DDoSアワー
NSP-Security-JP
(NSP-SEC-JP)

Peers Working Together to Battle Attacks to the Internet

JANOG15 – 20 Jan 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**
- **Monitoring/Detection**
- **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>　　＃2005/1/18現在**

  ISP　　x14

  Vender　　x2

  Team Cymru　　x1

  xSPのセキュリティオペレータ募集中!!

  営業活動も頑張ります!!

- **<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
  - DDoS対応での連携

1.3 NSP-SECとの連携

- 日本のネットワークに関するセキュリティ情報のフィード
  - 日本のASN（JPNICアサインASN）に関するセキュリティインシデントを NSP-SEC-JPに転送
  - 日本のISPへの対応依頼
- 日本での存在を確認された**botnet controller** の情報転送
- セキュリティ最新トレンドの相互共有
  - 最新ウィルス情報
  - 不正トラフィック（TCP/UDPポート毎）のトレンド

1.4 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
  - –各種ウィルス毎の感染ホスト情報等
- **Document**の日本語化

http://www.cymru.com/BGP/bogon-rs.html.jis

森信さん、ご協力感謝！！

また、よろしく！！

セキュリティレポート No.1

	2004/6/18		2005/1/6	
Virus	感染AS数	日本AS感染率	感染AS数	日本AS感染率
Beagle/ Beagle3	69 ---	14% ---	48 49	9% 9%
Blaster	76	15%	30	5%
Mydoom	26	5%	6	1%
Nachi	28	5%	6	1%
Slammer	68	14%	28	5%
SPAM	130	26%	66	12%
Phabot	---	---	102	36%
scan445	---	---	22	4%

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

- **IRC botnet**コントロールサーバ
  (2005/1/13現在**)**

	コントローラ	**AS**数
世界中	**1737**	**318**
日本	**23**	**7**

1.5 セキュリティインシデント対応

- **DDoS情報の共有**
  - 日本のASNに関連するDDoS等の情報共有
  - 各ISPからの情報提供
- **日本にあるIRC botnetコントローラーの対応依頼**
- **海外ISPとの連携（アジアの窓口）**
  - NSP-SECからアジアに対する依頼の中継
  - アジアのISPの窓口としてNSP-SECとの対応

1.6 今後の活動予定

- **IMS**プロジェクトとの連携
- 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
- カンファレンス等参加
  - JANOGでupdate（今日!!）
  - NANOG BoF参加
  - APRICOTでBoFやります

