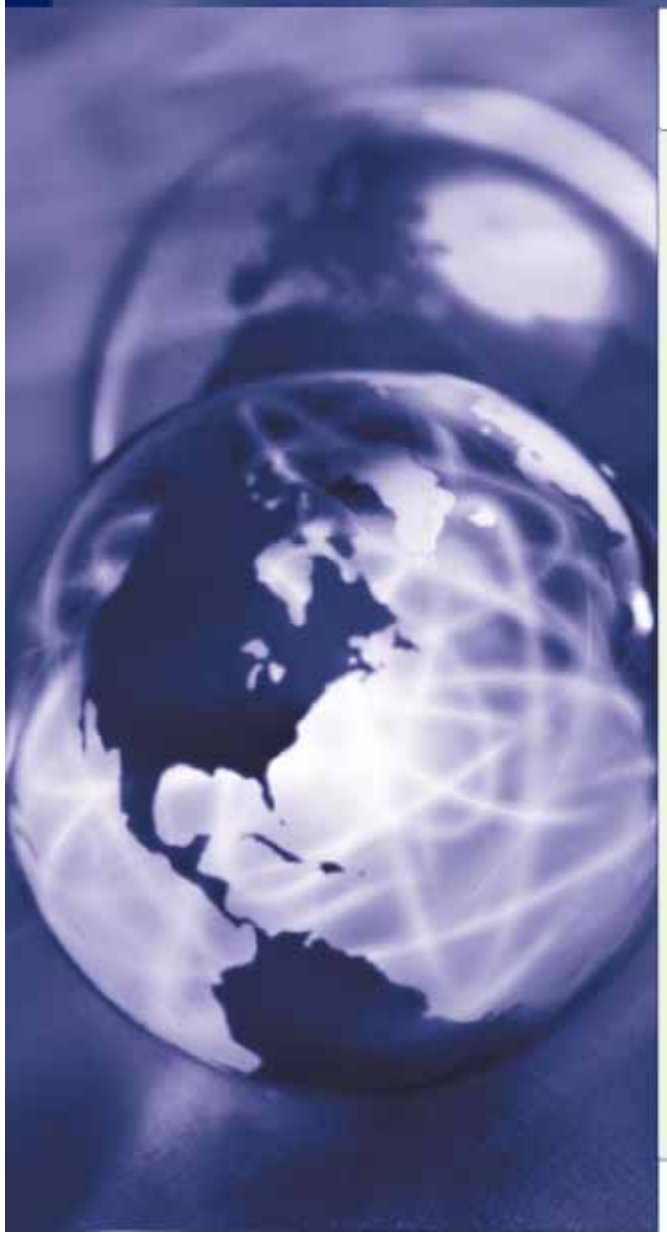


NSP-Security-JP (NSP-SEC-JP) Update

Peers Working Together to Battle Attacks to the Internet

JANOG17 – 20 Jan 2006
Matsuzaki Yoshinobu <maz@iij.ad.jp>
Tomoya Yoshida <yoshida@ocn.ad.jp>
Taka Mizuguchi <taka@ntt.net>

Agenda

- NSP-SEC-JP Update
  - ISPにおけるbogon routesフィルタリングの現状
  - bogonルートサーバの活用
- ISP Security surveyの結果
- Source Address Validation
  - 送信元検証
  - ACL, uRPF
  - How to use uRPF

1. NSP-SEC-JP Update

1. NSP-SEC-JP Update

- NSP-SEC-JPとは
- NSP-SEC-JPの現状
- Bogon Route-severについて
- 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>　　*#2006/1/6現在*

ISP　　25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！！

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

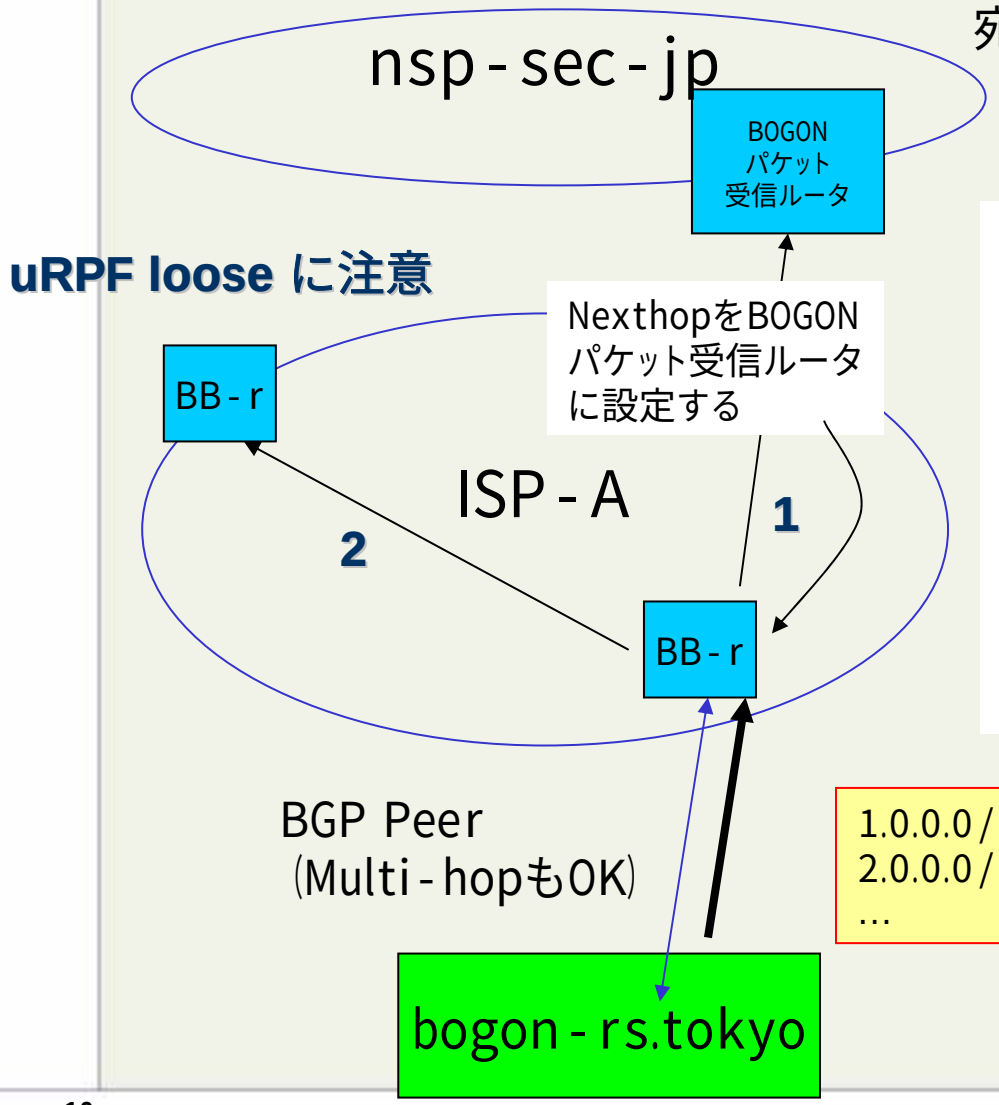
1.3.2 ISPにおけるBogon経路のフィルタリングの現状

- Bogonフィルタリングを実施しているISPが世界中にいる
  - 未割り振りアドレス空間
  - Privateアドレス、Link Localアドレス、TestNetアドレス、Multicastアドレスなどなど
- フィルタの更新が適切に行われていない
  - ISPそれぞれの運用ポリシーで実施されている
  - 未更新によりアドレス割り当て時に通信障害になる
  - リアルタイムでの運用対応が難しい

1.3.3 bogon route-serverの利用

- 経路情報
  - origin AS = 65333
  - community = 65333:888
- 様々な用途に利用可能
  - bogon経路宛のパケットを吸い込んで解析
    - ただしuRPF loose modeでsource addressが bogonなパケットをdropさせている場合には注意が必要
  - filteringの元情報として利用する
    - パケットフィルタ
    - 自動で経路フィルタ(含むmore specific)できれば嬉しい！！！

1.3.4 bogon route-serverの利用



1. ISPの内部から発生しているbogonルート宛てのPacketを集めて解析

2. BB-rで経路を受信する際に
 match community=65333:888
 set next-hop 192.0.2.1
 set local^pref 253
などを設定

破棄したいルータで
ip route 192.0.2.1 255.255.255.255 null0

などにしておくと、パケットを廃棄できる

```
1.0.0.0/8 community=65333:888 no-export
2.0.0.0/8 community=65333:888 no-export
...
```

