ワーム ホイホイ

～未使用アドレス空間を利用したハニーポットの運用～

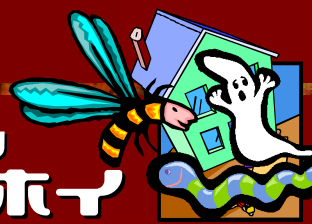
慶應義塾大学 政策・メディア研究科
白畑　真 <true@sfc.wide.ad.jp>

自己紹介

- 白畑　真
- 慶應義塾大学　政策・メディア研究科/村井研究室
  - インターネットセキュリティ(IDS, Honeypot)
- 株式会社クララオンライン
  - 専用サーバ, Web ホスティング
  - ネットワークエンジニア
    - といいつつもサーバなどもやってます

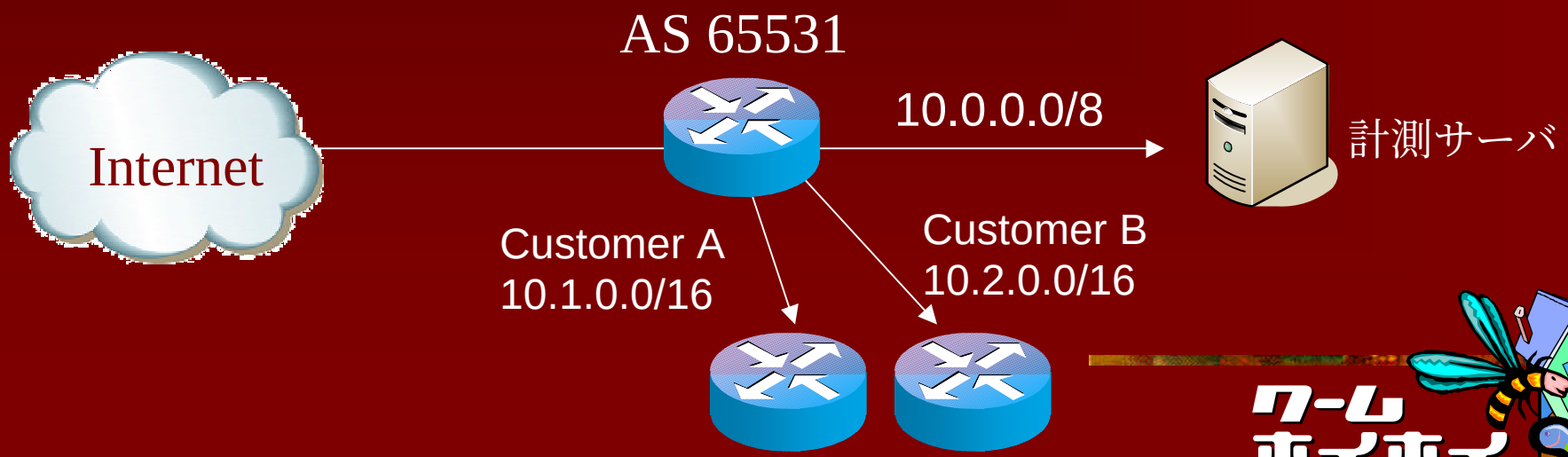
目的

- インターネット上における
  セキュリティリスクの計量
  - ワーム/ウィルス感染ホストの
    規模の推定
  - アタックに悪用されている
    ホストの傾向分析



関連手法: Darknet

- AS65531がインターネットに10.0.0.0/8の経路を広報している場合
  - 顧客用Prefixへはlongest matchで本来のnext hopへ
  - AS内で未使用のアドレス空間宛のパケットが計測サーバに



関連手法(続き)

- The Team Cymru Darknet Project
  - http://www.cymru.com/Darknet/
- Network telescope
  - http://www.caida.org/analysis/security/telescope/
- Internet Motion Sensor
  - http://ims.eecs.umich.edu/index.html
- Backscatter,**ワームの観測**

手法

- 低インタラクション型ハニーポットを
  ネットワークに配置、アクセス傾向を分析
  - 低インタラクション型ハニーポット
  - サーバの動作をエミュレート
  - 実際にホストには侵入させず

dumnet

- 低インタラクション型ハニーポットソフト
  - 村上さん(LAC) 作
- 動作
  - すべての TCP SYN に対して SYN+ACK を返答
  - すべての ICMP ECHO Request に対して ECHO Reply を返答
  - Bind() しないので、広いアドレス空間にも容易に適用可能

↓

  - 全TCPポートが開かれているかのように振る舞う

ハニーポットのメリット

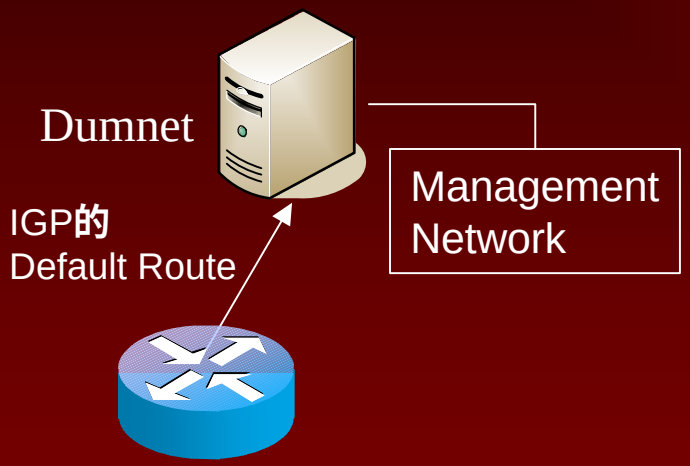
- 未知のワームや攻撃コードを入手できる(はず)
- ポート番号だけではわからない内容を入手可能
  - 例: Windows RPC
    - Windows は 135~139, 443 番ポートをさまざまな目的に利用
    - 同じポートに様々な種類のアタック
  - 未知のウィルス/ワームを捕獲可能
- IP Address Spoofingを判別できる
  - TCP の 3way handshake が成立するか