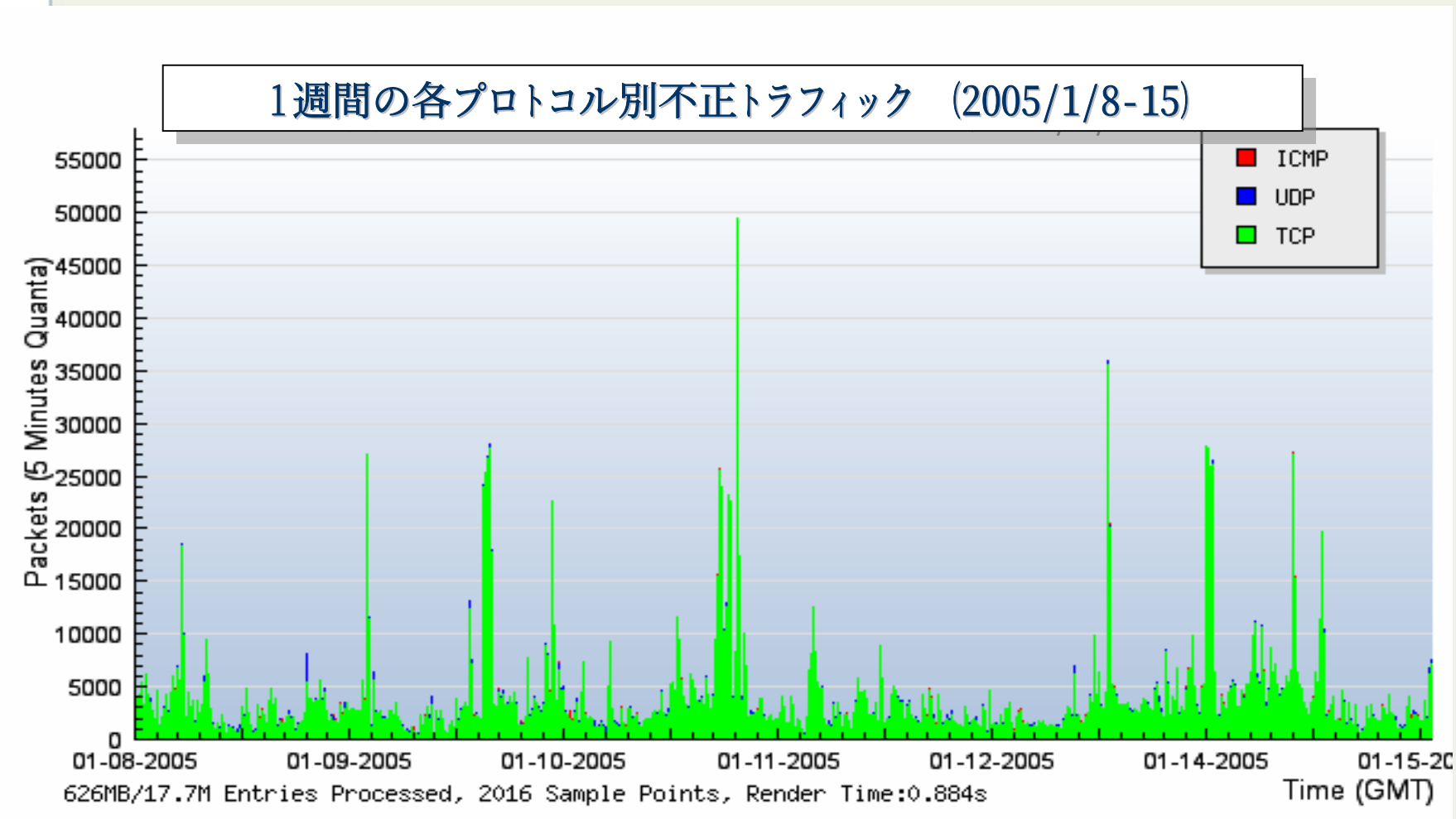
2. Security Trend

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

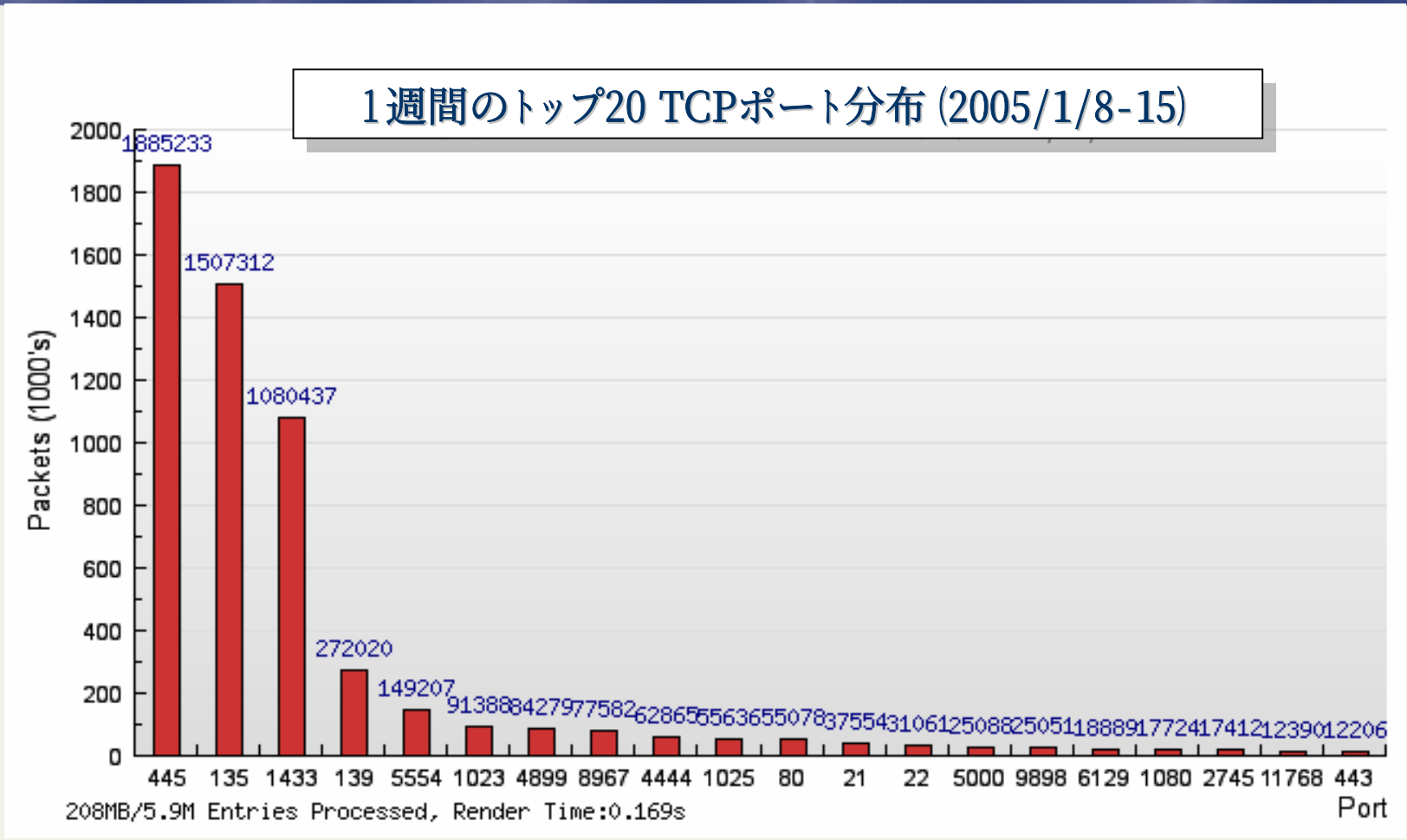
- プロトコル別
- TCPポート別
- UDPポート別

2.1.1 Protocol別



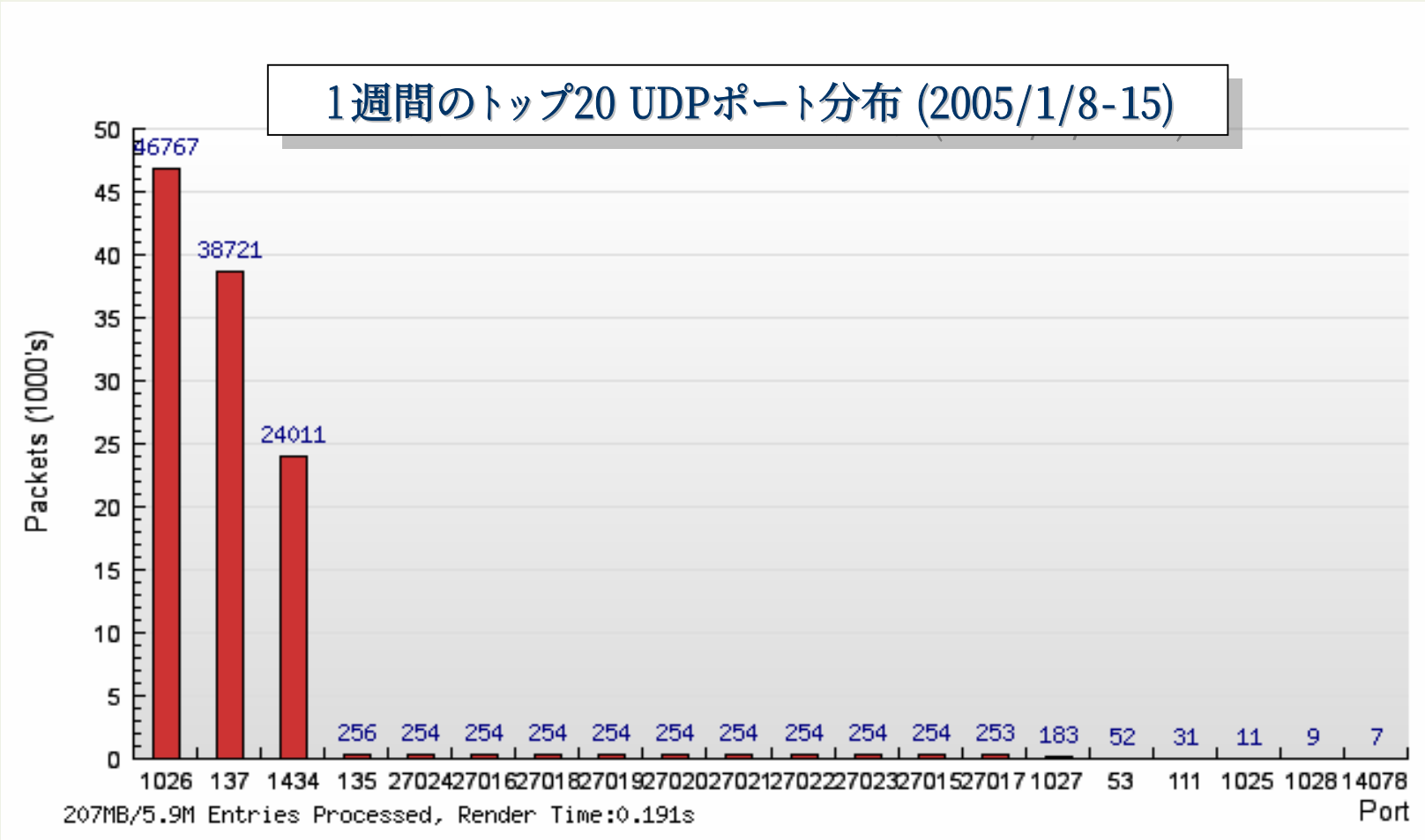
・TCPのトラフィックがほとんど

2.1.2 TCP Port別



- Port445：LSASSの脆弱性へのアクセス (Sasser等が蔓延している)
- Port135：MS RPCの脆弱性 へのアクセス (Blaster等が未だに収束していない)
- Port1433：MS SQLサーバの脆弱性へのアクセス

2.1.3 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

2.2.1 Security Trend overview

- セキュリティ犯罪の種類が変化
  - 個人犯から組織的な犯罪集団へ
  - 愉快犯からお金目的の犯罪化へ
  - 直接攻撃から間接的な攻撃へ
- 多様化するワーム･ウイルス被害
  - Witty（セキュリティツールの脆弱性を狙う）
  - フィッシングの被害が増大
  - Spywareの広がり
- **Botnet（ago/for/gt/phat/r/rx/sd/Spy/…）が拡大**
  - ゾンビPCをIRCのコマンドを利用しコントロールする新手の攻撃
  - オープンプログラムなのでカスタマイズが簡単
- その他
  - Lycos EuropeがSPAMサイトを攻撃するDDoSスクリーンセーバーを公開し、実際に中国のSPAMサイトがDownした
  - DDoS攻撃を示唆する脅迫事件

2.2.2 Security Trend

- 攻撃用コード開発スピードが加速

脆弱性	公開日	Virus/Warm	発生日	経過時間
MS02-039	2002/07/25	slammer	2003/1/24	6ヶ月
MS03-026	2003/4/27	Blaster	2003/8/11	3ヶ月半
MS04-011	2004/4/14	Sasser	2004/5/1	17日
ISS：BlackIce Real secure	2004/3/18	Witty	2004/3/20	2日

Zero day Attack

- セキュリティの連鎖活動
  1. 様々な方法でVirus/Worm感染し、トロイの木馬を仕掛けられてゾンビPC化
  2. ゾンビPCは、フィッシング被害（個人情報の搾取）、Botnetの一部になるなどの影響
  3. 踏み台にされたり、BotnetによりSPAM/DDoSのソース

2.3.1 フィッシングの変遷

- **初期のアクセス誘導**
  - IPアドレスのURLが記述された偽装サイトに誘導する幼稚なメール
  - 偽装サイトには本物のサイトに似たサイトを準備

  簡単なチェック＆対処方法：
  - URLがIPアドレスのように不審な場合はアクセスしない

- **アドレスバー偽造型**
  - HTMLメールなどでリンクとして誘導し、JavaScriptを利用してIPアドレス表示をURLで隠す
  - Windows IE6.0のJavascript表示の仕様っぽい

  例：

  ソースに 「vuln_y= window.screenTop-42;」 を挿入

  上記は、表示ページの上部のマイナス方向（-42）に文字列画面を挿入。

  これによりアドレスバーのアドレス表示「http://10.10.10.1」を上書き表示

  簡単なチェック＆対処方法：
  - IE以外のブラウザを利用する
  - HTMLメールは使わない（気をつける）
  - ツールバーをカスタマイズしておく等々

2.3.2 フィッシングの変遷

- トロイの木馬スタイプ　其の一
  - Windowsの脆弱性をついて、Hostファイルを書き換えてフィッシング用サイトに導く
  - URLは正規のURLのためメールを見ただけでは判断しにくい