2. Security Trend

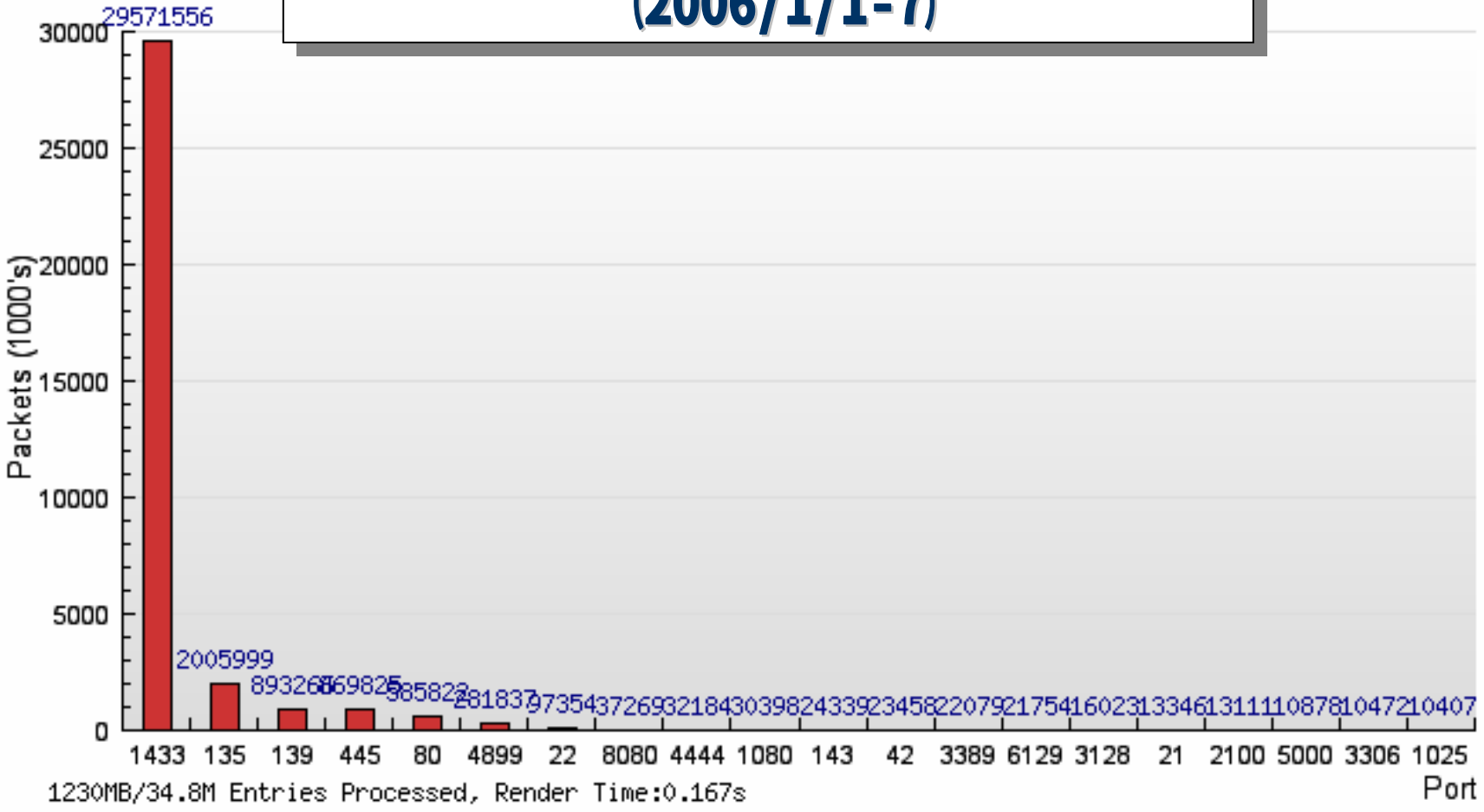
2.1 パケットタイプ別トレンド

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**

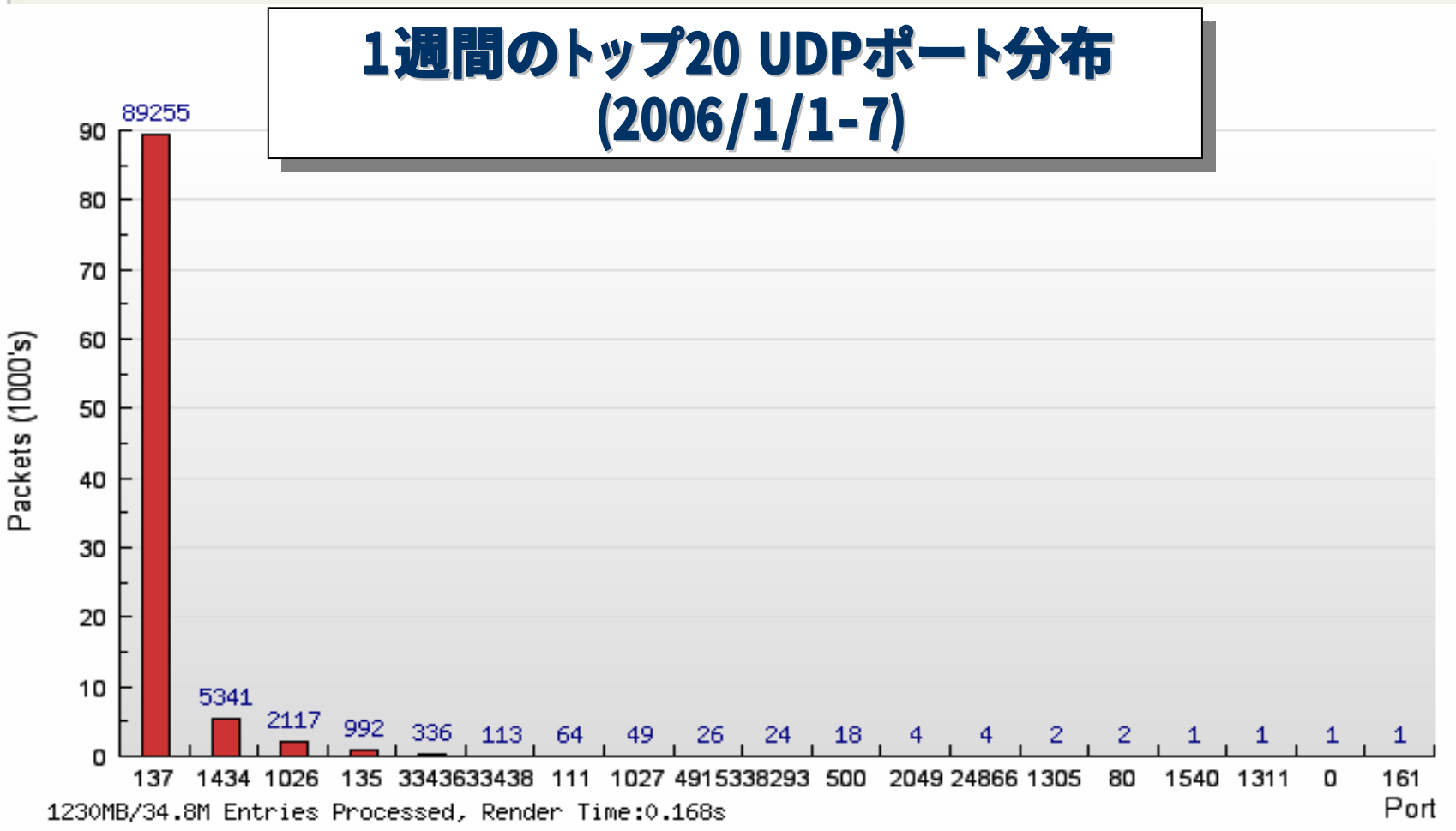
2.1.1 TCP Port別

1週間のトップ20 TCPポート分布 (2006/1/1-7)



