NSP-Security-JP (NSP-SEC-JP) Update

Peers Working Together to Battle Attacks to the Internet

JANOG16 – 29 Jul 2005
Matsuzaki Yoshinobu <maz@iij.ad.jp>
Tomoya Yoshida <yoshida@ocn.ad.jp>
Taka Mizuguchi <taka@ntt.net>

Agenda

- NSP-SEC-JP Update
- Security Trend
- DoS/DDoSの対処方法

1. NSP-SEC-JP Update

1. NSP-SEC-JP Update

- **NSP-SEC-JPとは**
- **NSP-SEC-JPの現状**
- **NSP-SECとの連携**
- **Team Cymruとの連携**
- セキュリティインシデント対応
- 今後の活動予定

1.1 NSP-SEC-JPとは？

- **NSP-SECのSub-communityとして立上げ（NSP-SECと連携）**
- **MLのメンバは、ISP/ICP及びベンダのセキュリティ関連オペレータの有志で構成**
- **非公開（confidential情報交換も有）**
- **リアルタイムでのセキュリティインシデント対応ML**
- **セキュリティに関する啓蒙活動も考慮**

1.2 NSP-SEC-JPの現状

<参加人数>　　*#2005/7/1現在*

ISP　　**17名（倍くらいには増えるといいな…）**

Vender　　**3名（日本のベンダさんも…）**

Team Cymru 1名（英語はちょっと…）

ｘSPのセキュリティオペレータ募集中！！

<他組織との連携>

–NSP-SECとの連携

–Team Cymruとの連携

–JPCERT/CCさん等と連携模索中

–ベンダ（脆弱性情報の共有等）

1.3 Team Cymruとの連携

- 個別インシデント毎のセキュリティレポート
  - 各種ウィルス・ワーム毎の感染ホスト情報
  - DDoSコントロールサーバの情報
  - SPAMホストの情報
- Documentの日本語化
  - 最近、あまり出来てません…。
- Bogon route-server
  - –アジアで初のbogon route-serverを日本に立上げ

FYI:

7/4からTeam Cymruが会社として再スタート！！

1.3.1 bogonルートサーバ

- アジアで初の **bogon route-server** を東京に設置
  - 世界で5台目
  - http://www.cymru.com/BGP/bogon-rs.html.jis
- bogonな最新の経路をBGPで配信するプロジェクト
  - **bogon**ルート情報が何かを経路情報を見て即座に確認可能
  - **AS65333**（全て共通）、**community = 65333:888**
  - 様々な用途に利用可能
    - **community** でマッチさせて、**next-hop** を **null0**に向ける
    - **filtering**の元情報として利用する

Peerの方法については、別途アナウンスします！

1.3.2 セキュリティレポート

ウィルス	日本の感染AS数			日本全体のAS感染率		
Virus	2004/6	2005/1	2005/7	2004/6	2005/1	2005/7
Beagle Beagl3	69 ---	48 49	1 31	14% ---	9% 9%	6%
Blaster	76	30	65	15%	5%	12%
Mydoom	26	6	3	5%	1%	0.5%
Nachi	28	6	22	5%	1%	4%
Slammer	68	28	31	14%	5%	6%
SPAM	130	66	118	26%	12%	22%
Phatbot+bot	---	102	94	---	18%	17%
scanner	---	22	61	---	4%	11%

- JPNICによる割り当てAS数：494（2004/06）、552(2005/1)、543（2005/7）
- AS感染率は日本の全ASからの割合

1.4 uRPFを日本で真面目にやろう

- 経路情報を利用した **Ingress Filter** の手法
  - unicast Reverse Path Forwarding
- 利点
  - 経路情報の変化に応じて動的に対応可能
  - トポロジーの変化などに応じた、静的な設定の整合性を保つ必要がない
- 欠点
  - 経路制御の変更時に注意が必要
- **RFC3704（BCP84）**
  - Ingress Filtering for Multi-homed Networks
- **RPF（Reverse Path Forwarding）**
  - 1. Strict Reverse Path Forwarding
  - 2. Feasible Reverse Path Forwarding
  - **3. Loose Reverse Path Forwarding**

ベンダの皆様、実装よろしくお願いします

1.5 今後の活動予定

- セキュリティ情報の収集
  - 自前での監視機器の設置
- 他組織（JPCERT/CC等）との連携
- セキュリティDocumentの和訳
- iNOC-DBAのサポート

