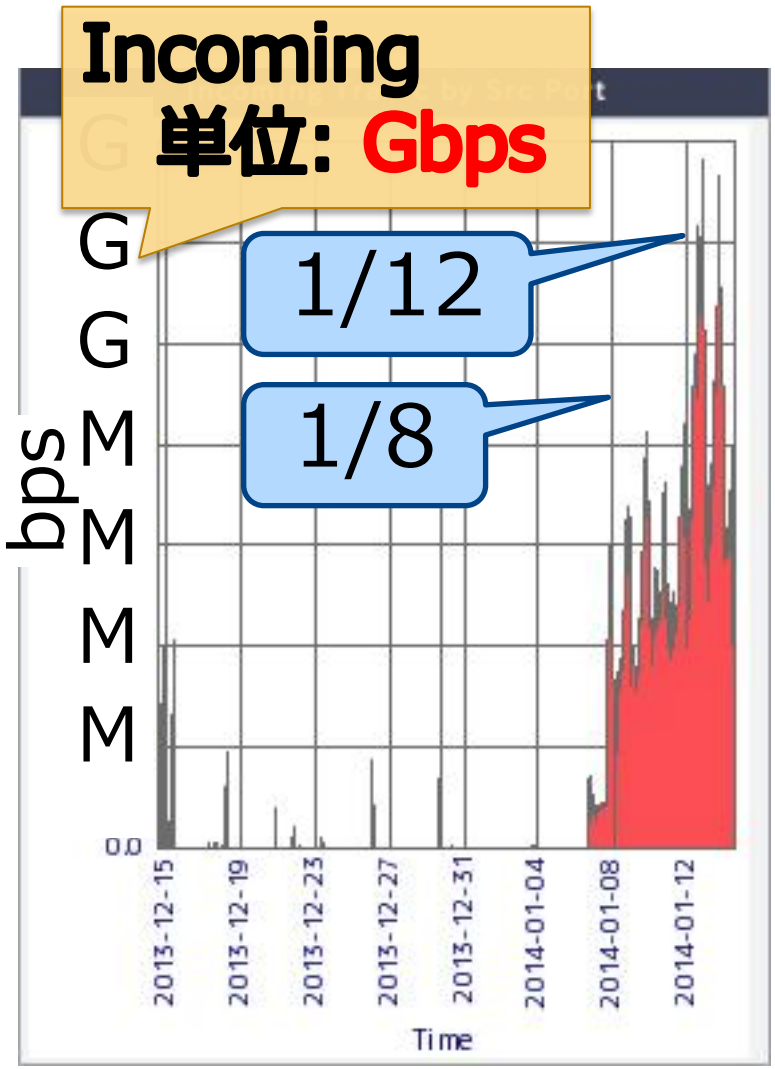
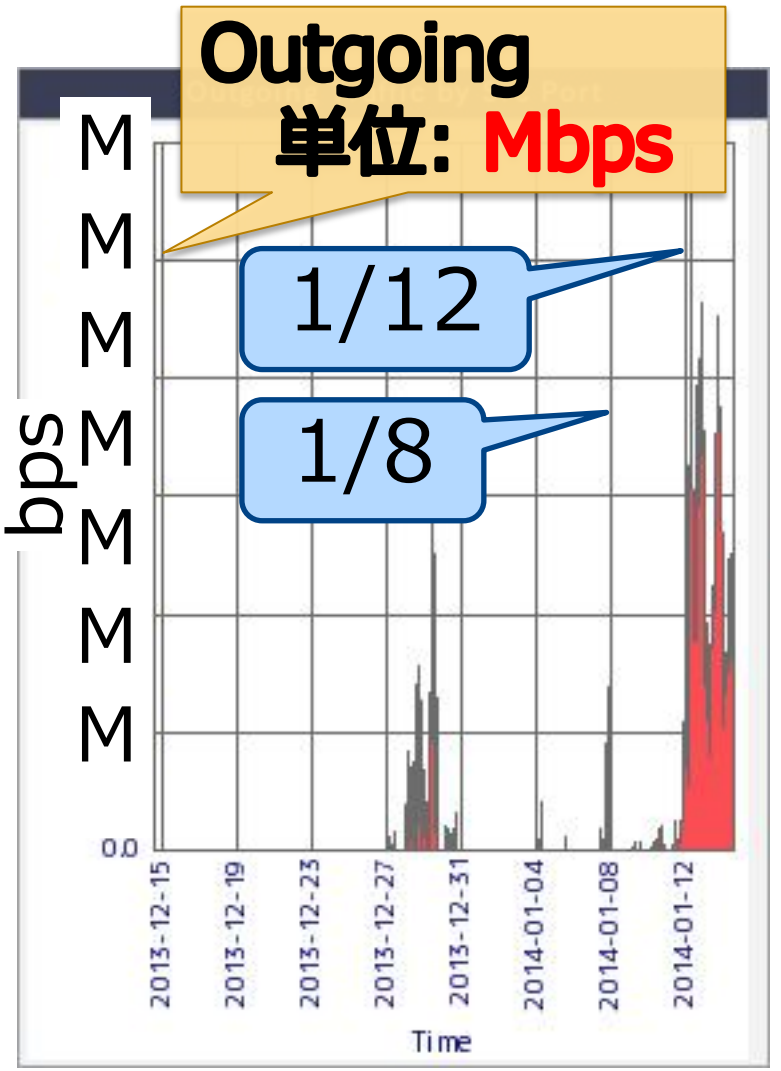
NTP reflection attackと NTPのトラフィック傾向