  例:
  - 変更されたhostsファイルの中身

    10.10.20.1　　www.yahoo.co.jp

    10.10.30.1　　www.btm.co.jp

  チェック＆対処方法:
  - Windowsの脆弱性をWindows update等で対処する
  - ファイル･システム監視ツール等（Hostsファイルを監視）の導入
  - サイトによってはSSLの証明書の確認

- トロイの木馬スタイプ　其の二
  - Windowsの脆弱性をついてトロイの木馬を埋め込む
  - 自然に対象サイトにアクセスするとそれをトリガにキーロガーが作動＆画面のスナップショットを保存！！

  チェック＆対処方法:
  - Windowsの脆弱性をWindows update等で対処する

2.3.3 フィッシングの被害

- 国内の被害
  - JCB
    - 2004/5-6
    - カード番号を問い合わせる幼稚なもの
    - 9件の申告
  - Yahoo! Japan
    - 2004/11/14以降
    - Yahoo! JAPAN IDやパスワードおよびクレジット番号、有効期限を不正に収集
    - JavaScriptを利用してIDをWebに埋め込む巧妙なタイプ
    - 千数百人がメールを受信
    - http://docs.yahoo.co.jp/info/notice21.html
  - VISA Japan
    - 2004/11/8以降
    - VISAのクレジット番号、有効期限を不正に収集
    - Webメールの中のURLのリンク先が不正なサイト（ルーマニアのサイト）
    - JavaScriptを使いIEのURLバーを上書きする
    - 約150人がメールを受信
    - http://www.visa.co.jp/newsroom/NR_jp_111104.shtml

2.4.1 Botnetとは？

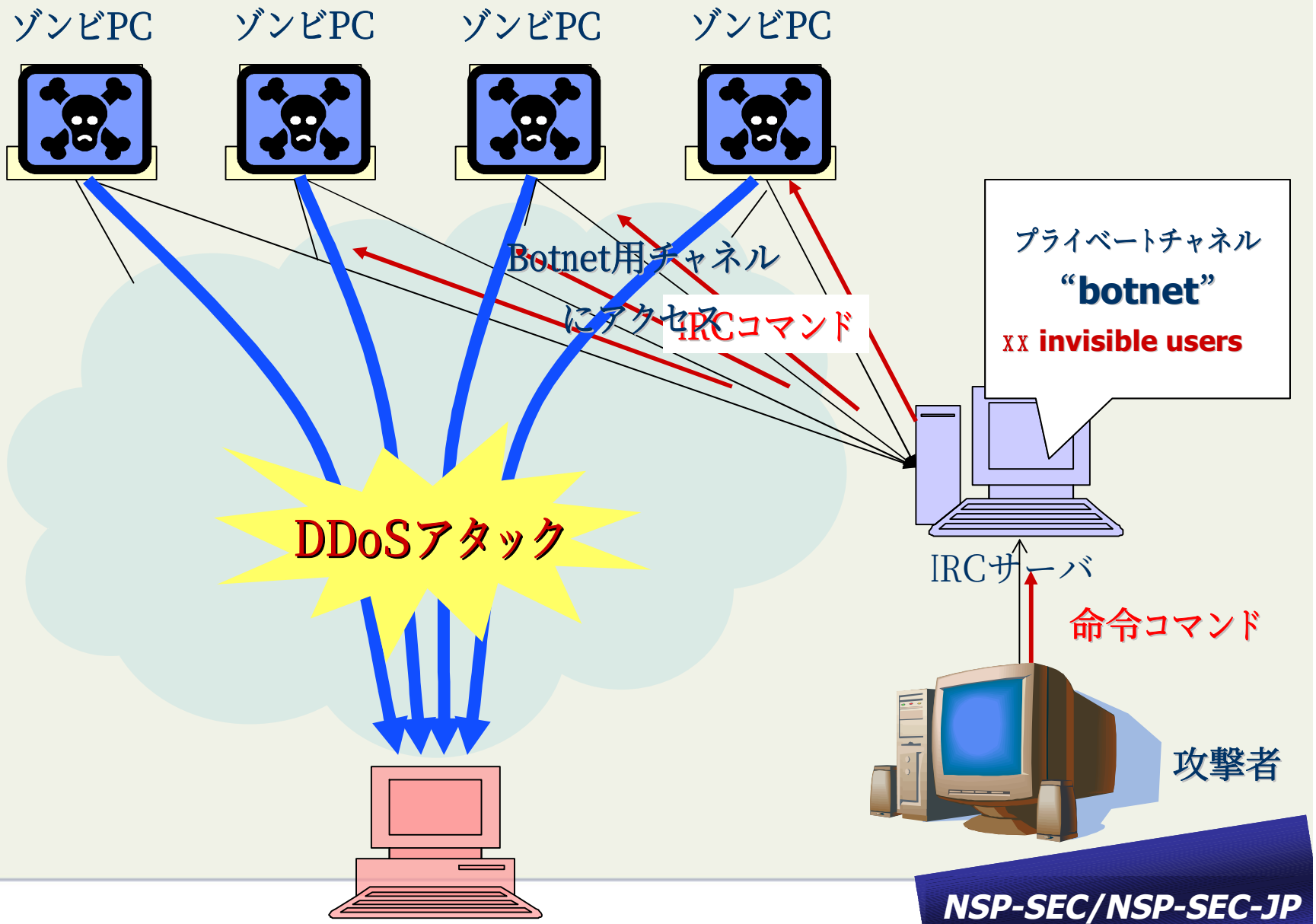
- 由来

  Botの語源は、「Robot」。IRC等からの命令に従って動作するPCをbotといい、そのようなPCの集まったネットワークを”botnet”, “bot network”という

- **Botnetの動作**
  - PCに不正に侵入
    - セキュリティホールをついたWorm等による侵入
    - パスワードの不備、弱いパスワードをつく
  - 不正なプログラム（トロイの木馬）を仕掛ける（ゾンビPC化）
  - マシン内の設定ファイルやパスワード･ファイル，ユーザーのキー入力などを記録して攻撃者に送信
  - ゾンビPCはIRCサーバの特定のChannelに接続する
  - アタッカーはIRCのbotnet用チャネルにコマンドを送信
  - ゾンビPCはそのコマンドによってコントロールされ忠実に実行する

    DoS攻撃、ファイル送信等10～100種のコマンド

2.4.2 Botnetの構成（DDoSアタックの場合）



2.4.3 Botnet攻撃手法

アタッカーから以下のDoS攻撃を可能

–SYN Flood

TCP3ウェイハンドシェイクを利用し、アドレスを偽ったSYNパケットを大量送りつける攻撃。ターゲットは3ウェイハンドシェイクを確立するために、SYN-ACKを返して、ACKを待つが正常なアドレスではないためACKが帰らず待ち状態のままとなる。このようなパケットを大量に送ると、ACK待ちの状態が大量に発生し、正常なアクセスを妨げる。

–ICMP Flood

大量のICMPパケット（サイズの大きいパケット：65536）をターゲットに送りつける。大量のトラフィックを発生させリンクの輻輳・またターゲットのリソース消費を引き起こす

–UDP Flood

コネクションレスである、UDPを利用し、大量の連続したUDPパケットやパケットサイズの大きいUDPパケットを送りつけ、ターゲットのリソースを浪費させる

–HTTP Flood

TCP80番ポートに対して大量のパケットを送りつけ、リソースを浪費するコネクションFlood

–LEET攻撃（Land攻撃に似ている）

ソースとデスティネーションに同じターゲットアドレスをセットして、SYNパケットを送り、その受け取ったターゲットが自分にACKを返し、ACKストームになり、CPUを浪費させシステムダウンを引き起こす

–TARGA3攻撃

IPスタックの脆弱性を狙う攻撃。異常なIPパケット（フラグメント、プロトコル、パケットサイズ）を送りつけ、ターゲットをクラッシュさせる

2.4.4 Botnetの特徴

- (ago/for/gt/phat/r/rx/sd/Spy/...) botなど様々
  オープンソースプログラム (ソースもツールも公開) のため
  - 2003年4月にオリジナルが確認、現在では数十分に1つの亜種が発生
    2005/1月
    spybot　　約**6000**
    Randex　　約**2200**
    gaobot　　約**2000**
  - ウィルス検出が追いついていない
  - カスタマイズが簡単
    controlコマンドのカスタマイズで特定の企業を攻撃
- アタッカーのトレースが難しい
  - Packetのソースは多数のゾンビPC
  - Filterが難しい
  - アタックの判断が難しい