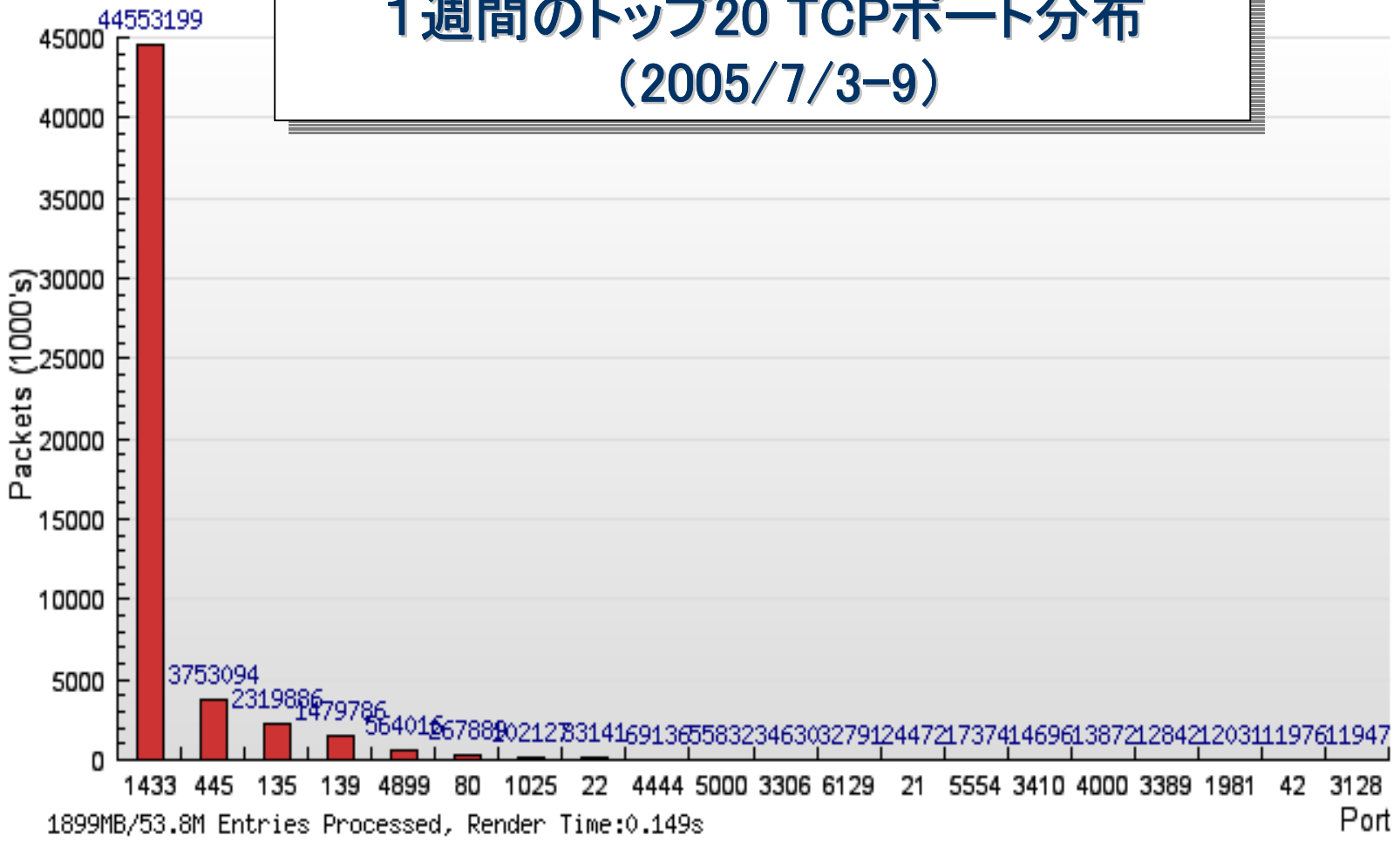
2. Security Trend

2.1 パケットタイプ別トレンド

Darknet手法による不正パケットモニタリングデータから以下の項目毎の傾向把握

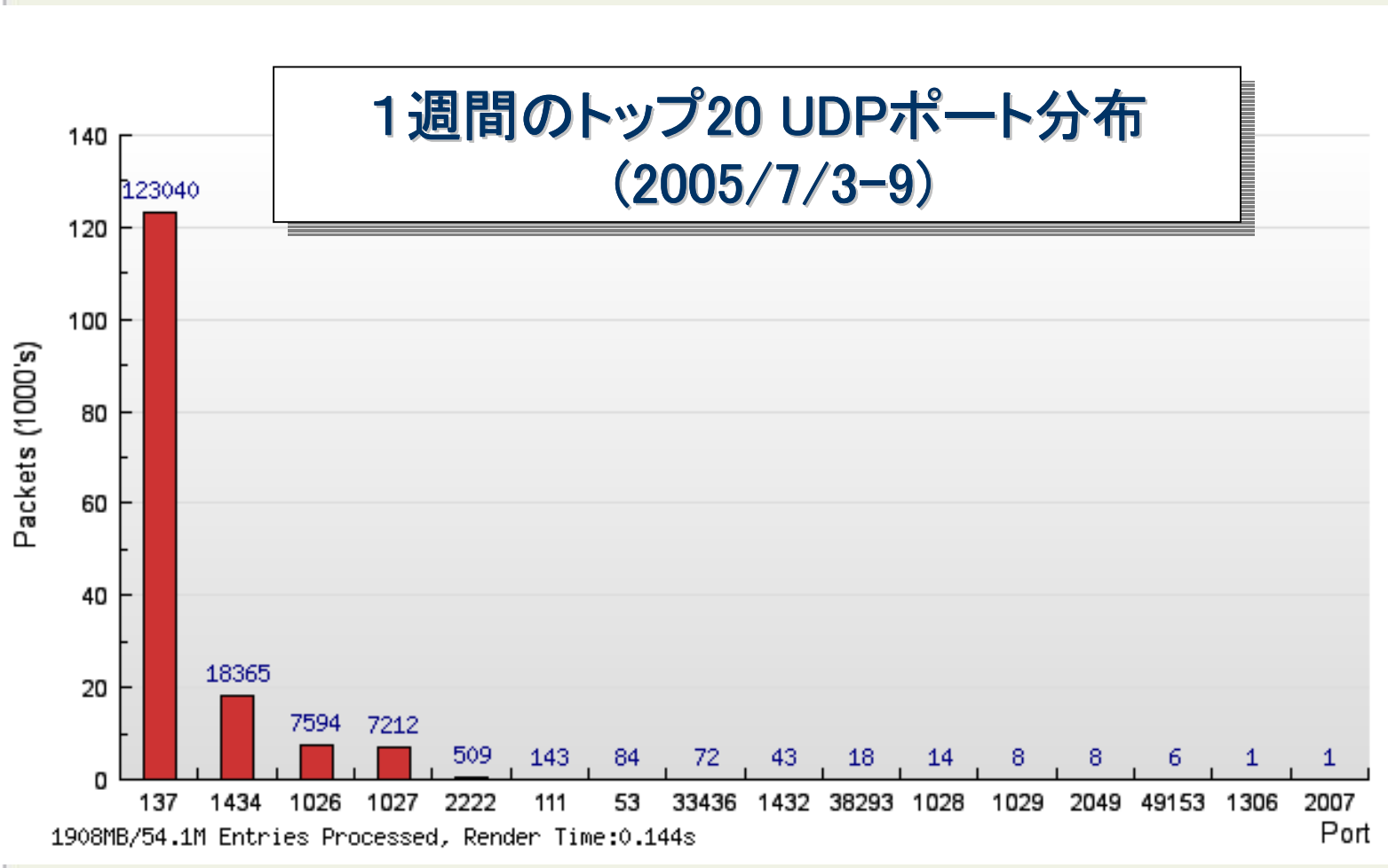
- –TCPポート別
- –UDPポート別
- –Warmトラフィック

2.1.1 TCP Port別



・Port1433：MS SQLサーバの脆弱性へのアクセス