・Port1433：MS SQLサーバの脆弱性へのアクセス

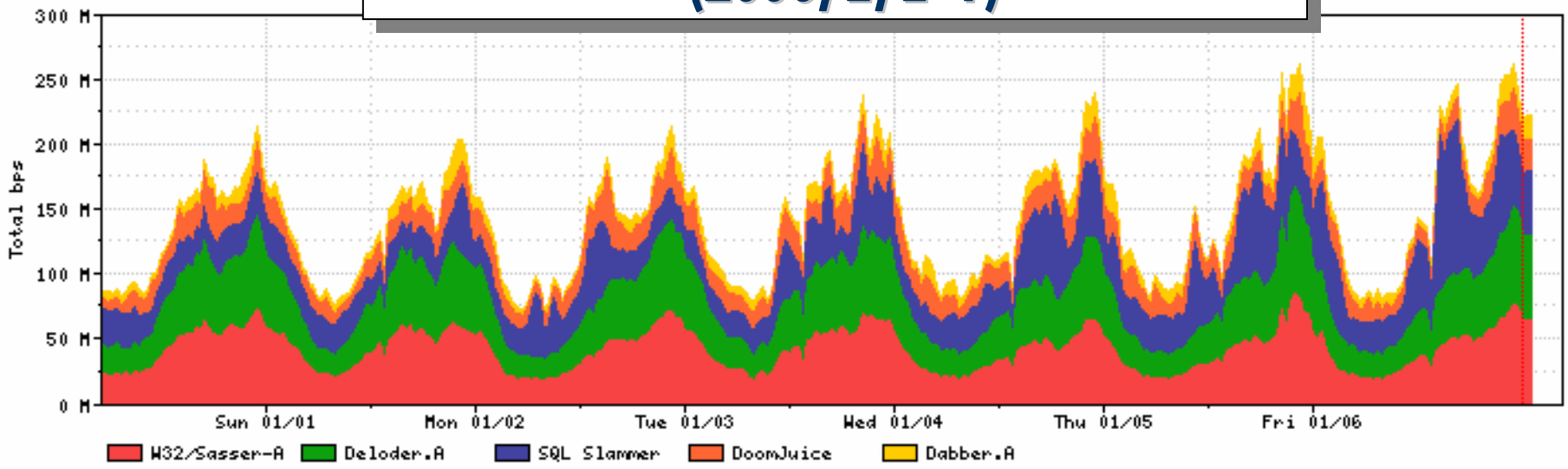
2.1.2 UDP Port別



- 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

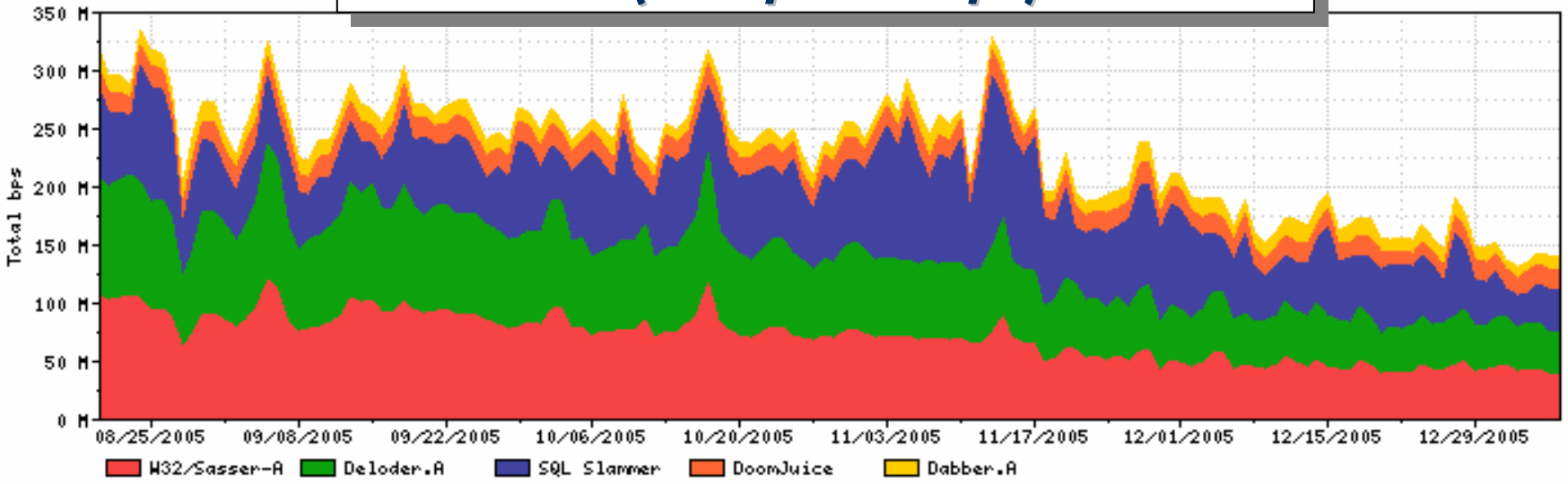
1週間のトップワーク分布 (2006/1/1-7)



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

2.1.4 Wormトラフィック

6ヶ月間の推移
(2005/8-2006/1)

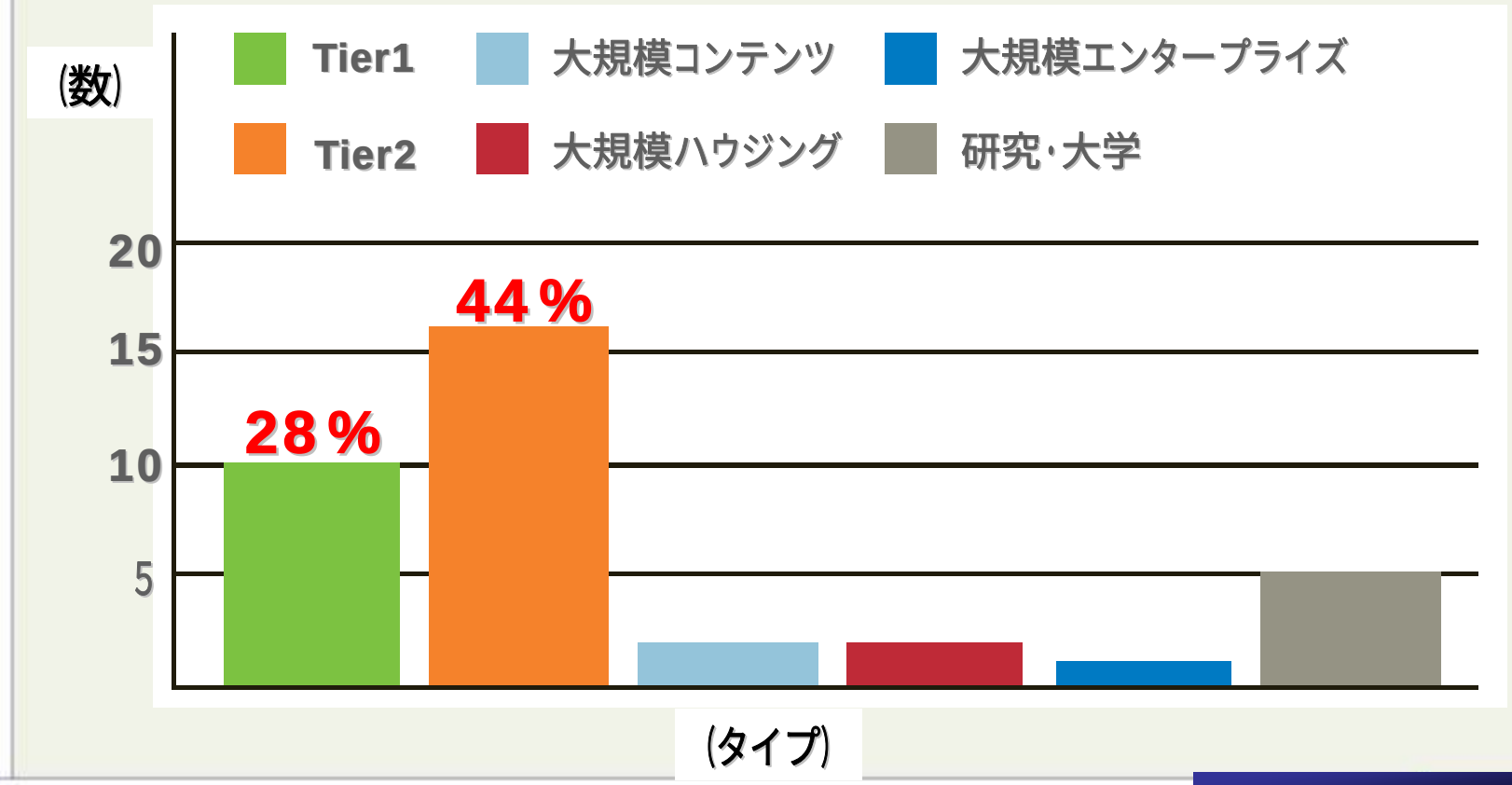


- W32/Sasser-A
- Doomjuice
- Deloder.A
- Dabber.A
- SQL Slammer

2.2.1 ISP Security Survey

＜調査対象＞

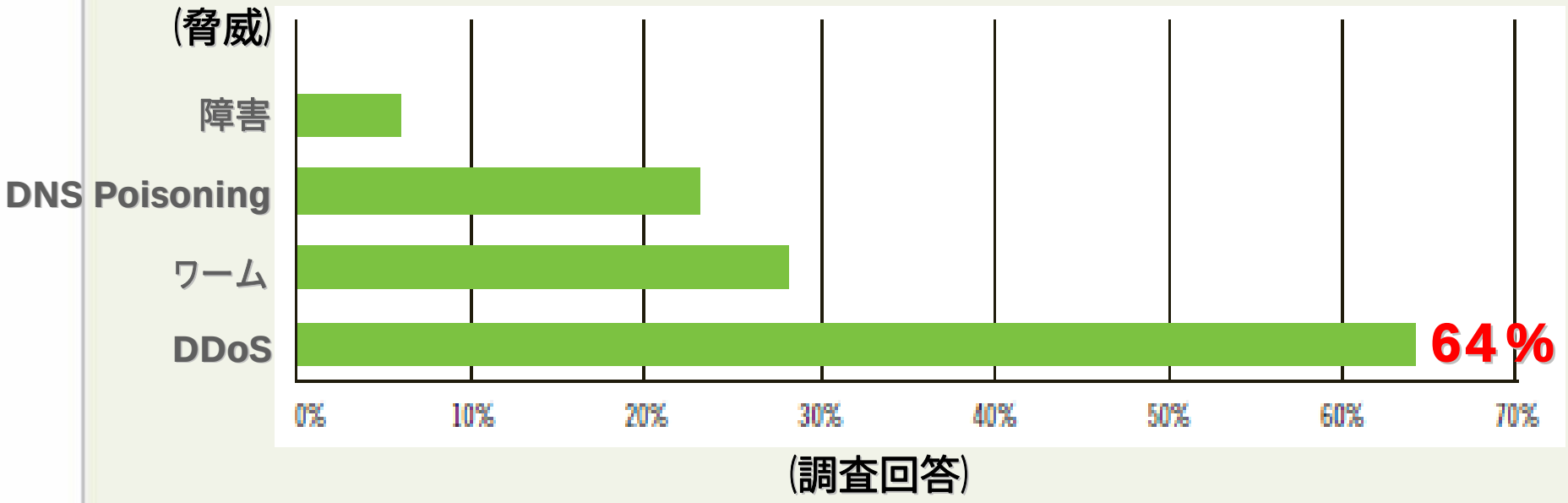
- 全世界の（アメリカ・アジア・ヨーロッパの）大規模ネットワーク
- Tier-1/2 ISP、大規模コンテンツ/ホスティングネットワークから大学まで