2.5.1 中国からのDDoSアタック

- 期間

  2004/8/1-9

- 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

  ~100Mbps程度のアタックが観測

  中国の掲示板で煽動された中国系の人々がアタックに参加

  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

2.5.2 日本から海外への不正アクセス

- **SPAM発信**

ソース：sophos
http://www.sophos.com/spaminfo/articles/dirtydozenyear.html

	国	*割合*
1	**United States**	**42.11%**
2	**South Korea**	**13.43%**
3	**China (incl Hong Kong)**	**8.44%**
4	**Canada**	**5.71%**
5	**Brazil**	**3.34%**
6	***Japan***	***2.57%***
7	**France**	**1.37%**
8	**Spain**	**1.18%**
9	**United Kingdom**	**1.13%**
10	**Germany**	**1.03%**
	Others	**19.69%**

2.5.2 日本から海外への不正アクセス

- フィッシングサイトのホスティング

順位	国	割合
1	**United States**	**27%**
2	**China/HK/Taiwan**	**21%**
3	**South Korea**	**10%**
4	***Japan***	***5.5%***

ソース：APWG

http://www.antiphishing.org/APWG%20Phishing%20Activity%20Report%20-%20November%202004.pdf

- **Broadband顧客からのアタック**
  - 日本はブロードバンド普及率、帯域速度は世界最高レベル
  - アタックソースとしても世界最高レベル（100Mクラスのアタック可能）

2.5.3 今後予想されるアタック

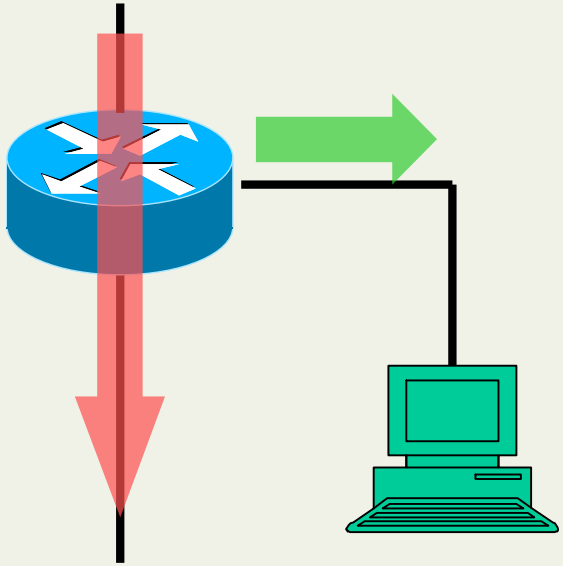
- **Grid-directed DDoS**
  - グリッドコンピューティング技術を応用したDoS/DDoS攻撃。BotnetやLycos EuropeのDDoS screen-serverは、まさにGridコンピューティング技術を利用したアタックと言える。
- **“Warhol” Worm**
  - カリフォルニア大学バークレイ校(UC Barkley/University of California at Barkley)のNicholas Weaver 教授が論文を発表

    「将来、誰でも15分間で有名になれる(In the future, everybody will have 15 minutes of fame)」を文字って「15分間でインターネット世界を征する（Warhol Worms: The Potential for Very Fast Internet Plagues)
- **Flash threats**
  - 一瞬にして世界中に感染するだとうウィルス・ワームを想定したアタック
- **IDS-directed attack**
  - IDSを狙ったアタック。StickというIDSの耐性を見るtoolを使ったアタック
- **VoIP attacks**
  - VoIPシステム系インフラ（SIPサーバ）に対する攻撃。SIPトラフィックに遅延やジッターを与えることによる音声通信のサービス障害を引き起こす。
- **Intranet attacks**
  - Intranetに対する攻撃。トロイの木馬感染PCの持ち込みなどにより、そのPCからIntranetに蔓延してIntranetのシステムを麻痺させる。

3. Monitoring/Detection

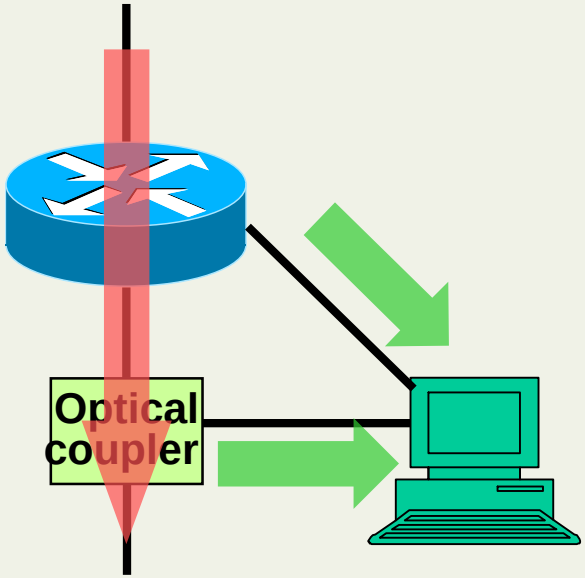
3.1 トラフィックモニタリング

Flow collector



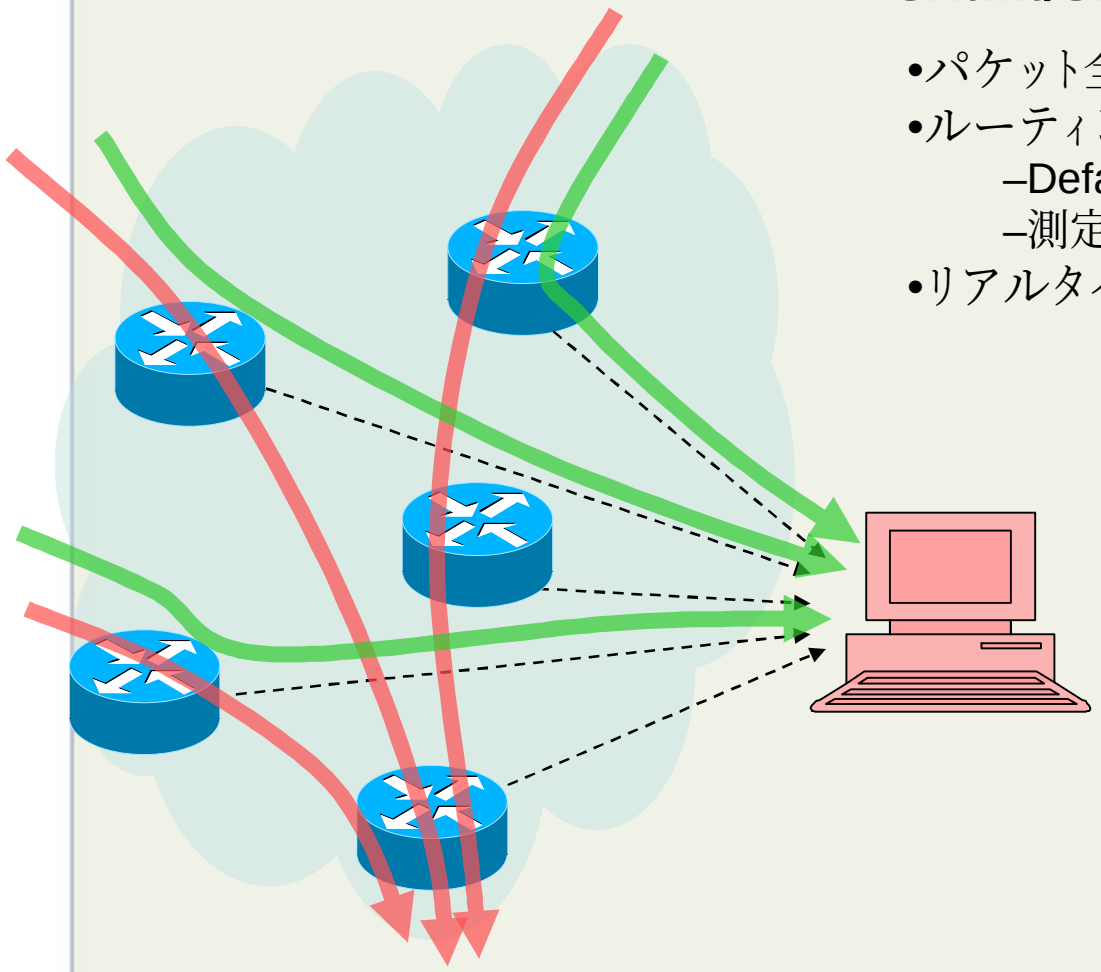
- 全てのPacketは測定が難しい (CPUパワー次第)
- L2-L4ヘッダ情報を収集する
- ルータのCPU負荷が高い (ASIC処理だと別)
- ネットワーク内に特別な機器は不要
- (Cisco Netflowは厳密にはリアルタイムでの収集ではない)