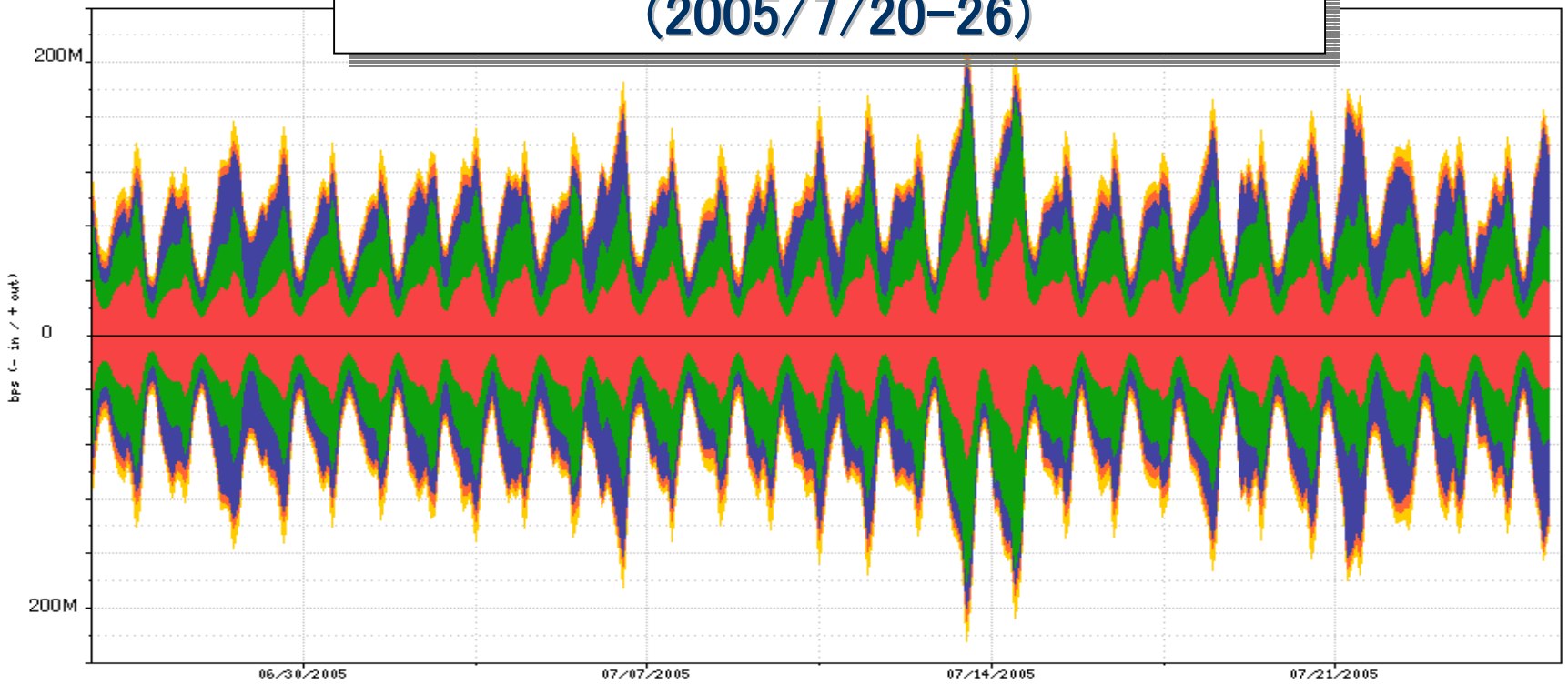
2.1.2 UDP Port別



- Port137：NBTへのアクセス（Blaster等でのアクセス、Signatureはバラバラ）
- Port1026：Messengerへのアクセス（Messenger SPAM、バッファオーバーラン）
- Port1434：Slammerがいまだに収束していない

2.1.3 Wormトラフィック

1週間のトップワーク分布
(2005/7/20-26)



- W32/Sasser-A
- Doomjuice
- Deloder.A