ハニーポットのデメリット

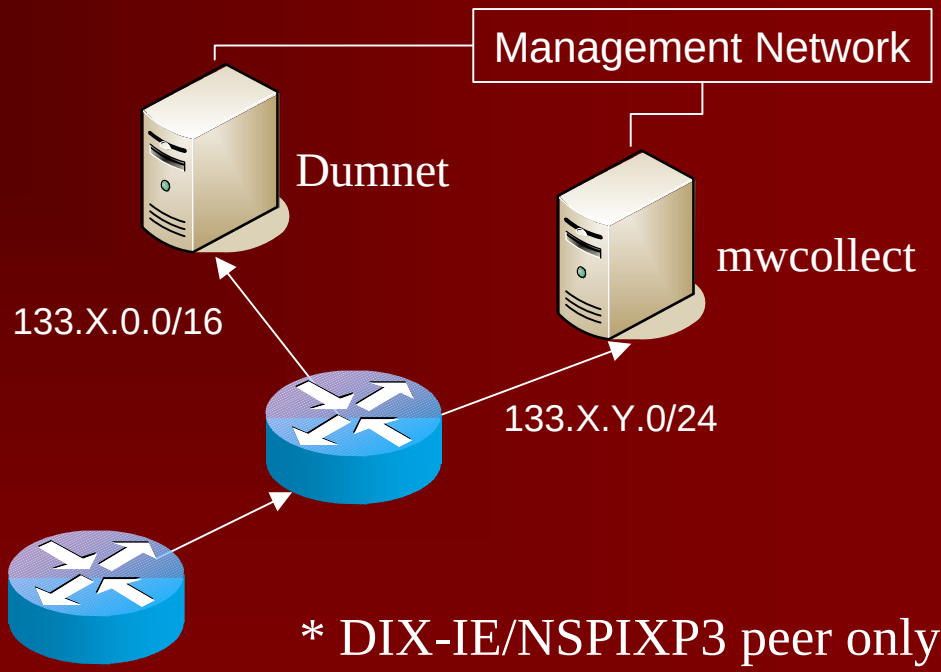
- 存在しないはずのホストから返事が…
  - なんか気持ち悪い
- トラフィックが増える
  - いまのところ数百kbps程度の増加(/16)

現在の構成

- 202.X.X.0/24 * 3



- 133.X.0.0/16



* DIX-IE/NSPIXP3 peer only

観測結果

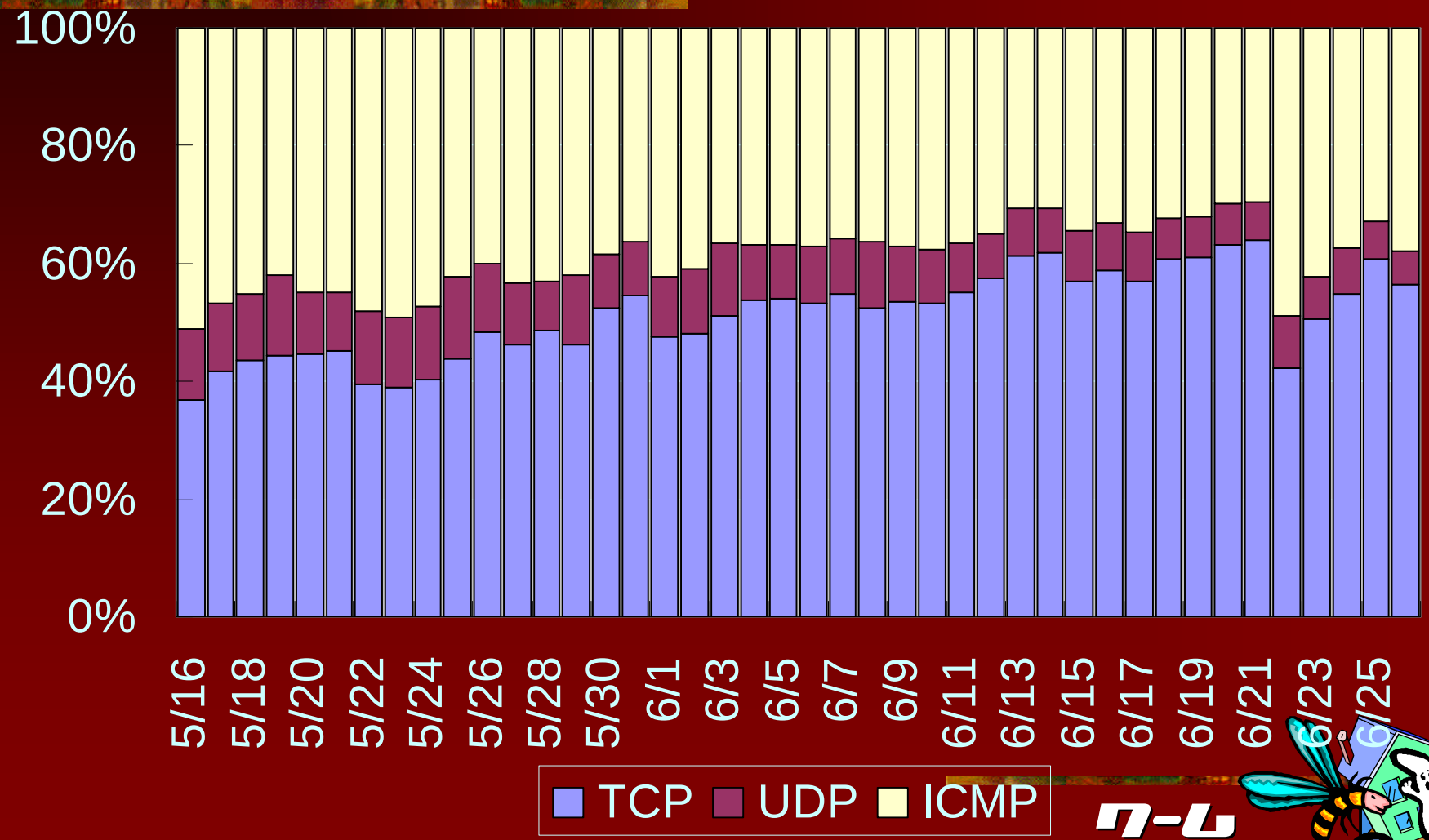
- サイトC
  - **Routable on the Global Internet**
- 5/16 19:16 ~ 6/26 16:46
- 90万0620件
  - 約2.3万件/日
  - 約261件/アドレス/日
  - 約5.5分/件

- サイトW
  - **DIX-IE/NSPIXP-3 Peer only**
  - Mostly from Japan
- 6/13 18:37~ 6/25 17:59
- 1億2396万4200件
  - 約1466.2万件/日
  - 約157件/アドレス/日
  - 約9分/件