Tapping/Port mirroring



- すべてのPacket (1/1) を収集可能
- パケット全体を収集する
- 物理的に分岐する
- ネットワーク機器のCPUの心配はない
- Optical couplerの場合、リンク毎に必要
- リアルタイムで収集できる

3.1 トラフィックモニタリング (続き)



Shunt/Sink hole routing

- パケット全体を収集
- ルーティングでパケットを収集する
  - –DefaultやBogonなどをルーティング
  - –測定したいDstのPacketをルーティング
- リアルタイムにパケット収集

3.2 モニタリングの比較

項目	Netflow/cflow collector	Inline-Tapping/ Port mirroring	Shunt/ Sink Hole routing
導入	容易（設定のみ）	専用の機器（Inline）	容易（ルーティング）
拡張性	高い	低い（リンク毎に必要）	高い
正確性	低い（Sampling rate次第）	高い	高い
トラフィック制限	あり（Samplingで制御）	なし（インタフェース速度）	一部のトラフィックのみ
設置箇所	エッジルータ ネットワーク全体	対象のリンク	ネットワークのどこか
収集対象	なんでもOK	リンクのトラフィック	一部のネットワーク
その他	Vender毎にFlow exportの仕様が違う	10G等高速インタフェース未対応	ツールが充実 Honey Potプロジェクト

3.3 トラフィックモニタリングの利用区別

- **Flow collector**
  - ネットワーク全体のトラフィックデータを収集
  - エッジルータでピア・顧客トラフィックデータの収集

  例：各種フローコレクタ（cflowdなど）
- **Tapping/Port mirroring**
  - 顧客との境界でトラフィックデータを収集
  - DMZサーバの手前など

  例：NIDS
- **Sink Hole/Shunt**
  - 一部のネットワーク情報のみ収集
  - 不正なトラフィックデータの収集（誤検知が少ない）

  例：Honey Potプロジェクト、IMSプロジェクト、Cymru Darknetプロジェクト、
  各ISP独自

3.4 不正トラフィック検知手法

ネットワークベースの検知

- パターン検知（シグネチャベース）;
  - 不正なパケットのペイロードにあるパターンをチェックする。
  - 各種シグネチャー（Blaster、Slammer、Nimda、CodeRed等）と比較し判別

    Blaster　　da4874932f7fcaba5277bbcdf2b5e6b0

    Slammer　　a0aa4a74b70cbca5a03960df1a3dc878

    #パケットペイロードのMD5のチェックサムより作成
  - 常時、最新のシグネチャーにUpdateする必要がある

- トラフィック検知 (統計ベース);
  - トラフィックプロファイル作成 (IPアドレス, プロトコル, トラフィック量, user login)
  - ベースのトラフィック量の上下閾値設定と比較し判別
  - 正常な通信を利用したDDoSアタック（トラフィック量のみ増加）に対処
  - ゼロデイ（Zero-day）アタックに対応化

3.5 DoS/DDoS検知の問題点

誤検知

- **False Positive**
  - 正常なPacketを不正なPacketと判断すること
- **False Negative**
  - 不正なPacketを正常なPacketと判断すること

解析稼動（運用コスト）過多

- ログの量が多いとチェック不可能
- リアルタイム検知のためには常時監視が必要

4. DoS/DDoSの対処方法

4.1 ネットワークセキュリティ関連用語

- **Backscatter**

  Spoofingされたアタックに対して、ターゲットが応答するパケットのこと。

  本来の通信では発生しない。

  応用例:

  – Backscatter traceback

- **Shunt**

  Staticやspecific経路の広告によるlongest-matchによってパケットを別のdestinationに導く

- **Black hole (shunt) routing**

  Shunt等を使ってパケットをアタックのターゲットまで到達させずに破棄すること

  応用例:

  – RTBF(Remote Triggered Black hole Filtering)、Black hole community

- **Sink hole**

  Shunt等により、パケットを解析・対処するために導きいれ、解析・Filteringを行う

- **Scrubbing**

  Filtering box等において正常なパケット以外の不要なパケットのみFilteringを行う

4.2 セキュリティ対策技術

- トレースバック手法
  - トラフィックの目視確認
  - 直感頼り！！
  - Traceroute
  - Logging on the router
  - Backscatter traceback technique
- 対処
  - Filtering
  - Blackhole and Discard routing
  - Sinkhole and scrubbing

4.3 トラフィックフロートレースバック

アタックには、**spoofing/non spoofing**の2種類のタイプがあり、アタックソースをトレースバックしないといけない

- **traceroute**はまず試しに
- ソースアドレス･トラフィックパターンから(直感)
  - Private、bogonアドレス、ありえないCIDR
- **MRTG**のトラフィック量の目視確認

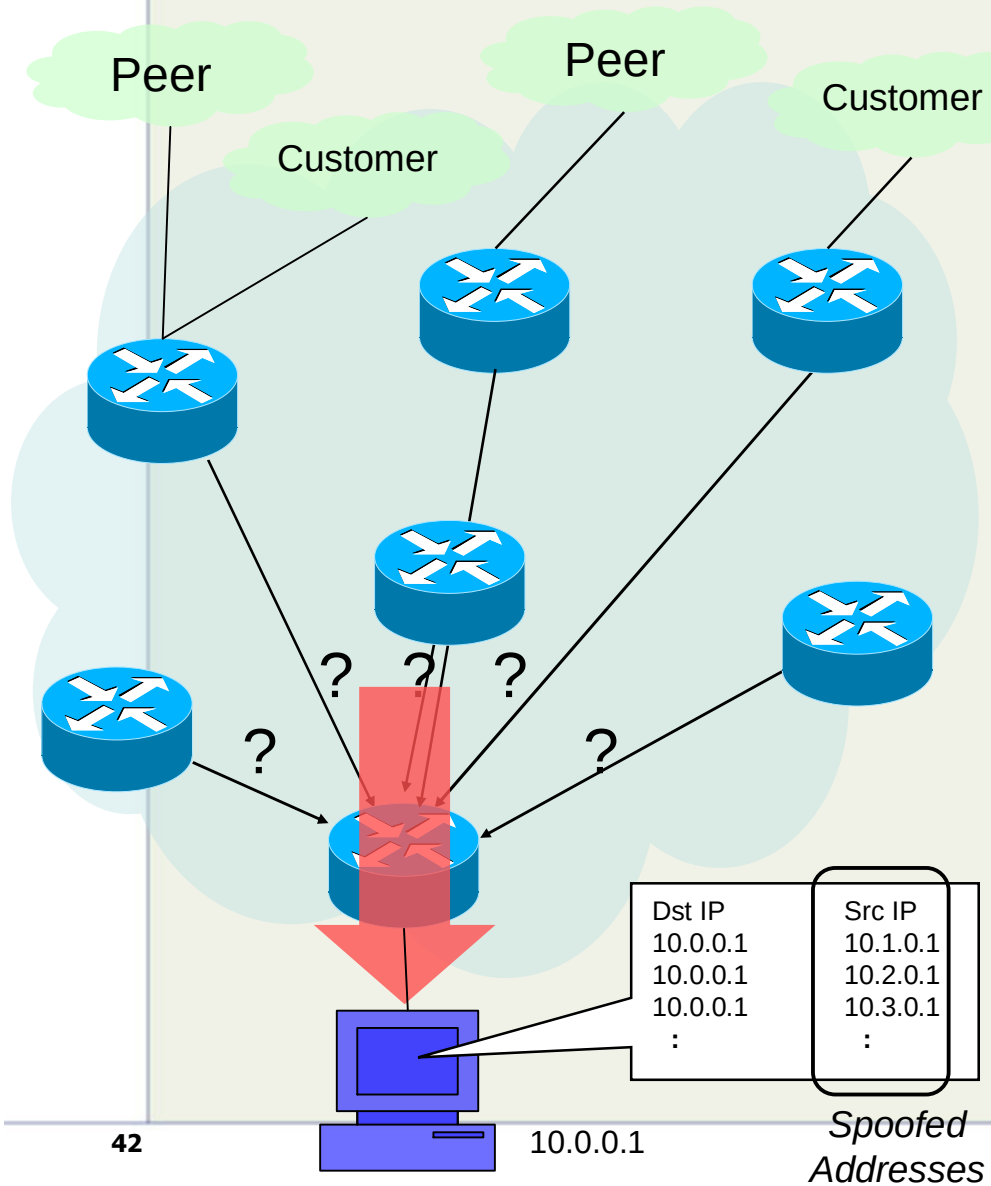
  実際のルーティングと異なるインタフェースのトラフィックが上昇
- **netflow data**による解析

  netflowデータによる本当のIncoming Interfaceの確認
- **Edge**で確認

  Traceroute結果より、edgeルータで上記確認を実施

問題なのはspoofed address!!