- Dabber.A
- SQL Slammer

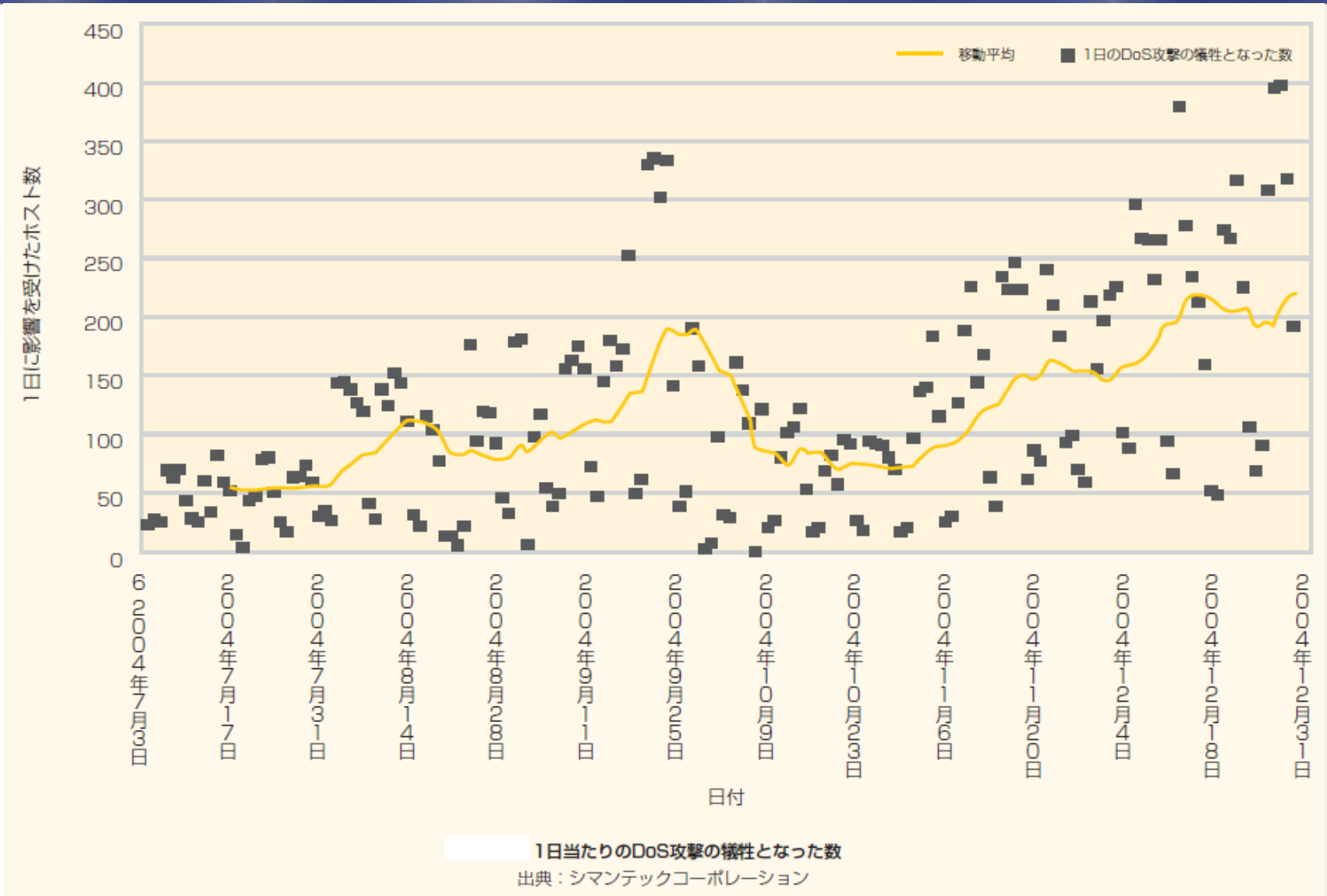
2.2 Security Trend overview

- セキュリティ犯罪の種類が変化
  - フィッシングからDNSポイゾニングまで
  - 金銭目的の犯罪化へ
  - 直接攻撃から間接的な攻撃へ
- 被害が社会問題化
  - 中国からのDDoSアタック被害
  - 価格.com等への不正アクセス＆ウィルスばらまき事件
  - 後を絶たない個人情報の流出（仁義なきキ〇タマ、トロイの木馬）