JANOG33@別府
DAY2 2014/1/24 (金) 13:20-13:40 Lightning Talk

NTTコミュニケーションズ株式会社
先端IPアーキテクチャセンタ 高田美紀

UDP/123トラフィック





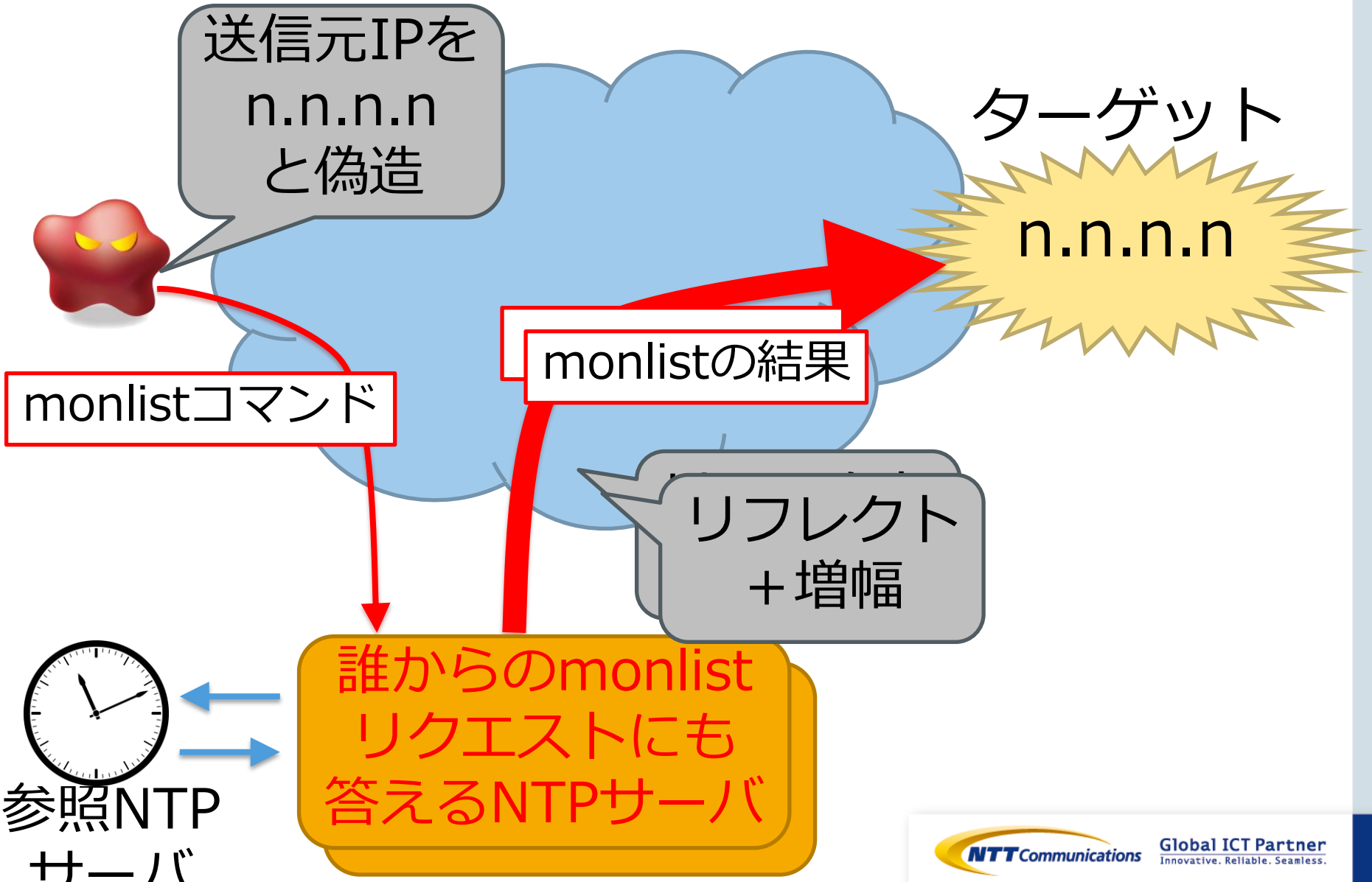
NTP reflection attackとは

- DDoSの一手法
  - ターゲットのアクセス回線帯域を溢れさせる目的

- 送信もとを偽装したNTP monlistコマンドによる攻撃
  - 送信もとを偽装
  - 反射板 (リフレクター: 不適切な状態のNTPサーバ) を利用
  - リフレクターでパケットサイズを増幅
    - ✓ 応答 / コマンド 倍率は数十～数百倍以上

