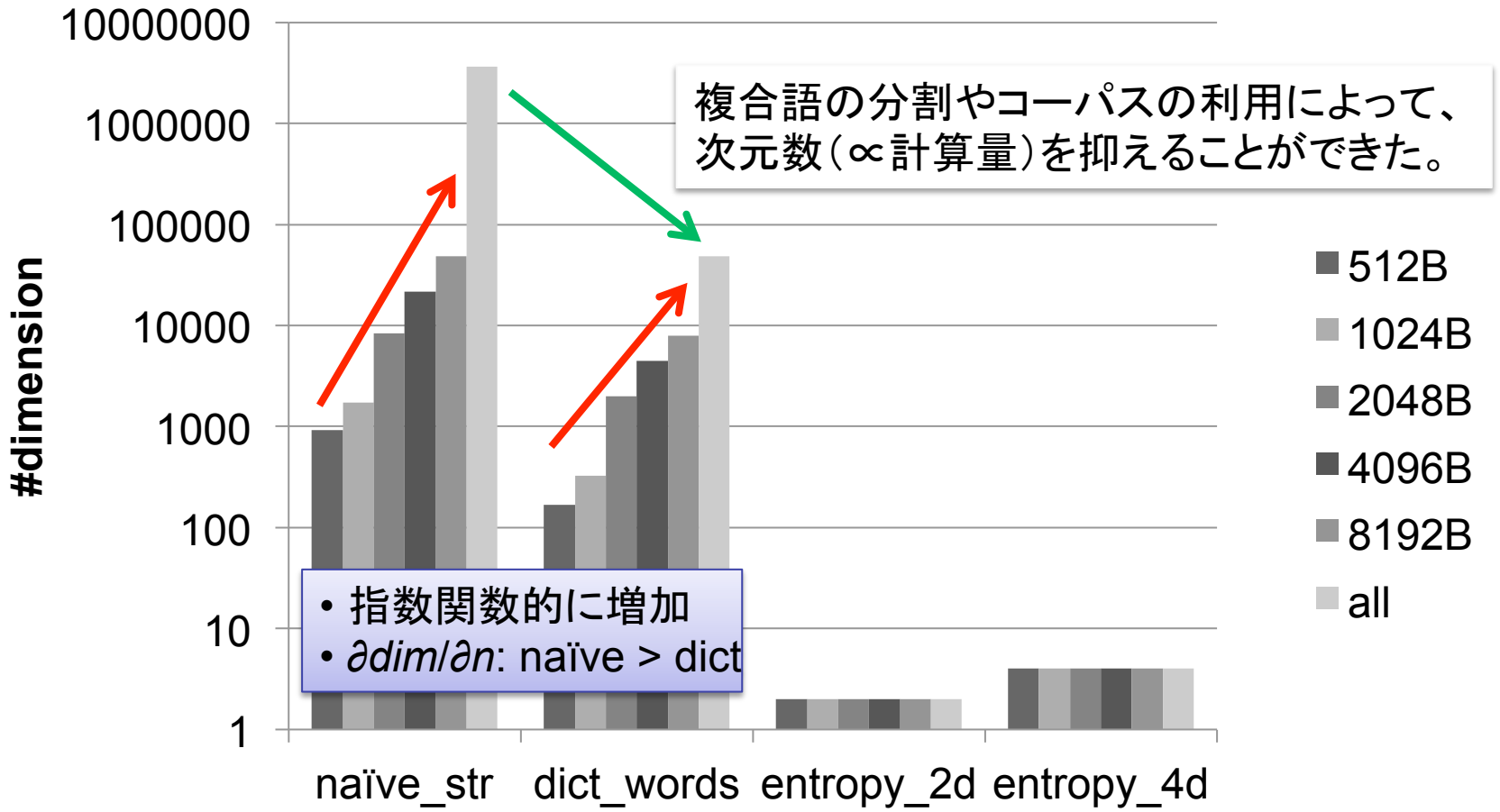
提案手法


本研究の成果
実行ファイル（の一部）
GNU strings
印字可能な
文字列の集合
特徴ベクトル
の生成
特徴ベクトル
教師あり機械学習
(e.g. Support Vector Machine)
マルウェア
通常のファイル
本研究の新規性
それぞれの文字列を単語単位に分割
e.g. {getURLbyID}
→ {get, url, by, id}
単語集合
コーパスに含まれる
単語のみを抽出
コーパス
単語集合’
以下のいずれかを特徴ベクトルとする
(a) 各単語の出現の有無 ※後述
(b) 各単語のtf-idf ※発表では省略

性能評価::精度比較
提案手法による精度の向上



性能評価::コスト比較
提案手法による次元数の削減



裏舞台

データの収集

- ネットワークセキュリティ：何はなくともデータがないと始まらない
  - 暗号や方式の検討とは異なる点
  - 手口はどんどん変わる
  - 敵を知る (Know your Enemy)
    - Honeypot, spamtrap, darknet