2.2.2 ISP Security Survey

【問：運用上の脅威】

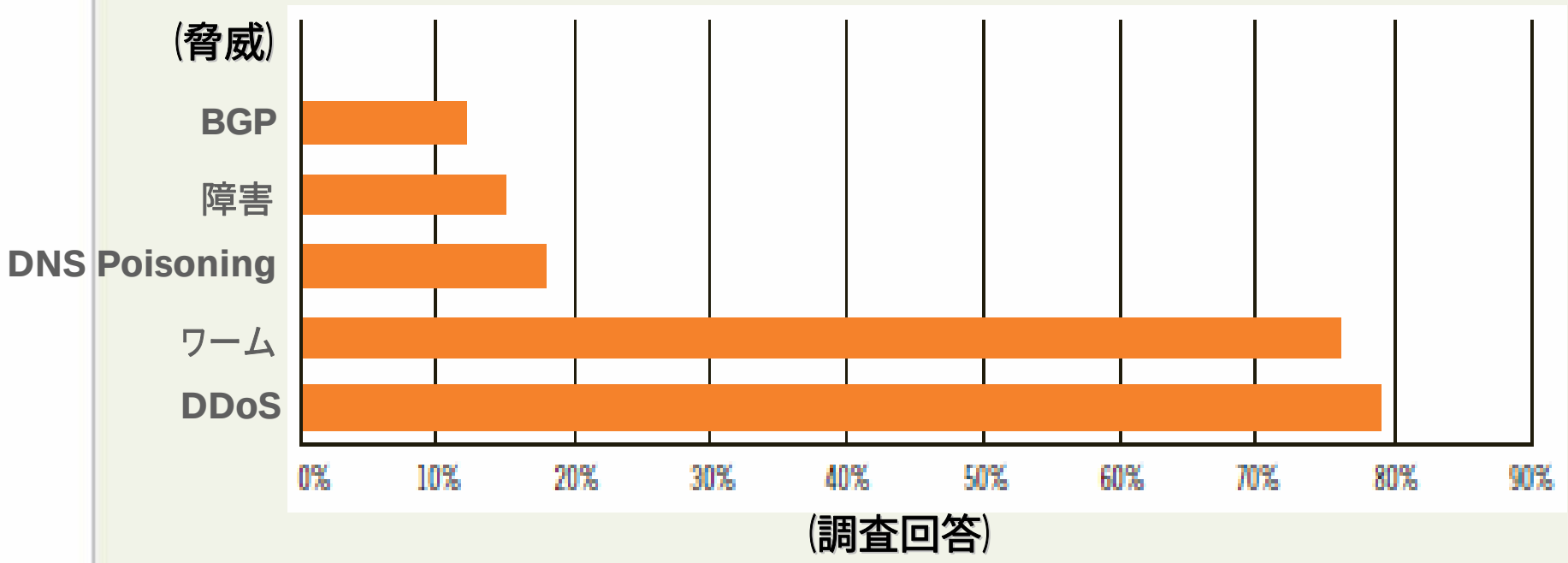
ネットワークセキュリティ運用者にとって、今もっとも脅威となる
セキュリティ問題は？