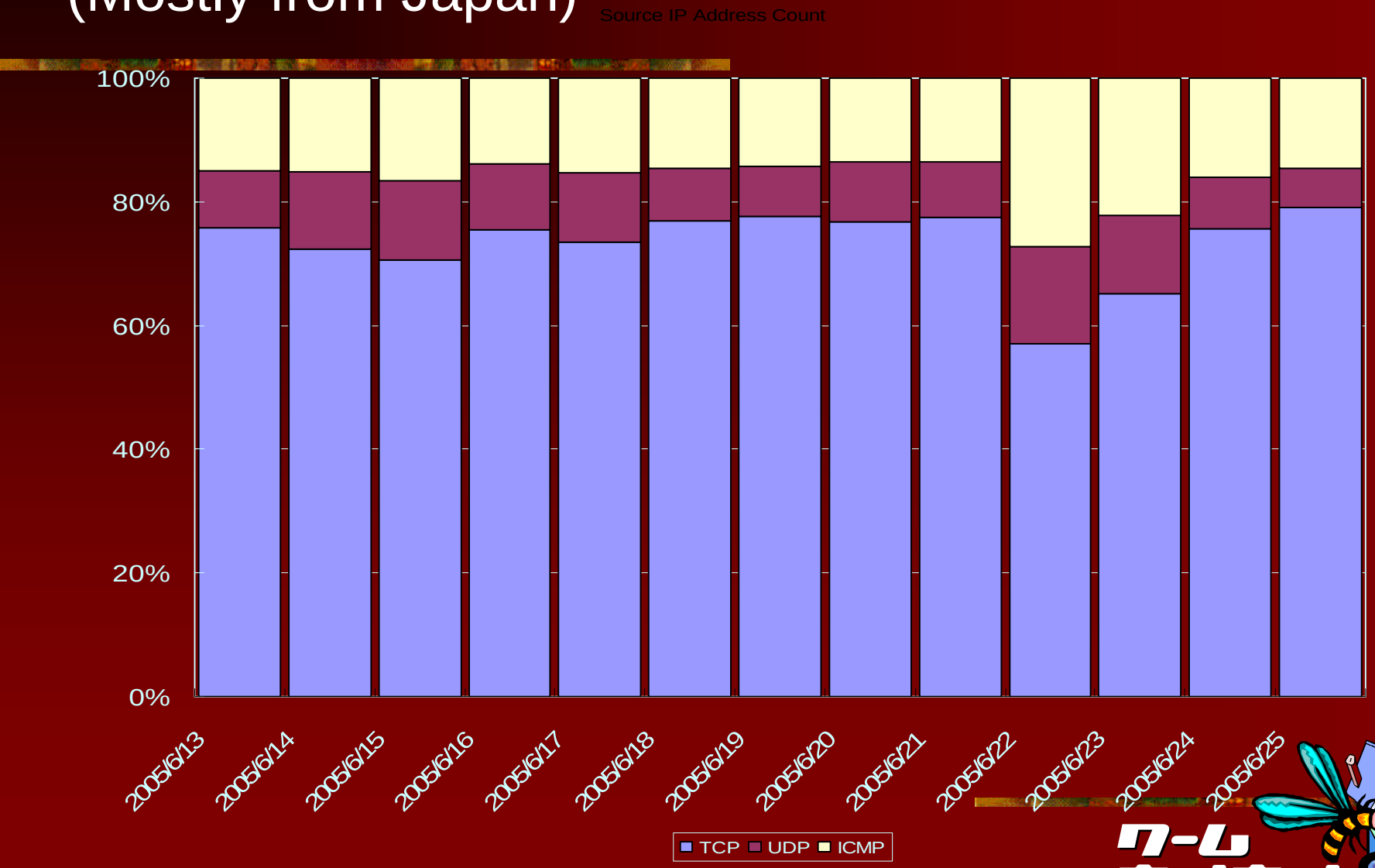
国名データの取得

- MaxMind GeoIP
  - http://www.maxmind.com/
  - RIRのWhoisから取得した(?)データをもとに、IPアドレスと国名のマッピングを提供するAPI
  - アクセス元のIPアドレスの国名を調査

サイトC: Source IP プロトコル分析
(Routable on the global Internet)



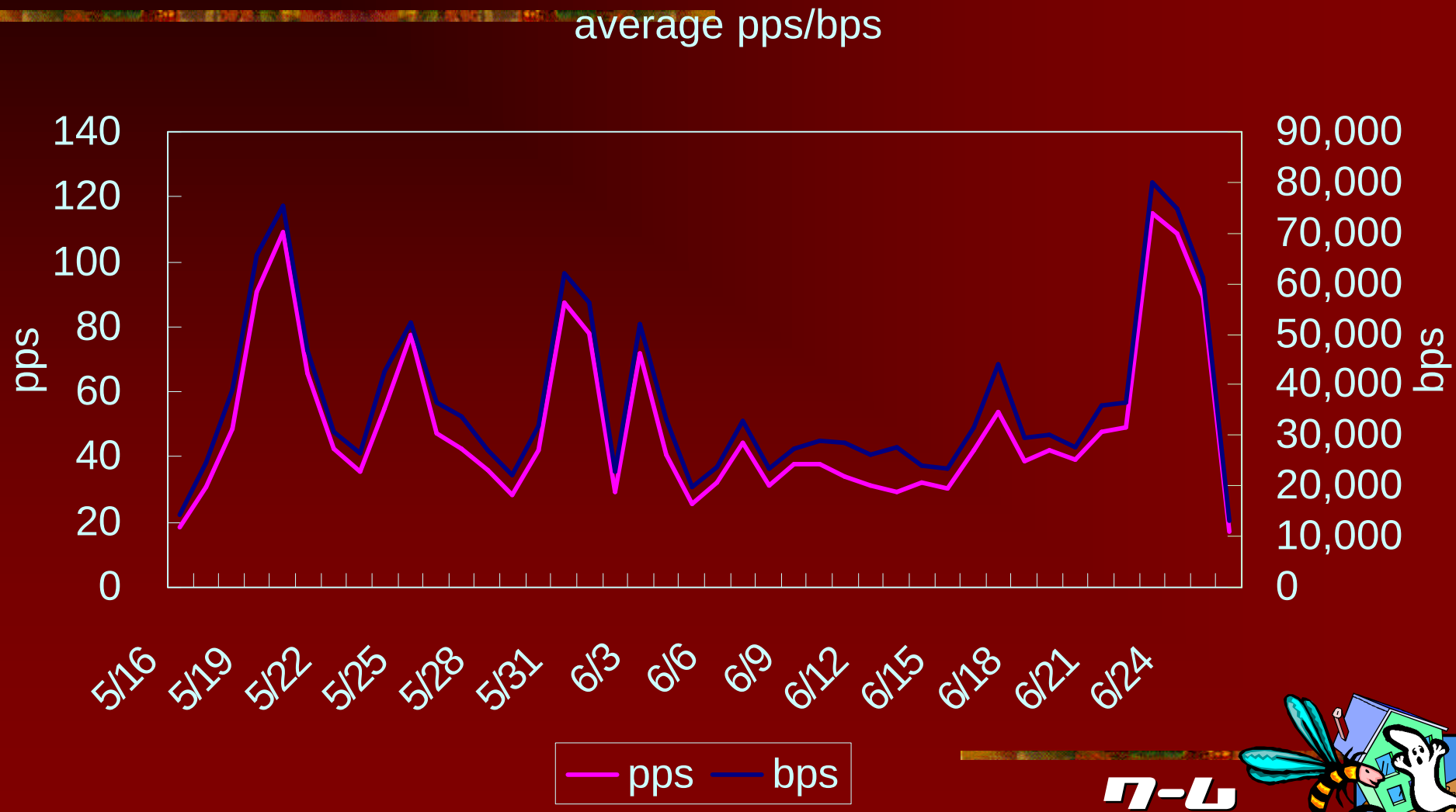
サイトW: Source IP プロトコル別分析
(Mostly from Japan)