2.2.1　ネットワークセキュリティに関わる被害

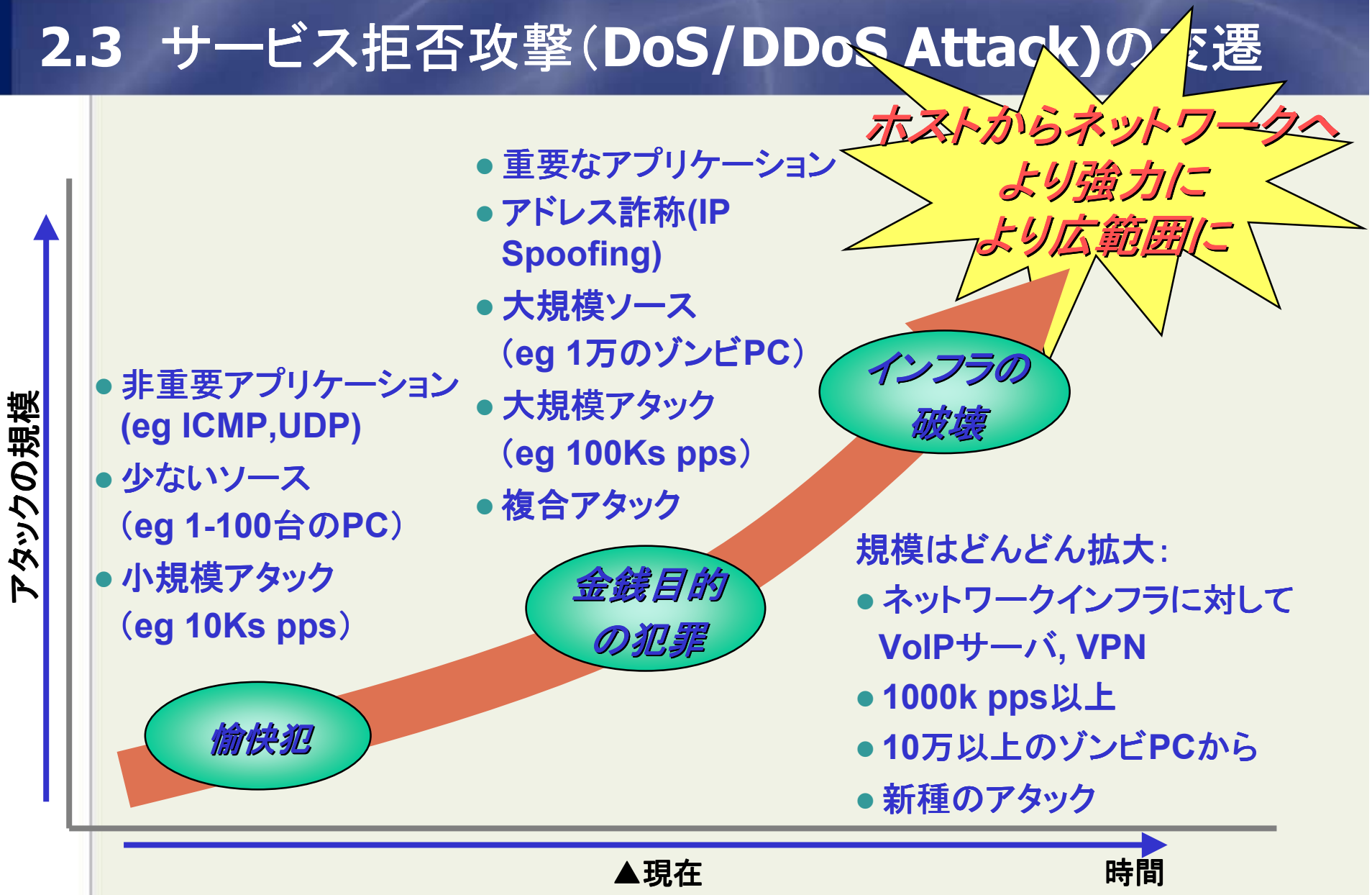
業界別の標的攻撃（出典）シマンテックコーポレーション

2.2.2 DDoS攻撃状況



出典：シマンテックコーポレーション

2.3 サービス拒否攻撃(DoS/DDoS Attack)の変遷



2.4 日本サイトへのDDoSアタック

- 期間

  2004/8/1-

- 攻撃対象

  政治色の強いサイト（靖国神社、自衛隊などなど）

- 攻撃手段

  TCP SYN flood, TCP ACK flood, connection flood, GET flood, POST flood, UDP flood, ICMP flood, ip proto 255 flood, igmp flood