2.2.3 ISP Security Survey

【問：運用上の脅威】

現在、ネットワークセキュリティ運用者にとって脅威となっているものは？

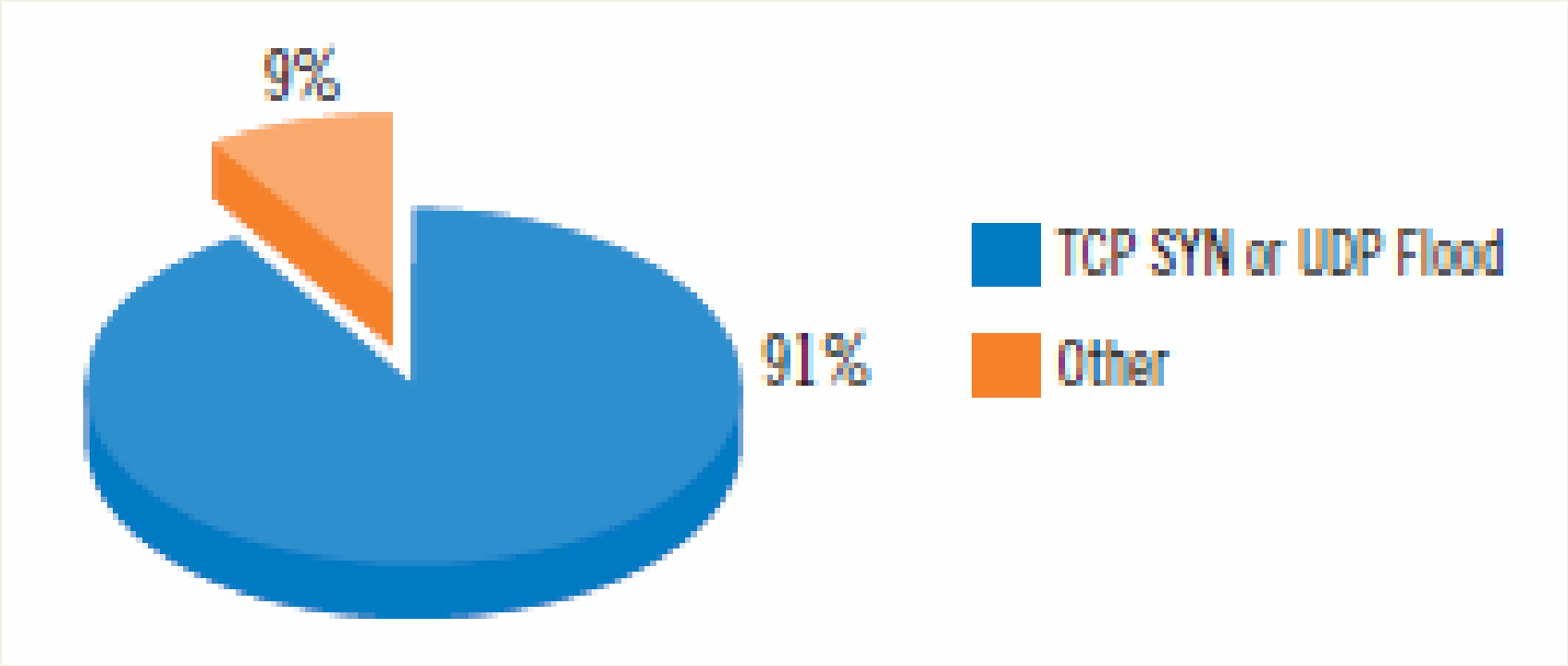


注：BGP：経路ハイジャッキング、BGPプロトコルの脆弱性

2.2.4 ISP Security Survey

【問：アタックに関して】

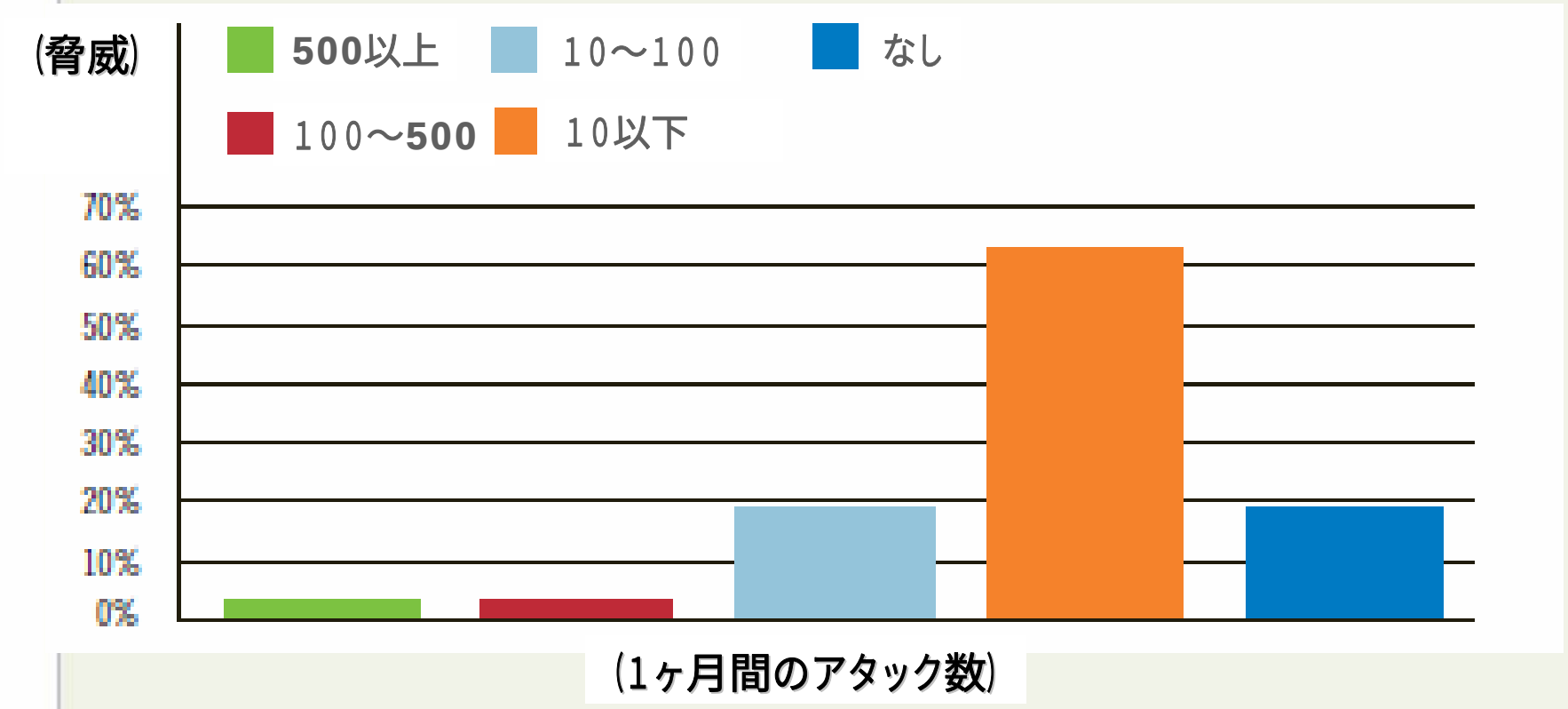
もっとも多く観測されたアタックは？



2.2.5 ISP Security Survey

【問：アタックのサイズと頻度】

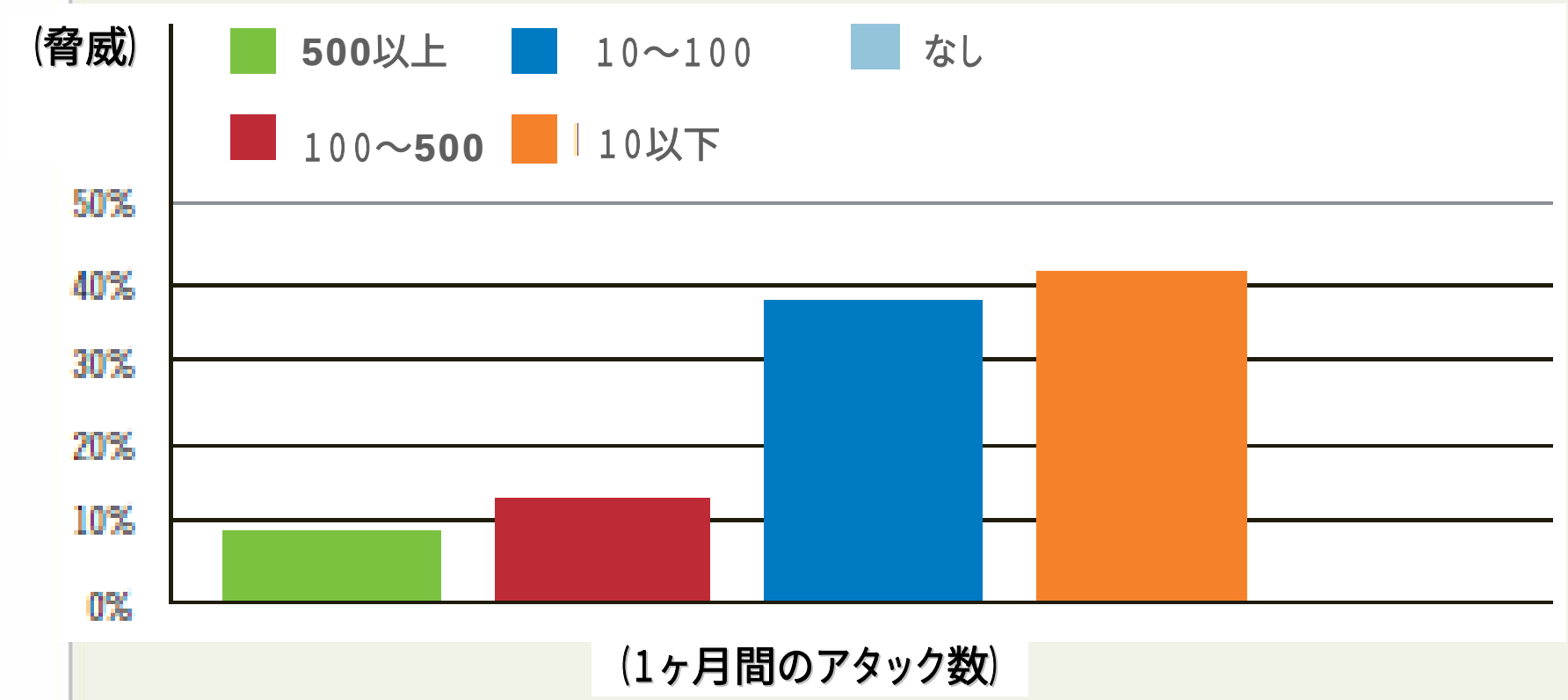
一ヶ月にインフラに影響のあるアタックの平均発生数？



2.2.6 ISP Security Survey

【問：アタックのサイズと頻度】

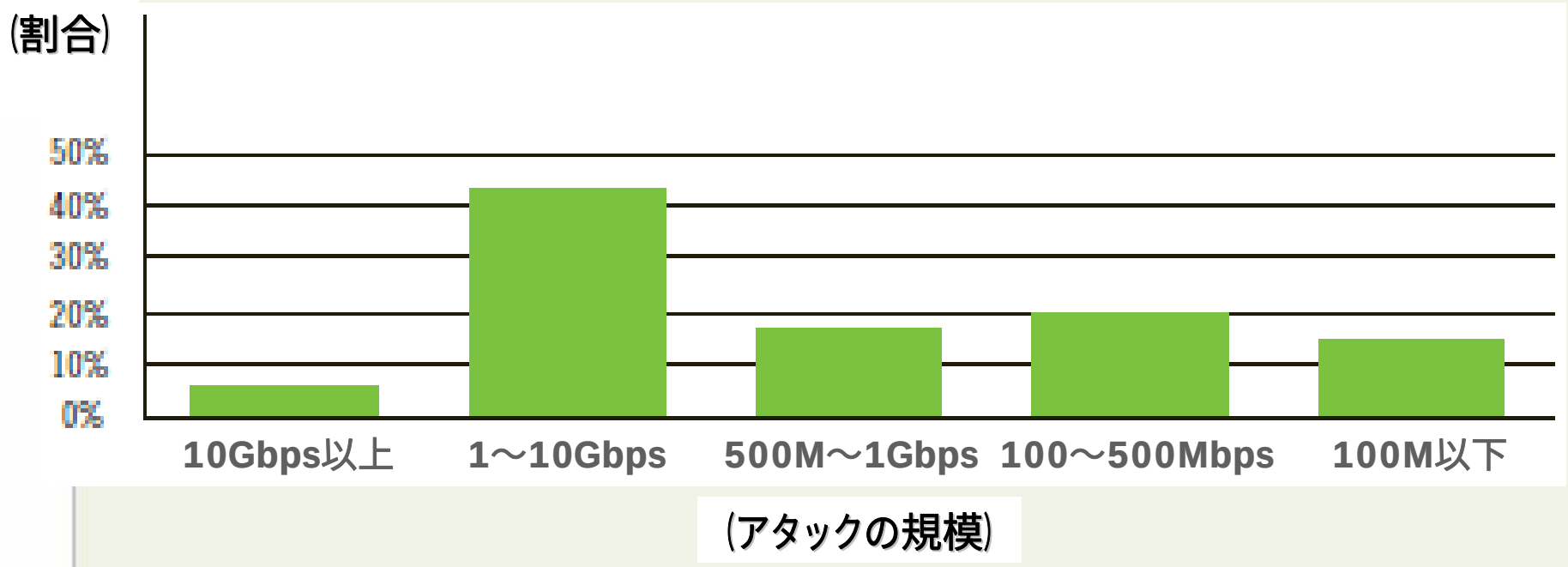
一ヶ月にカスタマに影響のあるアタックの平均発生数？



2.2.7 ISP Security Survey

【問：アタックのサイズと頻度】

過去6ヶ月以内に観測された影響のあるアタックの規模？

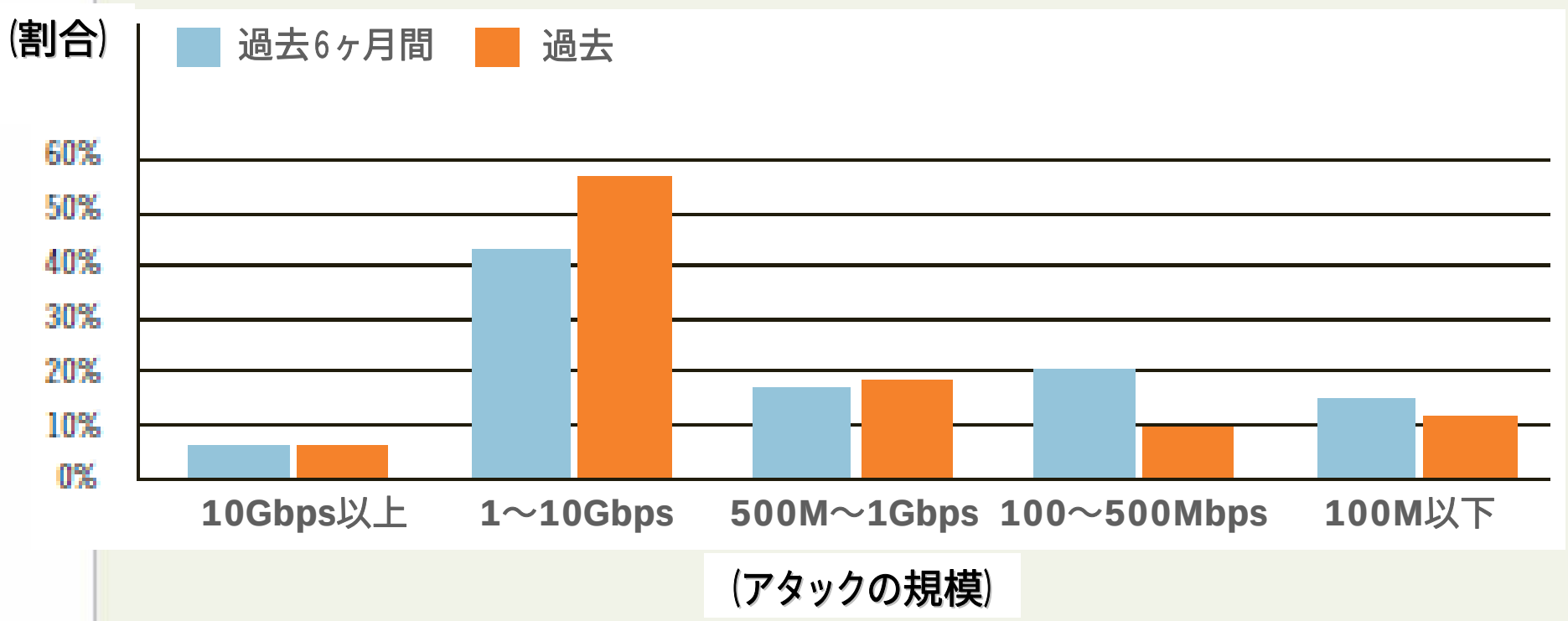


- 全Tier-1 ISPは1G以上のアタックを経験
- Tier-2とコンテンツプロバイダの多く(85%)は500M-1Gbps