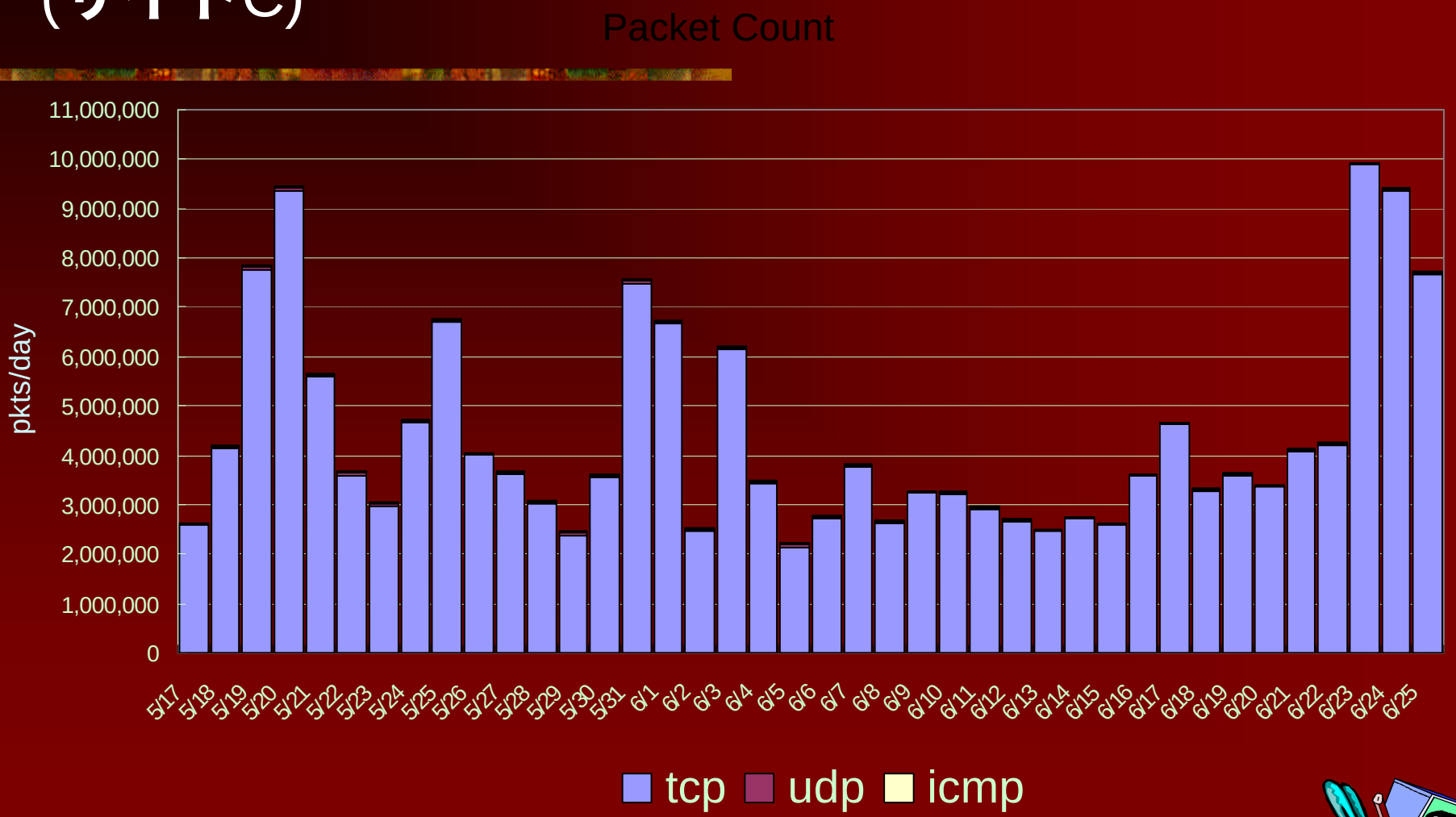
Source IPアドレス

- ワーム/ウィルス感染ノード数の推計(TCP)
  - サイトC: 776,318アドレス
    - うち日本国内: 64,813アドレス
  - サイトW: 203,611アドレス
    - うち日本国内: 112,604アドレス
- 日本国内の感染アドレス数 > 約11万

トラフィックのの推移 (サイトC)



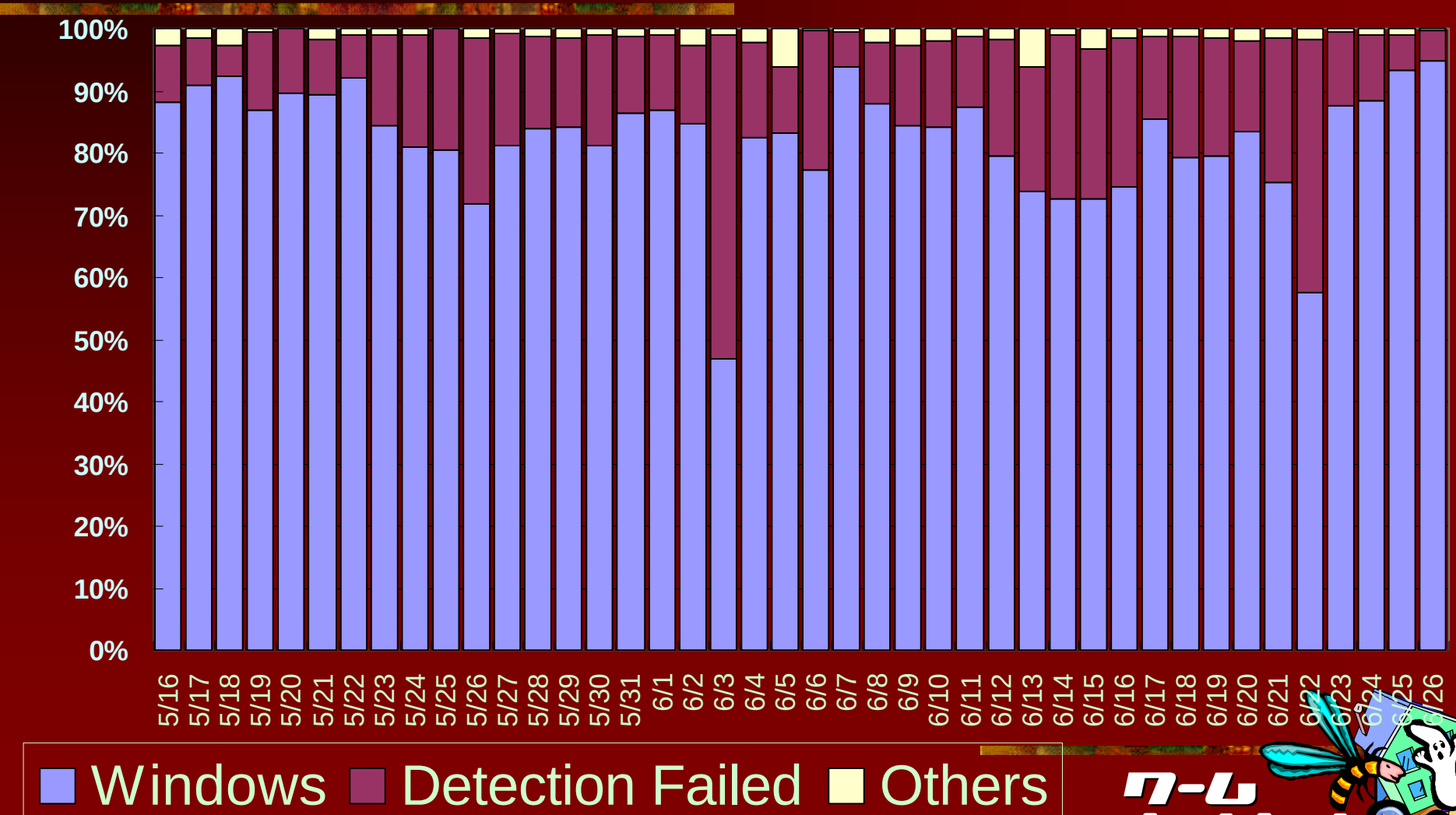
パケット数の推移
(サイトC)