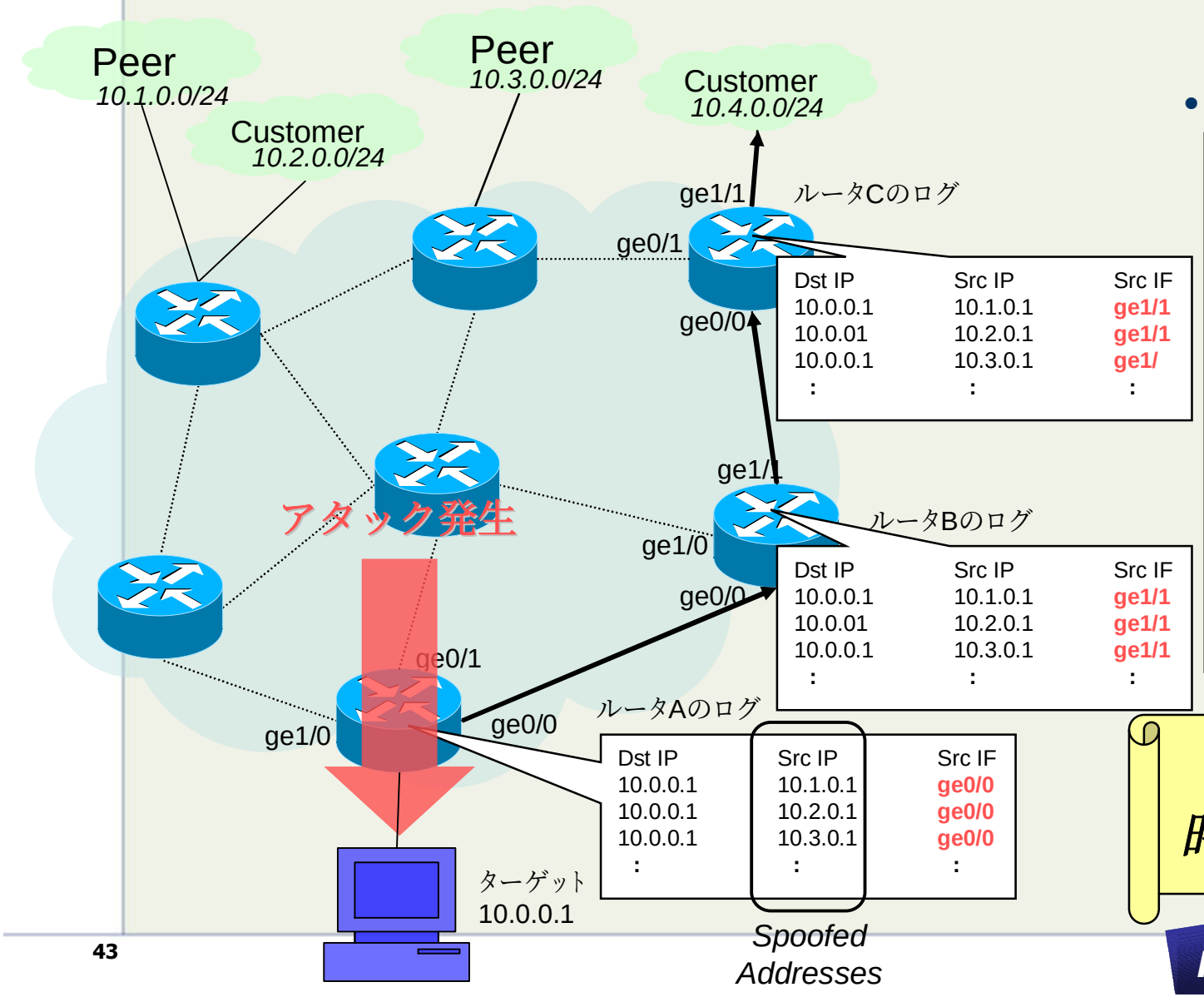
4.3.1 spoofed アドレスのトレースバック



- トレースバックにおける問題
  - SourceアドレスがIP spoofingの場合
  - 顧客申告が曖昧な場合が多い
    - ターゲットアドレス／ポート番号
    - アタックのタイプ
  - 迅速な対応が必要
    - 30分以内の対応が必要
    - 申告時にアタックが一旦収束している場合もある
  - 高いセキュリティ対応技術
    - トレースバックの方法
    - セキュリティタイプの判別

- トレースバック手法
  - ログによるHop-by-Hop
  - Backscatter traceback

4.3.2 ロギングによるトレースバック



トレース開始

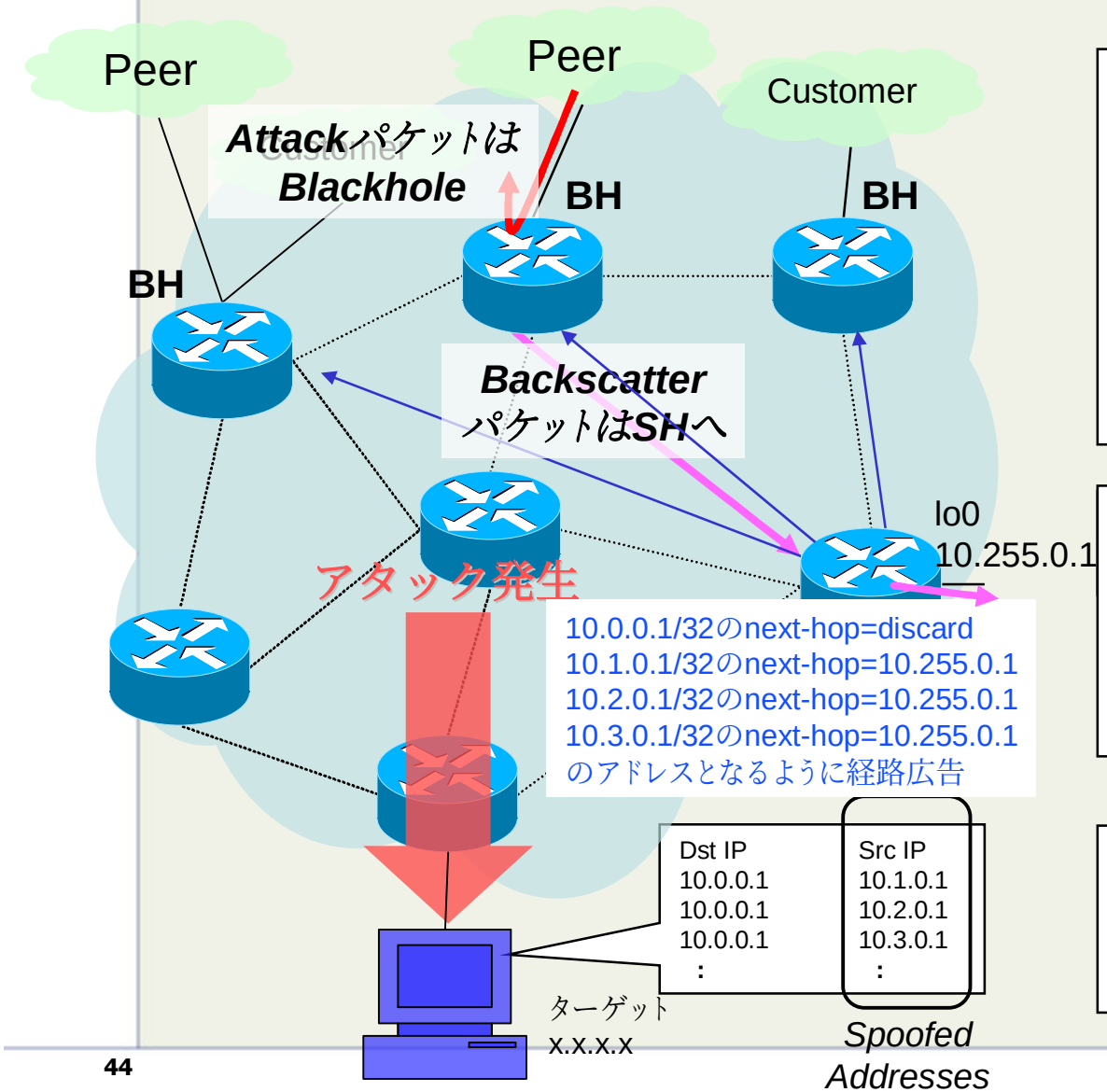
- *ルータでロギング開始*

被害の近いルータからログを解析してHop-by-Hopでトレースしていく。

ルータA
↓
ルータB
↓
ルータC
↓
オリジン

一台一台では時間が掛かる…

4.3.3 Backscatter traceback technique



SH-RTルータを設置（loopback0利用）
全ての境界ルータに以下の経路情報
を広告

route	next-hop
10.0.0.1	discard
10.1.0.1/32	10.255.0.1
10.2.0.1/32	10.255.0.1
10.3.0.1/32	10.255.0.1