2.2.8 ISP Security Survey

【問：アタックのサイズと頻度】

過去に観測された影響のあるアタックの規模？



2.2.9 ISP Security Survey

【問：アタックターゲット】

アタックのターゲットは？

- 過半数がギャンブルサイト、アダルト系Webサイトと回答
- それ以外では、IRCサーバ、RIAA(全米レコード協会)
- 1つのISPが中国と回答

  アタックのソースでもあり、ターゲットでもある

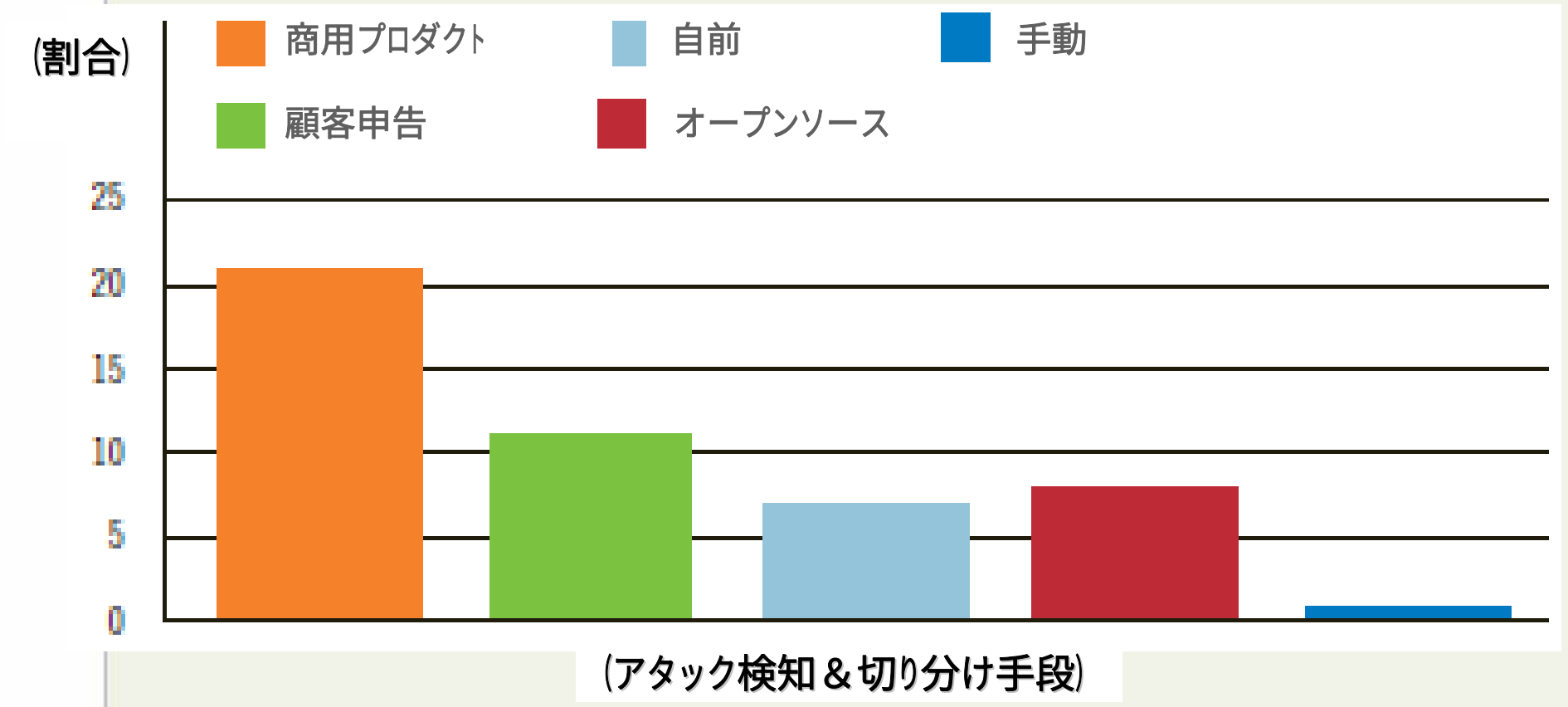
解説：

このような攻撃の背景には、インターネットの安定性、脆弱な回線を攻撃し、企業に対する金銭的な脅迫をする目的がある。

2.2.10　ISP Security Survey

【問：アタックの検知】

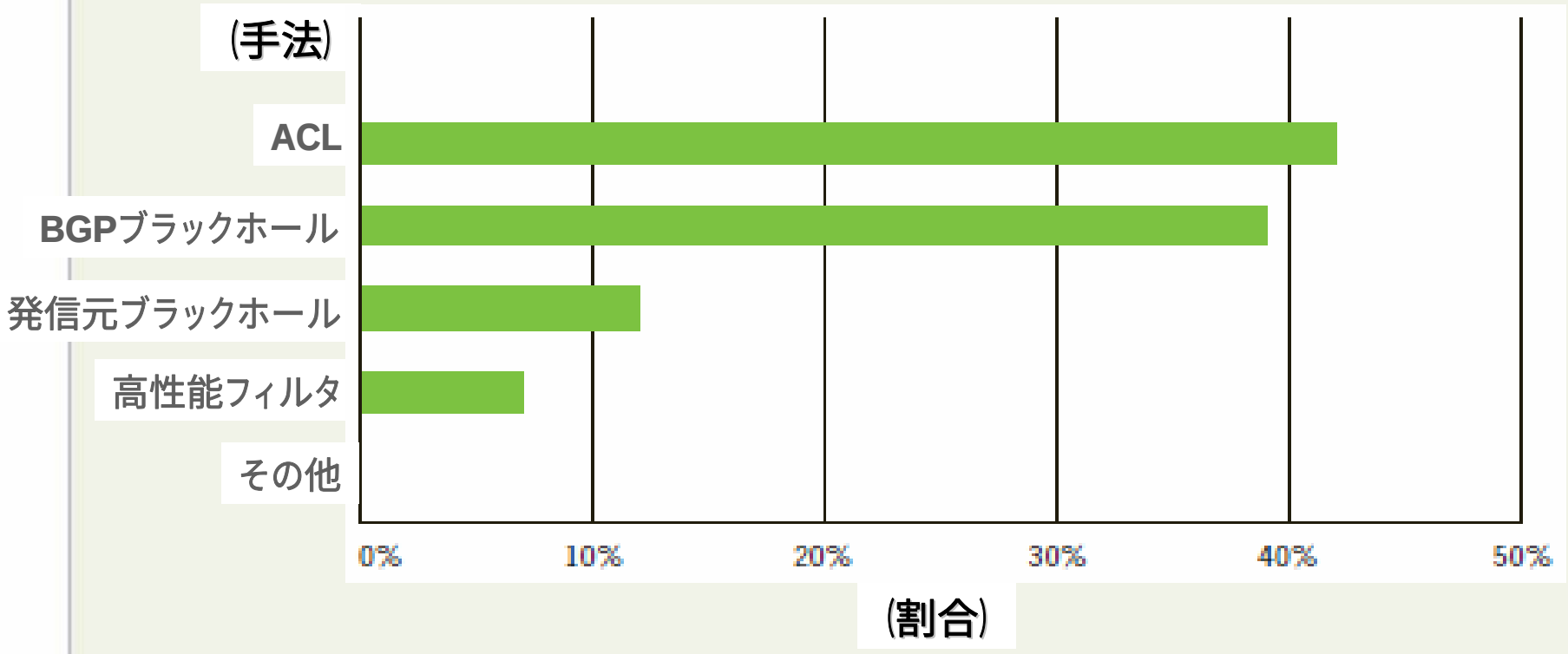
ネットワーク運用者がアタックを検知＆切り分けするためのシステムは？



2.2.11 ISP Security Survey

【問：アタックの軽減方法】

主な軽減方法は？



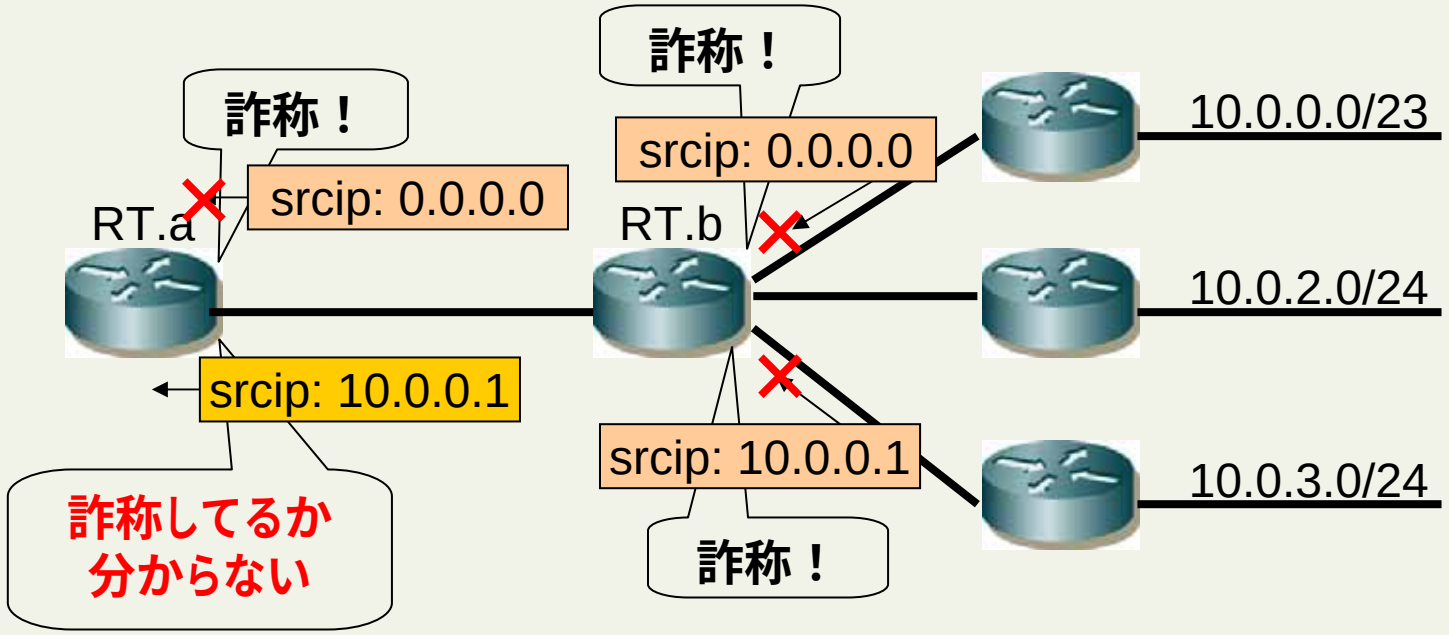
3 Source Address Validation

～ 送信元検証 ～

3.1 やりたいこと

- **Source IP addressの詐称を防止する**
- **RFC3704 (BCP84)**