OSの検出

- ハニーポットにアクセスしてきたノードのOSを推測
- p0f
  - Passive OS Fingerprintingツール
  - TCPのWindowサイズ, デフォルトTTL, TCPオプションの並び順などからOSを推測
  - http://lcamtuf.coredump.cx/p0f.shtml

OSの割合の推移
(サイトC)



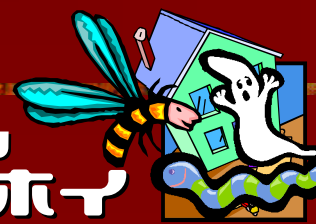
OS by Source IP Address

OS	Count
Windows	22,178,824
Detection Failed	4,252,537
Linux	333,671
Solaris	9,799
NMAP	3,699
FreeBSD	994
OpenBSD	993
CacheFlow	213
Novell	189

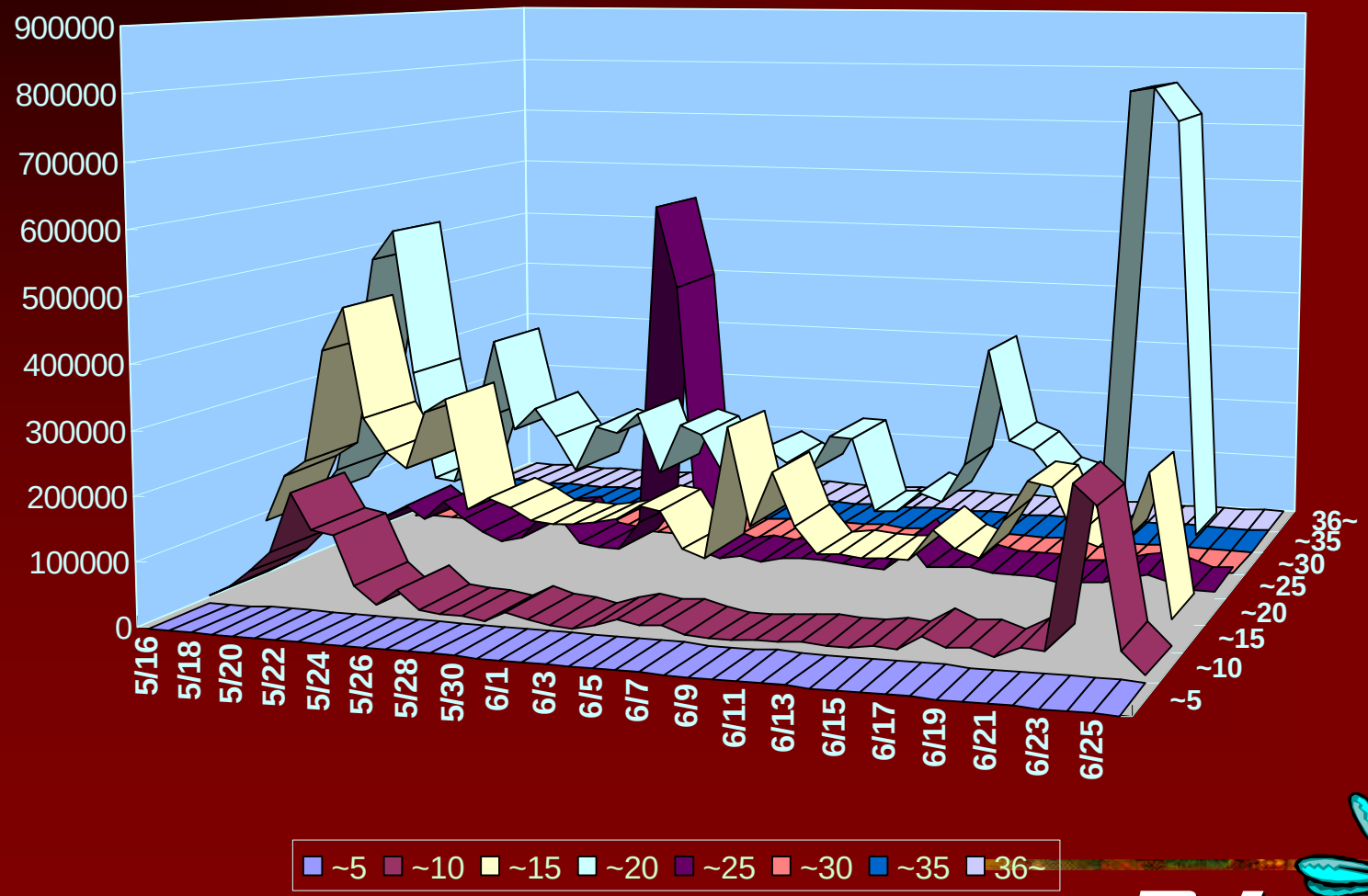
OS	Count
Cisco	67
NetCache	19
SymbianOS	12
Eagle	3
PocketPC	3
Redline	3
BSD/OS	2
HP-UX	1

推定ホップ数

- 多くのOSのDefault TTL:
  - 32, 64, 128, 256 のいずれか
- 到着したパケットのTTLと、よくあるデフォルトTTLを比較
  - 例: TTL 52 の場合、64-52=12なので推定 12 hop



推定ホップ数の推移


900000
800000
700000
600000
500000
400000
300000
200000
100000
0
5/16
5/18
5/20
5/22
5/24
5/26
5/28
5/30
6/1
6/3
6/5
6/7
6/9
6/11
6/13
6/15
6/17
6/19
6/21
6/23
6/25
~5
~10
~15
~20
~25
~30
~35
36~
~5 ~10 ~15 ~20 ~25 ~30 ~35 36~

3127/tcp

- **多くのWormが利用するバックドアポート**
  - Mydoom, DoomJuice, Novarg, Solame…
  - **参考**: http://www.nai.com/japan/security/virM2004.asp?v=W32/Mydoom.b@MM
- **アップデート機能**
  - Mydoom.B
  - **3127/tcpが開いているホストを発見すると、ワーム自体を送り込む**