境界ルータでの動作
・Attack PacketはBHされる。
・ICMP unreachableはSinkHoleルータへ送られる。
・ICMP unreachableは境界ルータのアドレスを持つ

SinkHoleルータでの動作
・lo0に入ってくるパケットをlogging
--->*入り口のルータのアドレスが現れる*

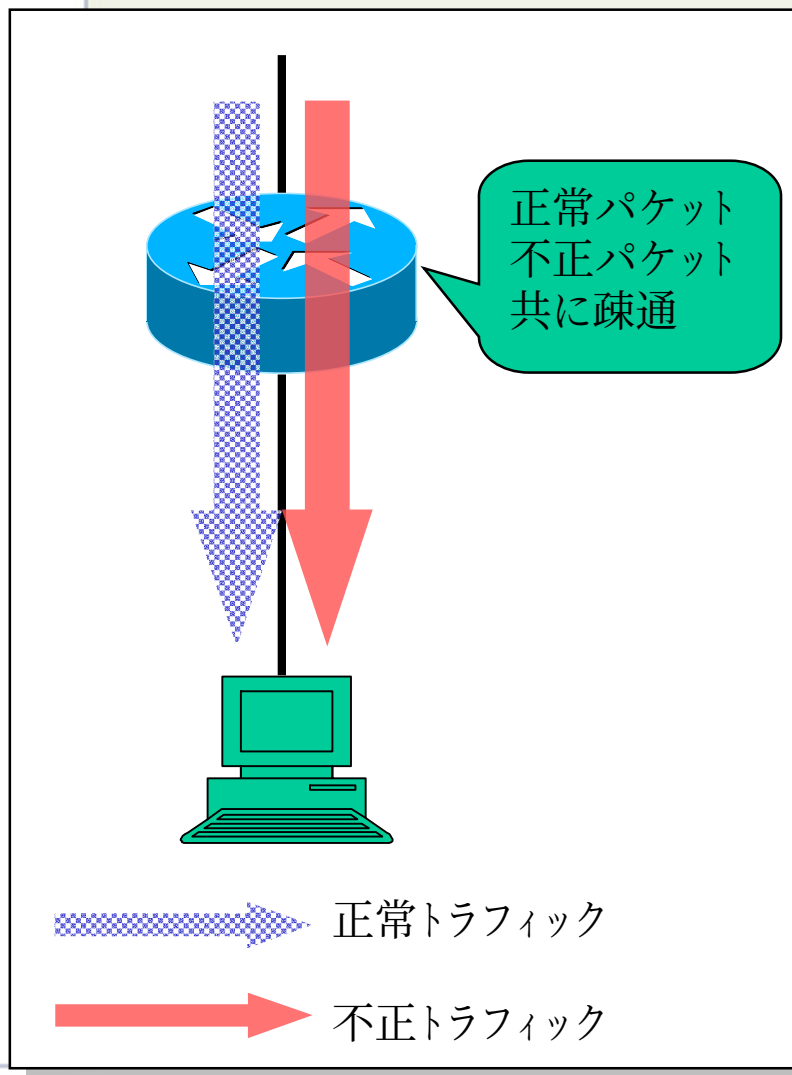
4.4 アタックの対処（DoS/DDoS対処技術）

- 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
- sinkhole+scrubbing

#今回は時間の関係で、上記3つについてのみ説明する

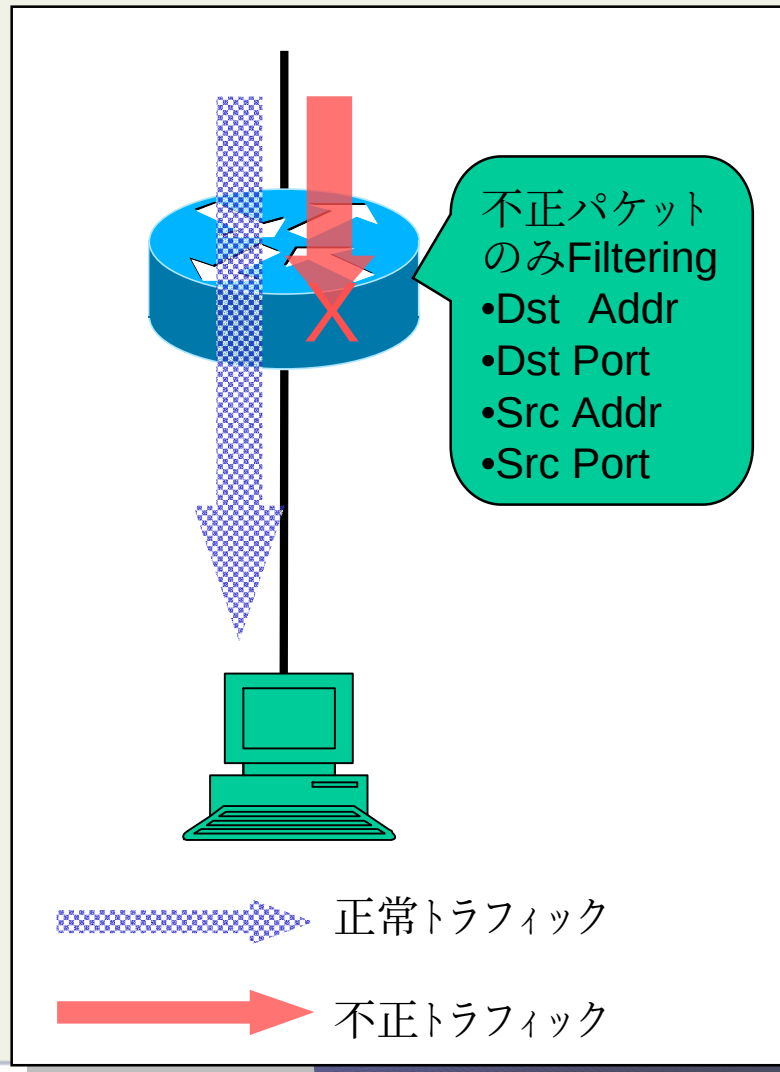
4.4.1 パケットフィルタリング

使用前

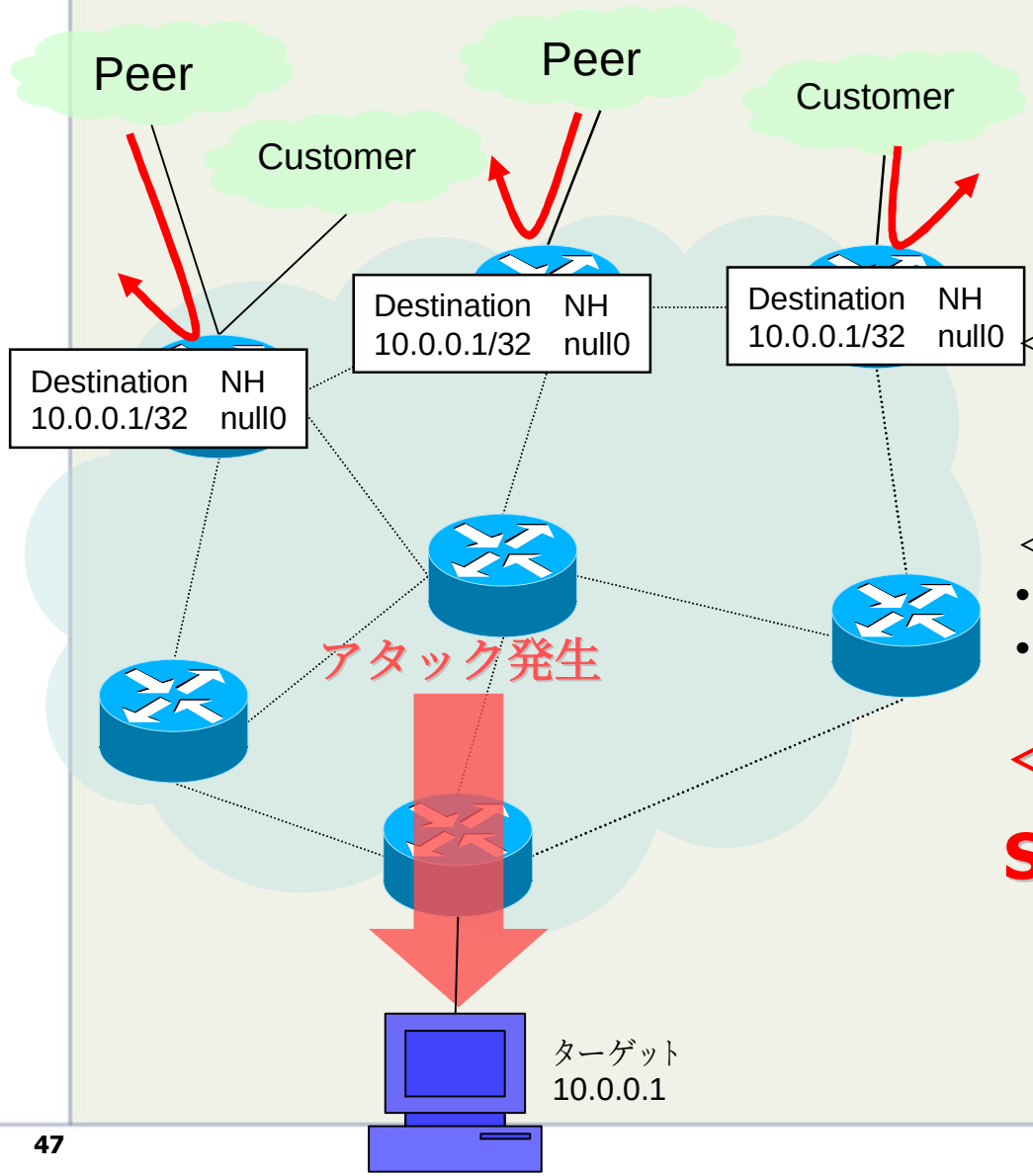


Filter

使用後



4.4.2 Black hole/Discard routing by static



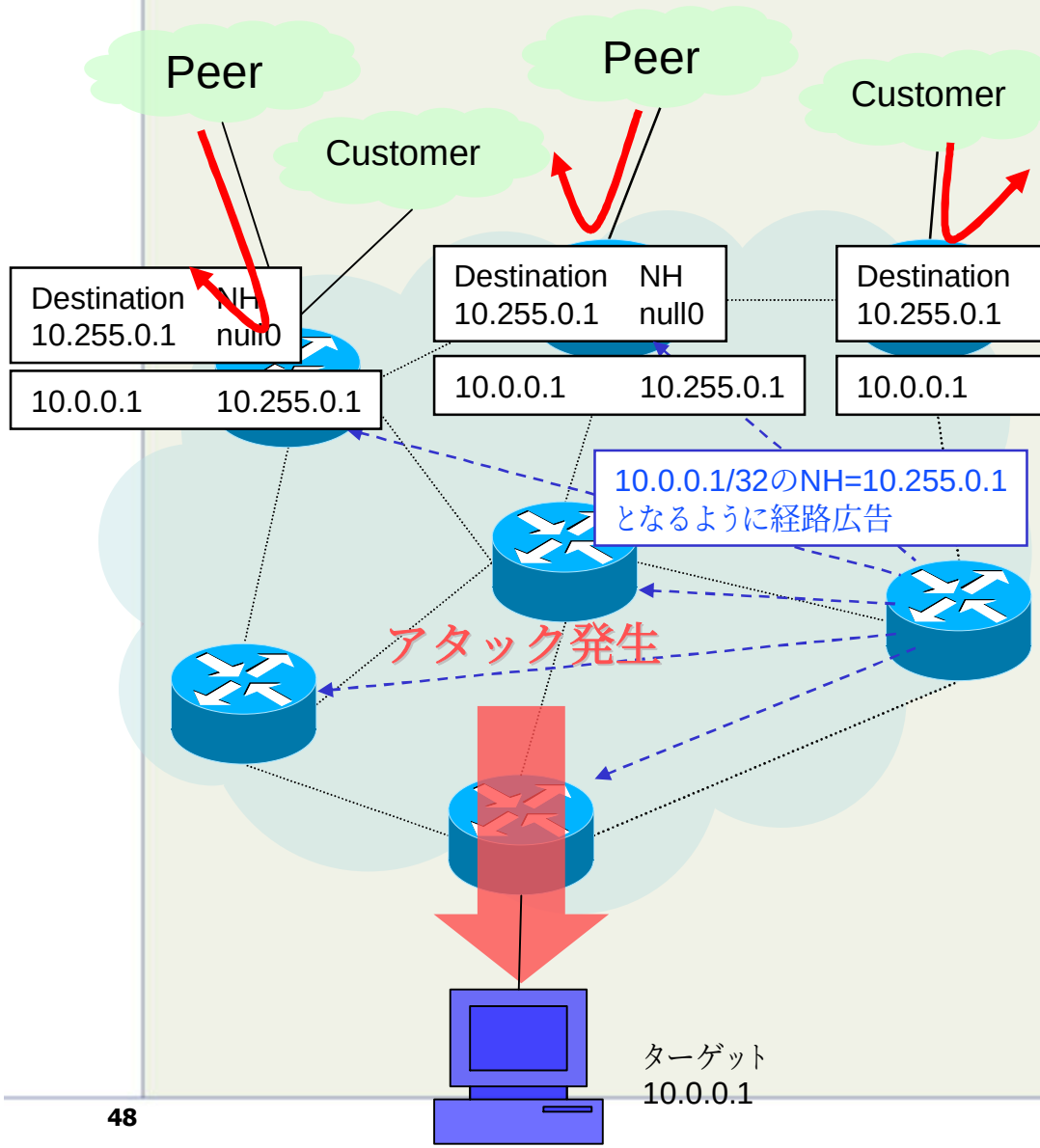
＜設定＞
境界ルータでvictumのアドレスに対して
null0にルーティングするように設定する

＜効果＞
- 境界ルータでAttackパケットを破棄
- ネットワーク資源を守る

＜問題点＞

Static routingである
- ー管理が大変
- ースケールしない

4.4.3 RTBF (Remote triggered Black hole Filtering)



＜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

4.5 Botnet対策

＜問題点＞

- **Botnetを利用したDDoS/DoSアタック対処が難しい**
  - 実際のソースはゾンビPC(加害者というより被害者)