  - Ingress Filtering for Multi-homed Networks

3.2 検証は送信元の近くで！



- 利用されないアドレスはどこでも判別できるが、利用されているアドレスの判別は送信元の近くでないと検証できない
- 無駄なトラヒックを網内に流さないためには、ネットワークの入り口で検証

3.3 送信元検証の技術

- **ACL**
  - **要はパケットフィルタ**
  - Interface**毎に個別のルールを適用する**
  - **ネットワークの変更時にはルールの変更が必要**
- **uRPF check**
  - **経路情報を基にパケットの**Source IP address**を検証**
  - **経路情報を適切に保てば、ルールは自動的に追従する**

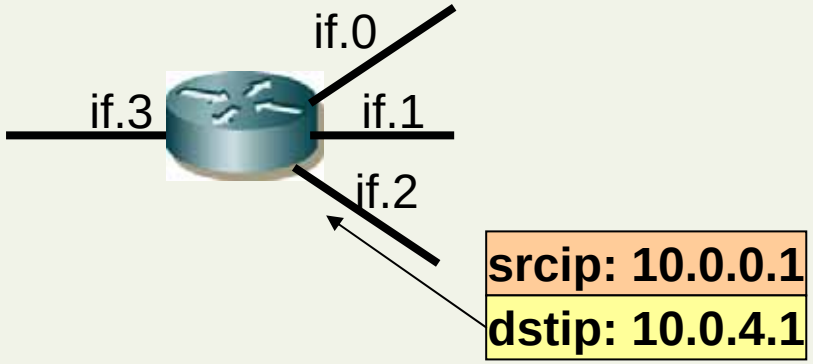
3.4 uRPF check

- **用途に応じた幾つかのモード**
  - strict mode
    - **流入interfaceが正しいか確認する**
  - loose mode
    - **経路が存在するか確認する**
  - feasible mode**は現時点では実利用に向かないので、忘れておきます・・・。**

3.5 経路の検索とuRPF

経路情報

10.0.0.0/23 via <if.0>
10.0.2.0/24 via <if.1>
10.0.3.0/24 via <if.2>
10.0.4.0/24 via <if.3>