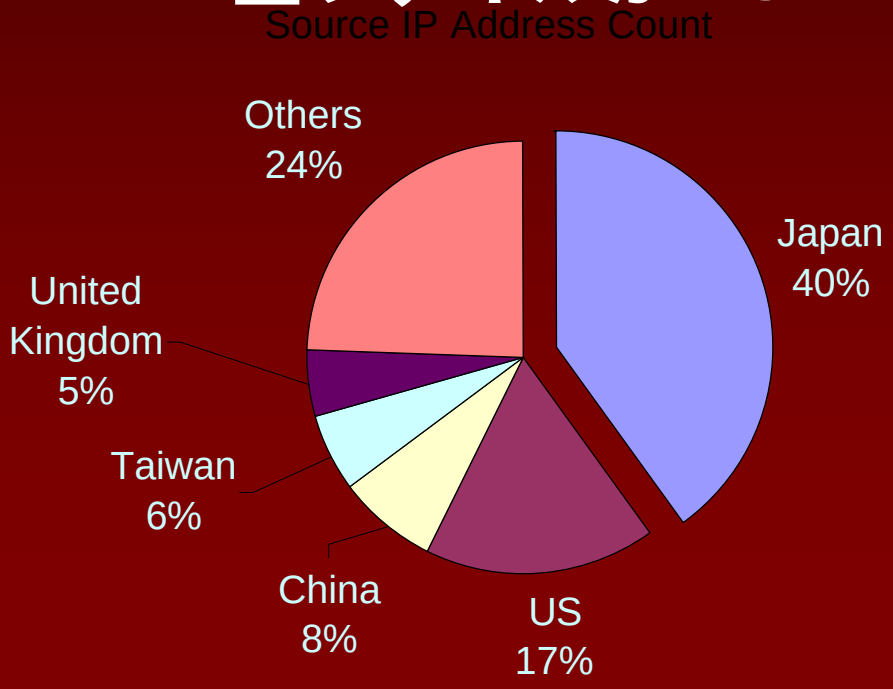
新種発見?

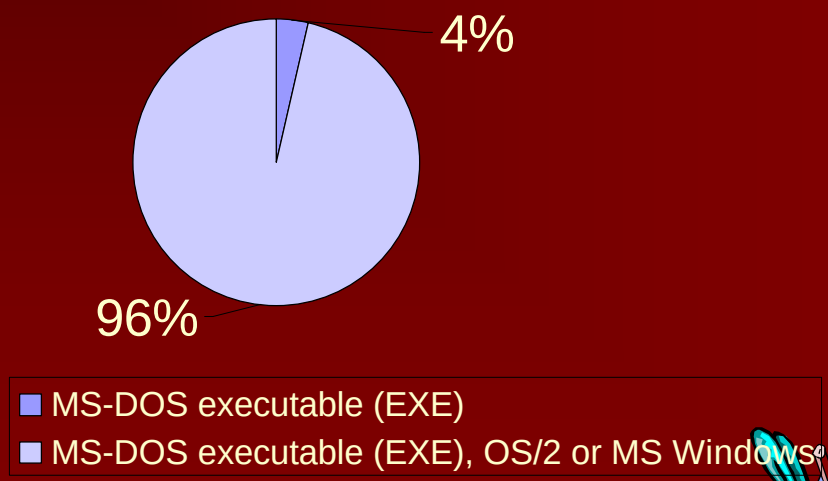
1. TCPストリームを再構成
2. 512byte未満のファイルを除外

3. 先頭5バイト(認証コード)を除去
4. ファイルの内容
   - file(1)コマンドで調査

送られてきたファイル

- サイトCに送られたファイルを分析
  - 分析期間: 5/16 19:16 ~ 6/26 16:46
  - 50カ国、2718アドレスからアクセス
  - 全ファイルがMS-DOS executable