  ~数百Mbps程度のアタックが観測

  ツールも使われていると思われる。

- 攻撃の影響

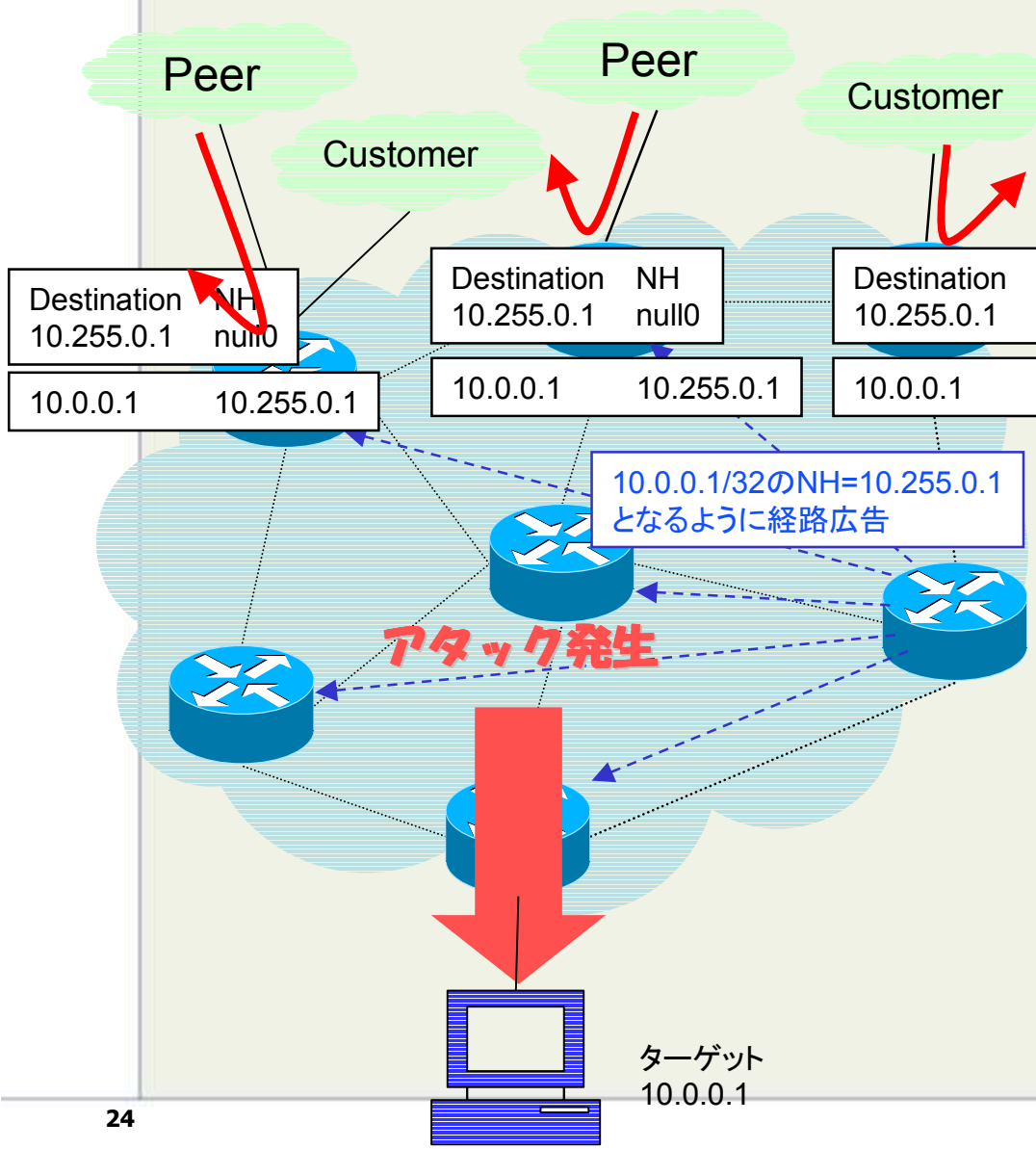
  WebサイトがDown、高負荷によるアクセス障害

3. DoS/DDoSの対処方法

3.1 アタックの対処（DoS/DDoS対処技術）

- パケットフィルタリング
- Black hole/Discard routing by static
- **RTBF（Remote Triggered Black Hole Filtering）**
- **RTBF control by customer**
- セキュリティ関連新技術