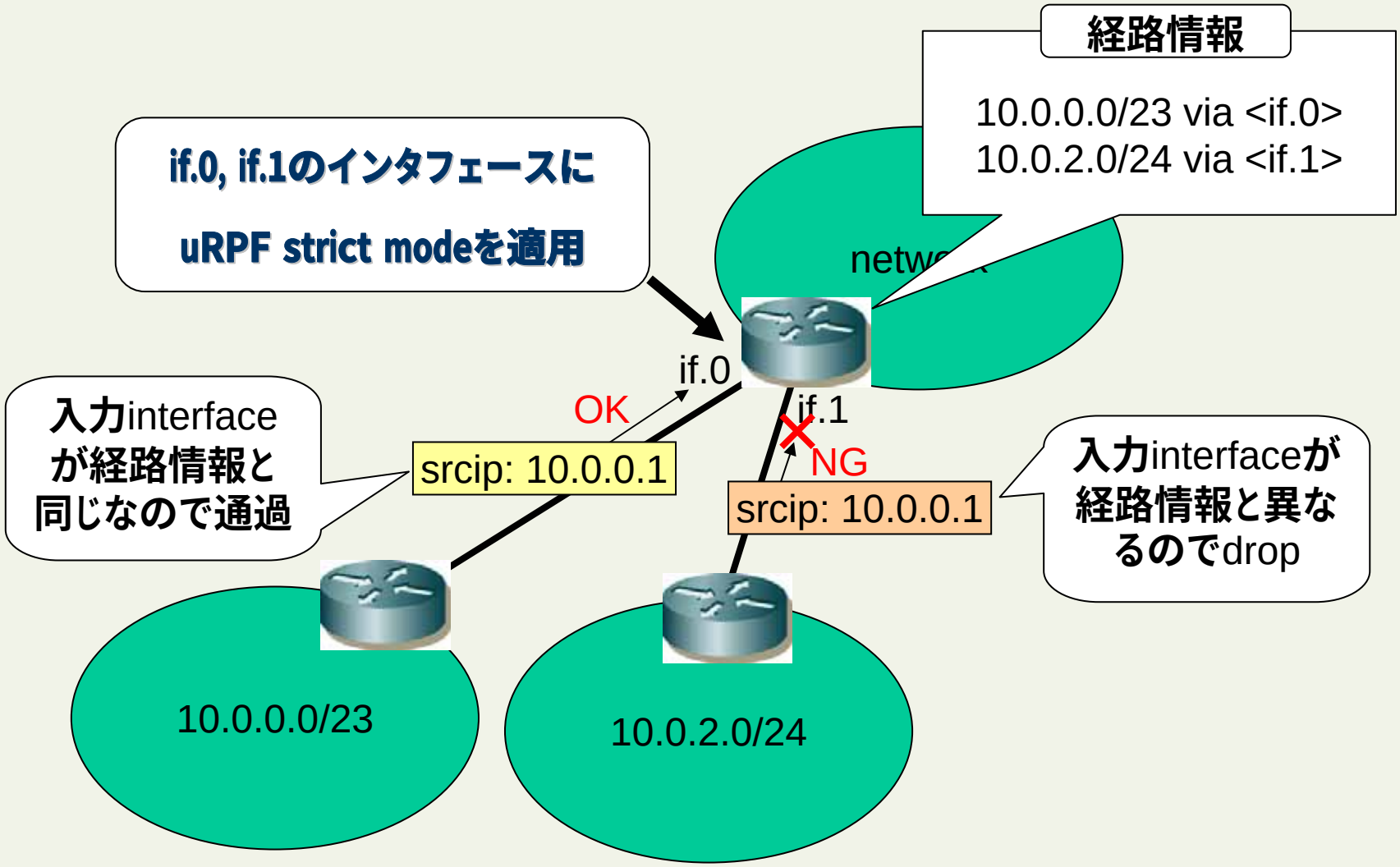
■ 通常のforwarding

1. dst-ipで経路情報を検索
2. 結果が無ければdrop
3. 転送先に従って、次の機器へパケットを転送

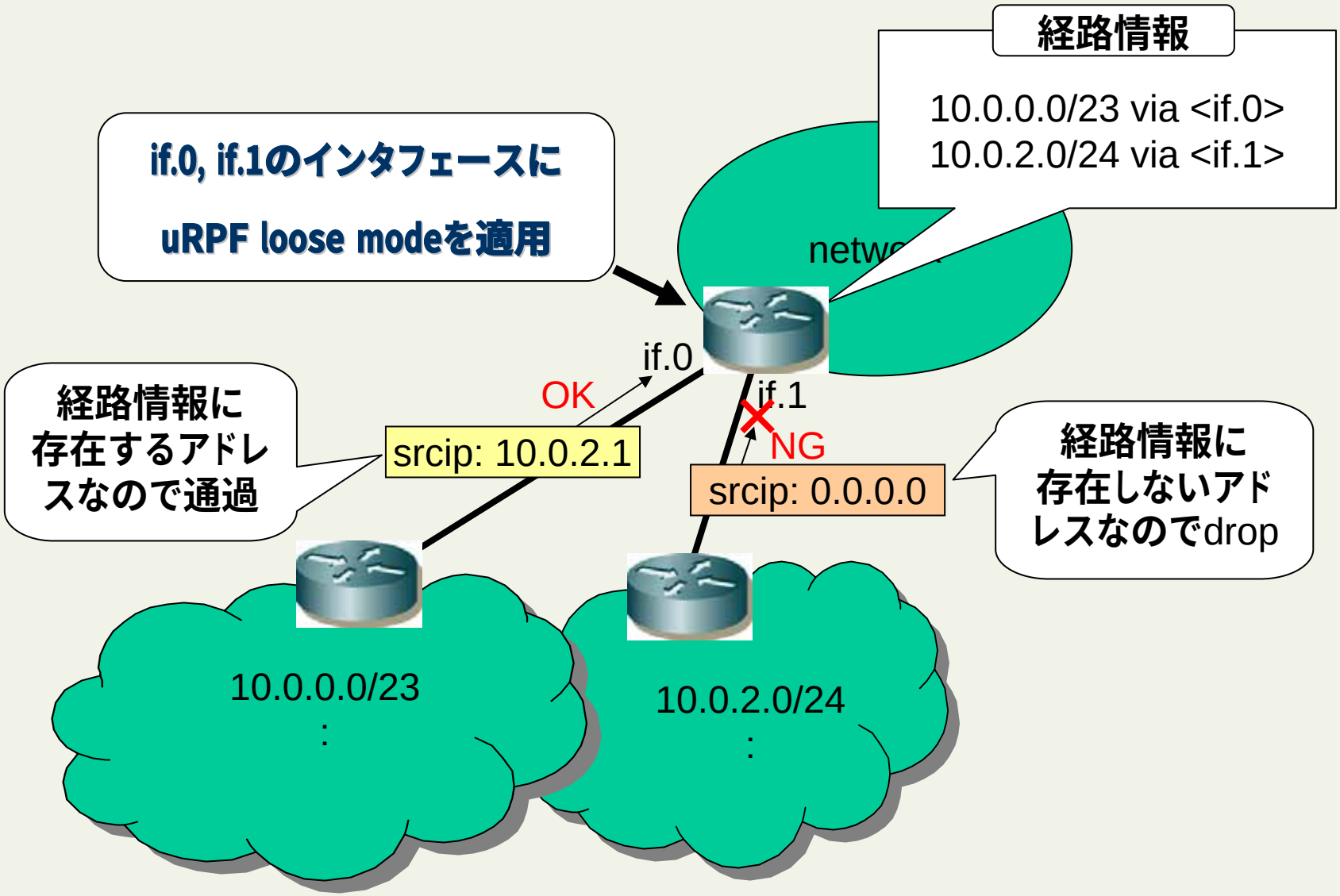
■ uRPF check

1. src-ipで経路情報を検索
2. 結果が無ければdrop (loose)
3. 入力interfaceが経路情報の転送先interfaceと違う場合はdrop(strict)
4. uRPF check OK!

3.6 uRPF strict mode



3.7 uRPF loose mode



3.8 ベンダのuRPFの実装状況

- **Cisco**
  - strict/loose modeを実装済み
  - 概ね動作するが、機種/Engine依存
  - uRPF MIB未対応
  - dropしたpacketもnetflowで見える
- **Juniper**
  - strict/feasible/loose modeを実装済み
  - 良く動作する
  - uRPF MIB対応済み
  - dropするとcflowdで見えない
- **AlaxalA**
  - 知る限りまだ実装されていない

ベンダの皆様、実装
よろしくお願いします

3.9 How to use uRPF?

例えば…

- Strictモード

  コンシューマとの接続インタフェースで設定

  – Single-homed Static顧客

- Looseモード

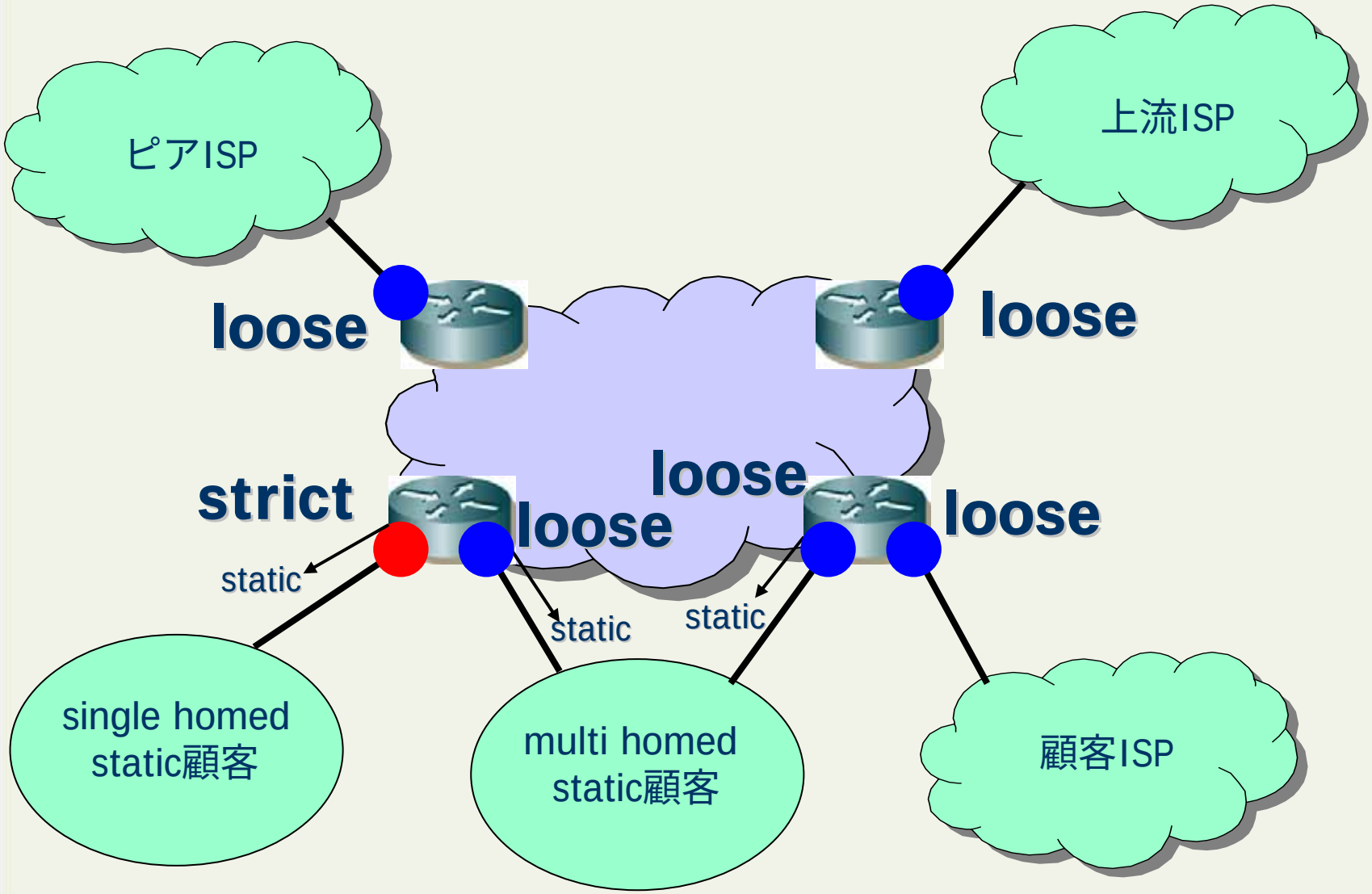
  上流ISPとの接続やPeer ISPとの接続インタフェースで設定、Transit ISPの場合、顧客ISPとの接続インタフェース

  – Multi-homed Static顧客

  – BGP顧客のデフォルト設定

  – Peer ISP

3.10 uRPF 適用事例



Let’s Join NSP-SEC-JP !!

参考URL:

- http://puck.nether.net/mailman/listinfo/nsp-security-jp
- http://puck.nether.net/mailman/listinfo/nsp-security
- http://www.cymru.com/
- http://www.arbor.net/downloads/Arbor_Worldwide_ISP_Security_Report.pdf