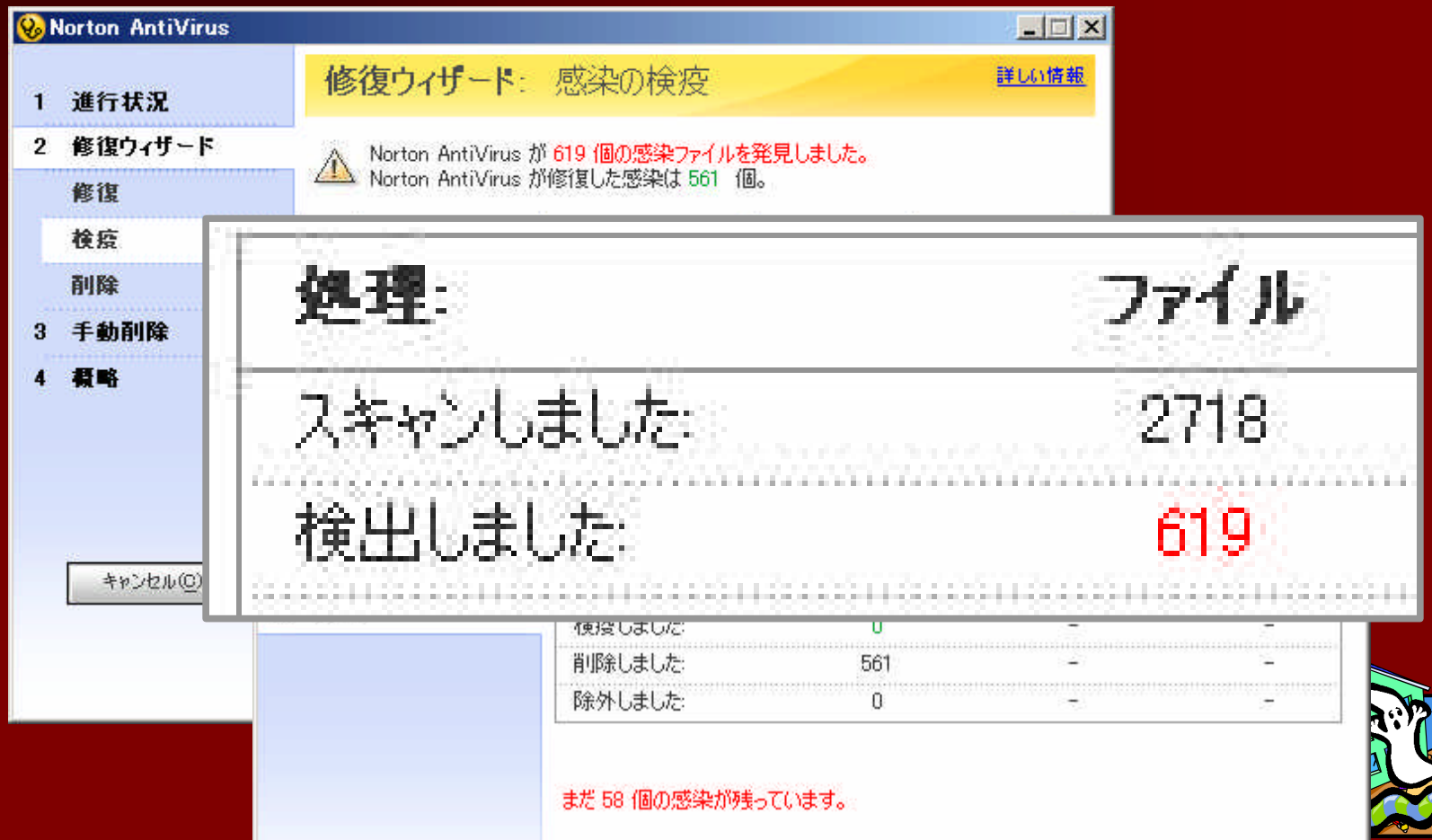




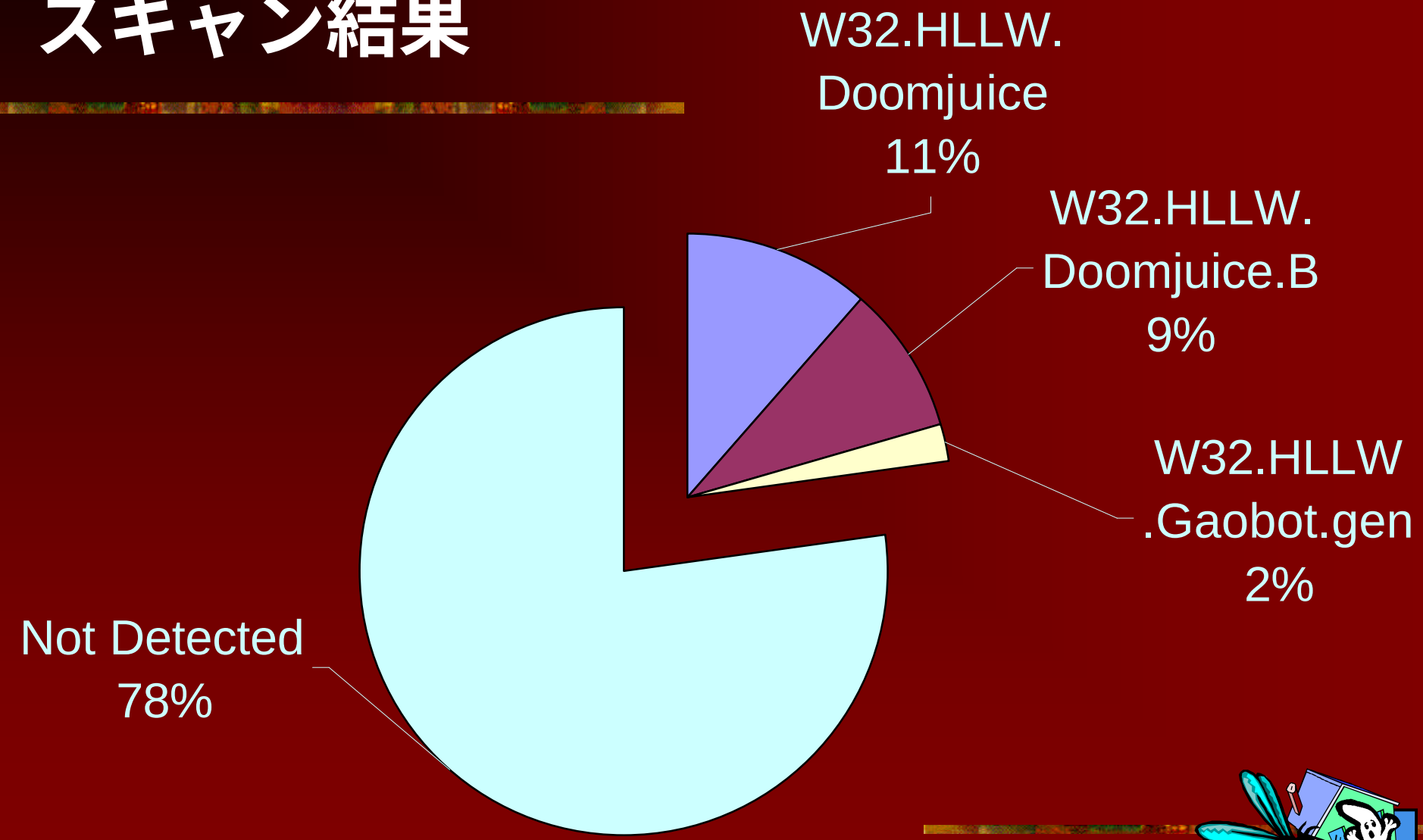
ウィルススキャン

2005/7/8現在のパターンファイルで2718ファイルをスキャンしました

が、

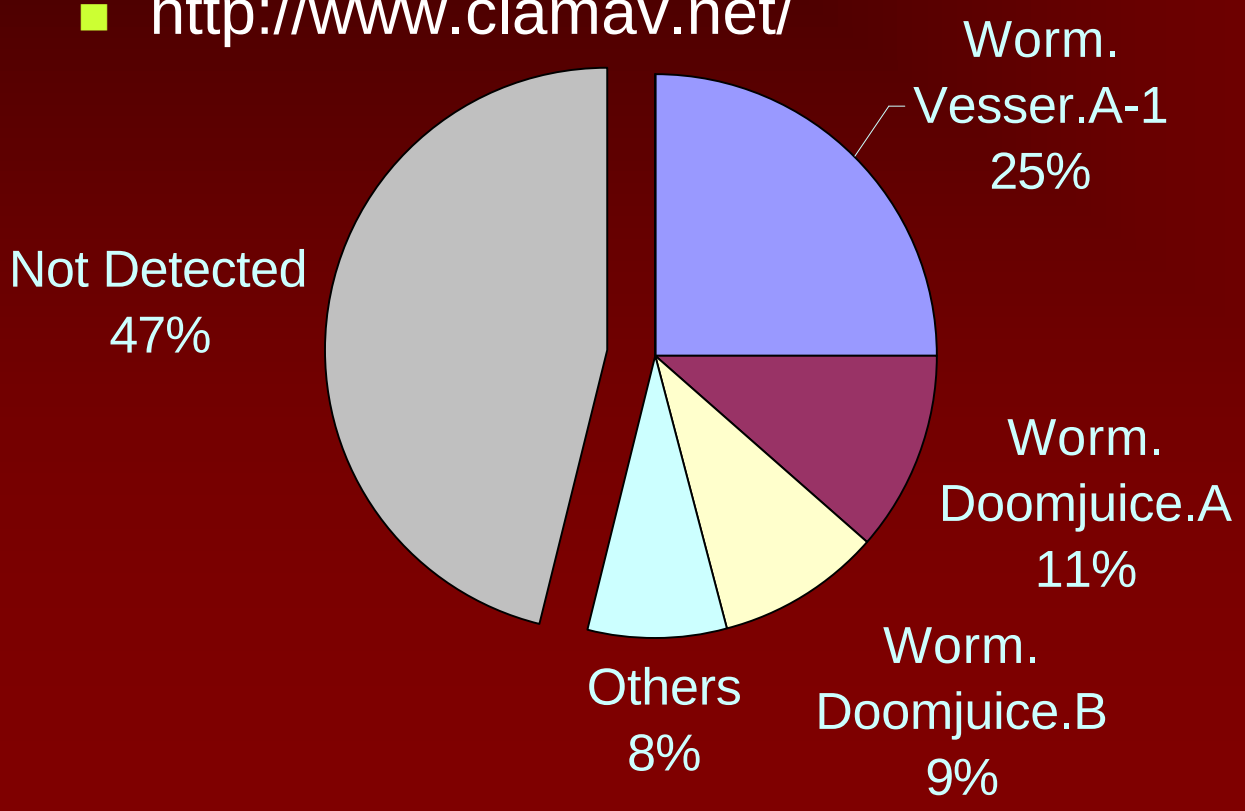


ある商用アンチウィルスソフトのスキャン結果



ClamAVでも試してみました

- オープンソースの Anti-Virus ソフト
  - ウィルスシグネチャもユーザコミュニティで作成
- http://www.clamav.net/



Virus Name	Count
Trojan.Downloader.Delf-35	51
Worm.Gaobot.HK	40
Trojan.Gobot.A	30
Trojan.Gobot.T	28
Trojan.Ghostbot.A	25
Worm.Mytob.BP	16
Worm.Mytob.GE	15
Worm.Gaobot.336	11
Trojan.Gobot.R	4
Worm.Winur.D	2
Worm.W32.Welchia.E	1

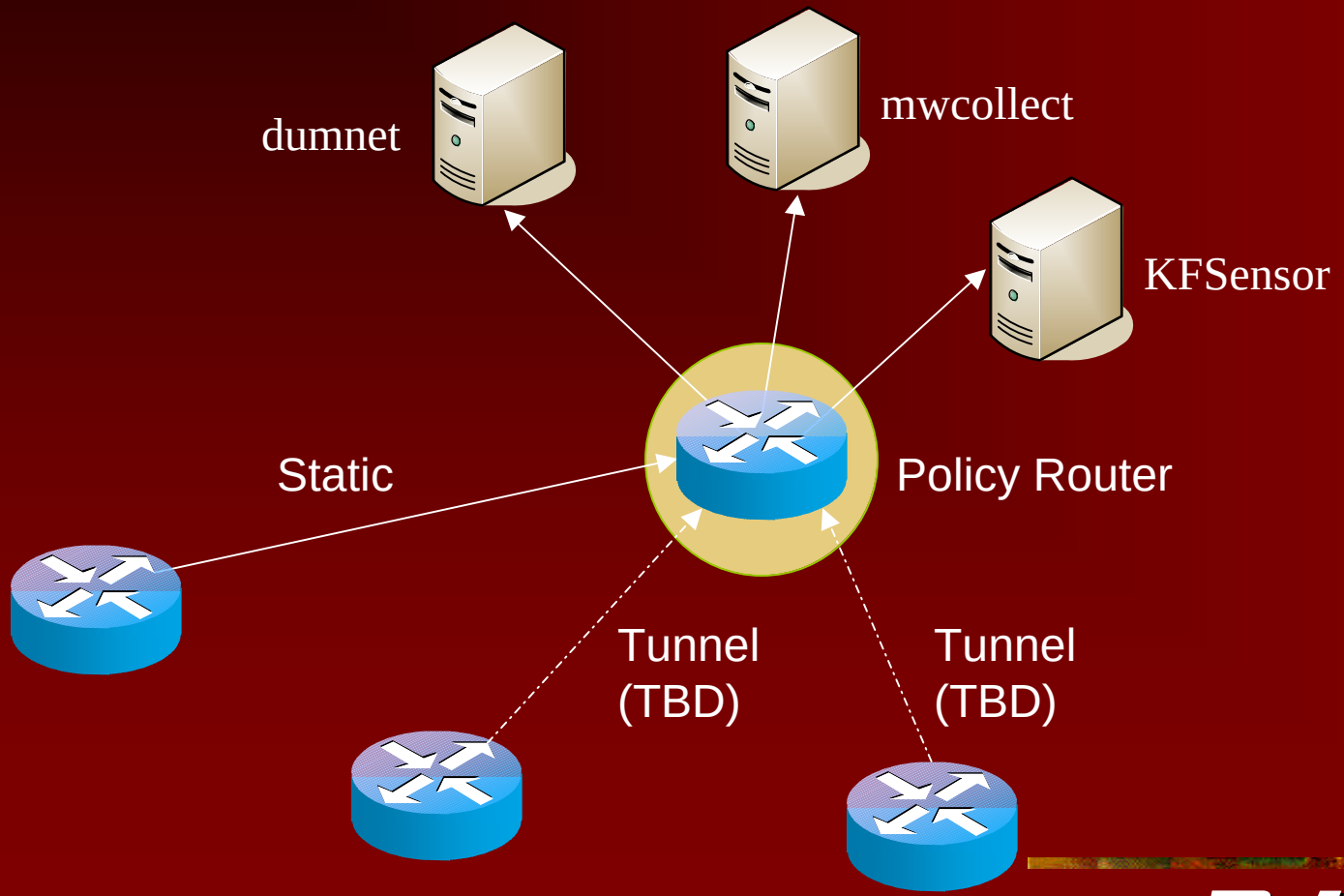
この手法の課題

- ハニーポットのIPアドレスが判明した場合、意図的なアタックが行われる恐れ
- → 観測対象のIPアドレスを分散させる
  - 他のアドレスブロックのデータから、ある程度の補正が可能に

ハニーポットの比較

Software	dumnet	Mwcollect	KFSensor
OS	*UNIX	*UNIX	Windows
Supported Protocols	TCP	Bagle Backdoor, Windows RPC, CIFS, WINS	HTTP, SMTP, CIFS, SOCKS, MS SQL, FTP, POP3, Telnet, RDP(Terminal Server), VNC, Relay
Overhead	Very Low	Low	Low
Network Interface	Not Required	Required	Required
URL	http://tf.happyhacking.net/	http://www.mwcollect.org/	http://www.keyfocus.net/kfsensor/

今後の構成


dumnet
mwcollect
KFSensor
Static
Policy Router
Tunnel
(TBD)
Tunnel
(TBD)

今後の予定

- 広域化
  - 複数拠点での展開
- ブラックリストの構築
- 統計手法の検討
  - 視覚化
- レイティング
  - 得られた情報の共有

Q&A

おねがい

- 未使用アドレス空間をハニーポット用にルーティングしてもいいという方
  - (and 計測に箱を置いてもいい)
  - 統計情報のみ公開
  - IPアドレスはいつでも返却
- ぜひ白畑 (true@sfc.wide.ad.jp) までご連絡ください！