どういうデータを収集するか

- サーバログ
  - メール, web, proxy, MySQL, …
- ネットワーク通信ログ
  - Tcpdump, NetFlow, sflow, MIB, …
- 囮サーバ・ネットワーク
  - Darknet, Honeypot, HoneyNet, Spamtrap,…

データを収集する上での二大障壁

- 技術的問題
- 政治的問題

技術的問題

- パケットをキャプチャする場合だけでも・・・
  - ネットワークを止められないので、
    - タップを挟めない
    - 冗長系があったとしてもルート切り替えするのは大変
  - テストしたことないので
    - ポートミラーリングはダメ
  - ミラーリングしてあげられるけど
    - 10G の I/F で受けられる？
- 枚挙にいとまがありません。

政治的問題

- プライバシー問題
  - これが一番大きい
  - Network security研究のために不可欠であることをauthorized にする（裏の）努力が必要
- 予算問題
  - 計測にはお金がかかることもあるので計画的に
  - 10G capture装置など
- 多組織問題
  - 研究者が複数組織にまたがるようなケース
  - NDAを結ぶ場合もある（ボスに任せれば良い人はラッキー）

データ収集の例

- Darknet 運用
  - 空きIP アドレスに届いたパケットを収集
    - Scan や backscatter の大域的な傾向が分析できる
  - ルーティングの変更が必要
  - パケットが返らないようなフィルターの設定
  - パケットキャプチャ・分析サーバを設置
  - 無効なパケットなので、プライバシーの問題を考えずに済むメリットあり

データ収集の例

- メールサーバログ分析
  - 生ログは使わない（使えない）
  - 個人情報(メールアドレスなど）を完全に匿名化する parser を渡して、管理者に動かしてもらう
    - ログフォーマットの仕様がない場合、目で見てリバースエンジニアリングを繰り返すしかない
  - Parser によって Sanitize された結果のみをもらう

うまく進めるコツ

- キーパーソンを把握し、動かすこと
  - 長期的に良好な関係を築く
  - Give and Take の精神で。自らも泥仕事をやる。
  - データ収集のインセンティブを示す
    - 予算・稼働を割いてまで協力するメリットは何かを丁寧に示す
- 妥協点を探る
  - 完全なデータは入手できない事は多い。そこであきらめず、不完全なデータをどう料理できるかを考える
- 悪い前例を絶対に作らないこと
  - 二度と同じような要望が通らなくなる
  - 厳重なデータ管理

その他のTips

- データ収集の開始は早めに
  - 思い立ったが吉日
  - データはある程度集まらないと価値がない
  - 修論の1週間前 → アウト!
  - Web API を使ったクラウドサービス系の計測などは個人でもお手軽にできるので、1年くらいのデータをとってみる
- 複数のデータを入手する
  - それぞれのデータを関係つける
- フリーのデータ・サービスはフル活用する
  - アカデミアならでは入手可能なデータも多い
  - CCC (MWS dataset), Planetlab, CAIDA, WIDE/Mawi, etc…
  - 自組織でやる場合、データ管理のポリシーを明文化してしまう（最初は大変だが、二度目以降が楽になる）

データの料理

- データの料理（分析・処理）の重要性
  - 得られた素材を生かすも殺すも料理次第。良い素材があっても料理が下手なら×。
  - そこそこの素材でも料理が上手いと良い成果が。
- どういう統計・処理をするかが大事。ツールは二の次
  - 何を示したいのか、まずストーリーを作る
  - それが決まった上でツールを選ぶ

様々なツールと実装の例

- 基本的な統計
  - 平均、分散、分布、ソート等々
  - 自作 script, R, GSL, etc…山のようにある
- 統計的機械学習・推定
  - NBC, K-NN, SVM, K-means, EM, …
  - R, Weka, SVM_light, libsvm, NR, 自作…

統計的手法について

- 専門外の人であってもツールを適用してみるとなんとなくそれらしい結果は出ます
- が、手法の本質的な理解がないと誤った結果を導くことが非常に多いです
  - 違う目的で使ってしまう
  - パラメタチューニングをしない
  - 十分なサンプル数がないのにツールを適用してしまう
  - 結果の平均・標準偏差をとらない
  - 解釈がおかしい
  - etc. etc.…
- 手法の勉強・本質的理解に沢山の時間を投資しましょう
  - ○○本読み会
  - 数学・統計に強い仲間を作る

Tips

- いずれの方法も直感的に正しい結果を得られているのかを徹底的に確認
- そうでない場合はなぜそうなのかをとことん突き詰める
  - 実際にはこの作業が一番時間がかかる
  - 新たな発見があることもあるが、多くの場合はバグやデータに固有な性質など
- 複数の実装が使える場合、必ずダブルチェックする
  - データ分析の研究でバグは致命的

まとめ

- ネットワークセキュリティに関する研究の紹介
  - 表舞台：スパムとマルウェアを例として
  - 裏舞台：データ収集・データ料理について

参考情報

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）