3.2 RTBF/RTBH



＜事前設定＞

境界ルータでblack hole用アドレス(10.255.0.1)に対してnull0にルーティングするように設定する

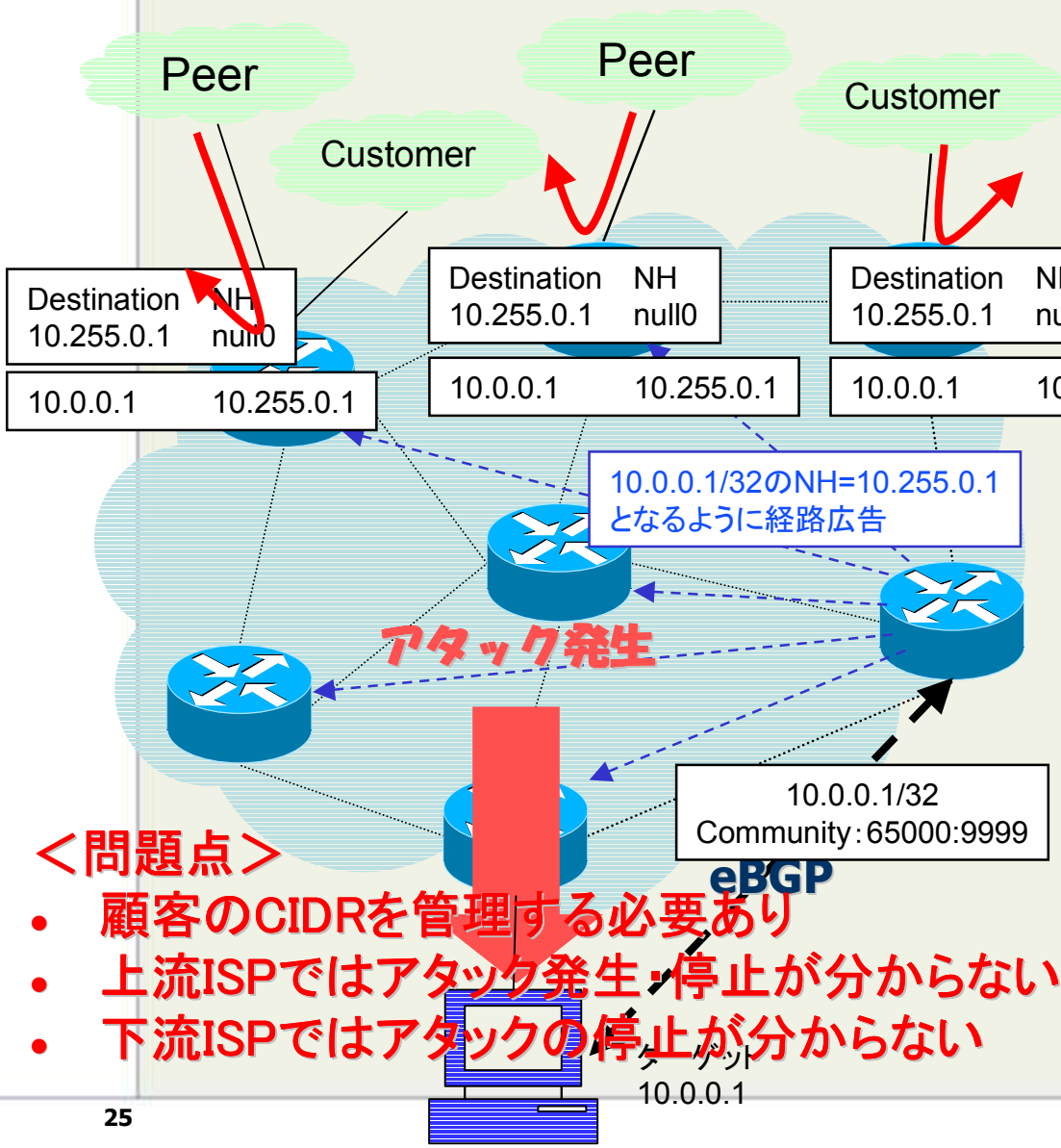
＜Attack発生後＞

VictimアドレスのNHをblack hole用アドレスとして広告する

＜効果＞

- **1ヶ所のRoute Serverの設定のみでAttackパケットを破棄**
- **迅速にネットワーク資源を守る**

3.3 カスタマ制御によるRTBF/RTBH



＜事前設定＞
- RTBFの設定
- RTBF用eBGPセッション
  ISP側:（経路受信条件）
  ー顧客のCIDR内の/32
  ーblack hole用communityの経路