  - ゾンビPCは数が多くFilteringするソースアドレス数も半端じゃない…
  - ゾンビPCからの通信はTCP SYN floodとは異なる通常の通信（スリーウェイハンドシェイク）
  - 本当のアタッカーはIRCサーバにコントロールコマンドを送るのみ
- **実パケットのソースアドレスは量も多く、実行上Filteringは難しい**
- **Botnet自体がL2トンネリング（/w IP-SEC）等で構築されている場合、コントロールパケットの検知が困難である**

＜解決策＞

- **ゾンビPCにならない**
  - Windows Update等のパッチをタイムリーに利用する
  - 各個人がセキュリティの脆弱性の意識を高める
- **アタッカの通信を止める**
  - アタッカを突き止めるのは難しい
- **IRCサーバからの通信（ゾンビPCのコントロール）を止める**
  - IRCサーバをblackholeする

4.6 セキュリティの今後

“アタッカーの技術は日々進歩している”

将来予想されるアタック:

- Grid-directed DDoS
- “Warhol” Worm/attacks
- Flash threats
- IDS-directed attack
- VoIP attacks
- Intranet attacks

- 対応するにはセキュリティのスキルが必要
- 各ISP、データセンタでの個別対応には限界

Let's Join NSP-SEC-JP !!

参考URL:

- http://puck.nether.net/mailman/listinfo/nsp-security-jp
- http://www.cymru.com/
- http://www.giac.org/practical/GSEC/Ramneek_Puri_GSEC.pdf
- http://www.cyberpolice.go.jp/detect/pdf/report_gaobot.pdf