＜アタック発生時＞

顧客:
アタックを受けているサイト(/32)の経路にblack hole用communityを付与して経路広告。

ISP側:
境界ルータで受信経路のnexthopをblack hole用アドレス(10.255.0.1)に書き換えて他ルータに広告する。

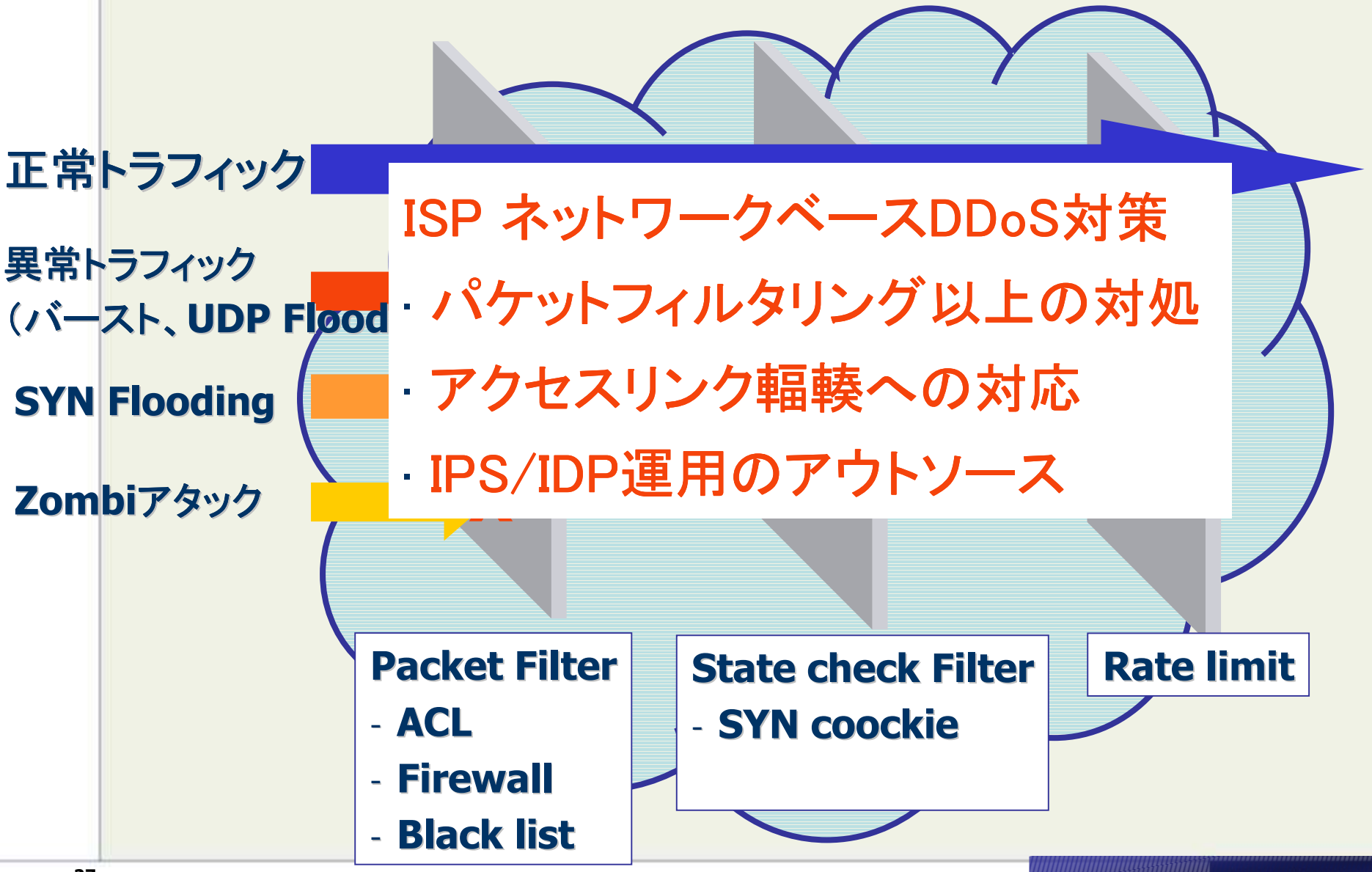
＜問題点＞
- 顧客のCIDRを管理する必要あり
- 上流ISPではアタック発生・停止が分からない
- 下流ISPではアタックの停止が分からない

＜効果＞
- 顧客による上流ISPのFiltering制御ができる
- 上流ISPでの運用が不要

3.4 セキュリティ関連新技術

- ネットワークベースScrubbing/Cleansing
- BGP Flow Specification
- ソースアドレスベースRTBH
- 地域型RTBH
- Fingerprint sharing

3.4.1 スクラビング/クレンジング



3.4.2 BGP Flow Specification

- 定義：
  - –draft-marques-idr-flow-spec-03.txt
    - #June 16, 2005に期限切れ
- **BGPでのフロー詳細ルール（Flow specification rule）の配送方法を明記**
- **(D)DoSアタック軽減を目的としたパケットフィルタリングのための付加機能**
- フロー詳細ルールを**BGPのNLRI**としてエンコードする手順を定義

3.4.2 BGP Flow Specification (2)

- **flow specification**とは、**IP**パケットデータに当たる複数の条件の組み合わせを表す
- 到達性情報（**NEXT_HOP**等）は含んでも含まなくてもよい
- **Well-known**もしくは**AS**個別の**community**を設定された動作（**blackhole**、**PBR**、**rate-limit**等）のトリガとして使える
- アプリケーションは、**specific**（**AFI,SAFI**）ペアとで特定され、**RIB**のセットと区別に相当する

3.4.2 BGP Flow Specification (3)

Flow specification encoding例：

“10.0.1/24 TCP 25 に対する全パケット”

```
+--------------+---------+---------+
01 18 0a 00 01 03 81 06 04 81 19
```

＜タイプ＞

01: Source address

03: Protocol

04: Port

Let’s Join NSP-SEC-JP !!

参考URL:

- http://puck.nether.net/mailman/listinfo/nsp-security-jp
- http://www.cymru.com/
- http://www.symantec.co.jp/region/jp/istr/
- http://www.cqr.org/mailman/listinfo/flow-spec/