- 基本的な構造は DNS amp と同様

NTP reflection attack: 基本的な仕組み



monlist

- monlistコマンドって?
  - clientのIPアドレス他、管理情報のリストを得る
  - 最大600行 => 44KB => 100パケット
    - ✓ NTPdのバージョンにもよるかも
  - アクセスしたclientが多ければ多いほど、効果が高い

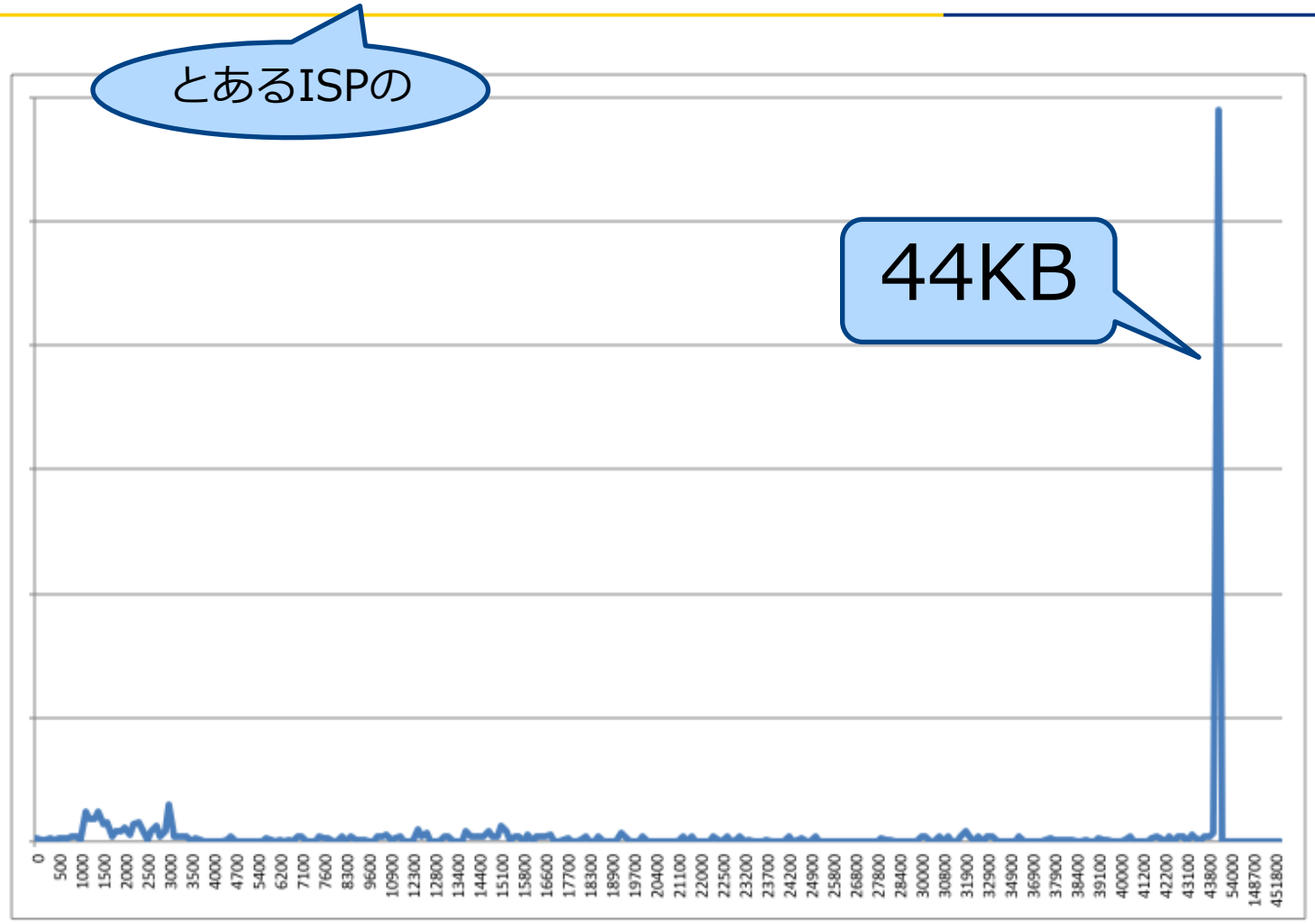
- コマンドライン
  - ntpdc –n –c monlist NTPサーバのIPアドレス

```
$ /usr/sbin/ntpdc -n -c monlist 192.0.2.123
remote address          port local address      count m ver code avgint  lstint
===============================================================================
192.0.2.70           57124 192.0.2.123          3 7 2     0   3194      0
192.0.2.51             123 192.0.2.123       3387 4 4     0   1008     39
192.0.2.69           38323 192.0.2.123         11 7 2     0  27441  63313
192.0.2.2            60947 192.0.2.123          2 7 2     0 554028 101944
   :                    :                  :          :
192.0.2.27           58440 192.0.2.123          1 7 2     0      0 244503
```

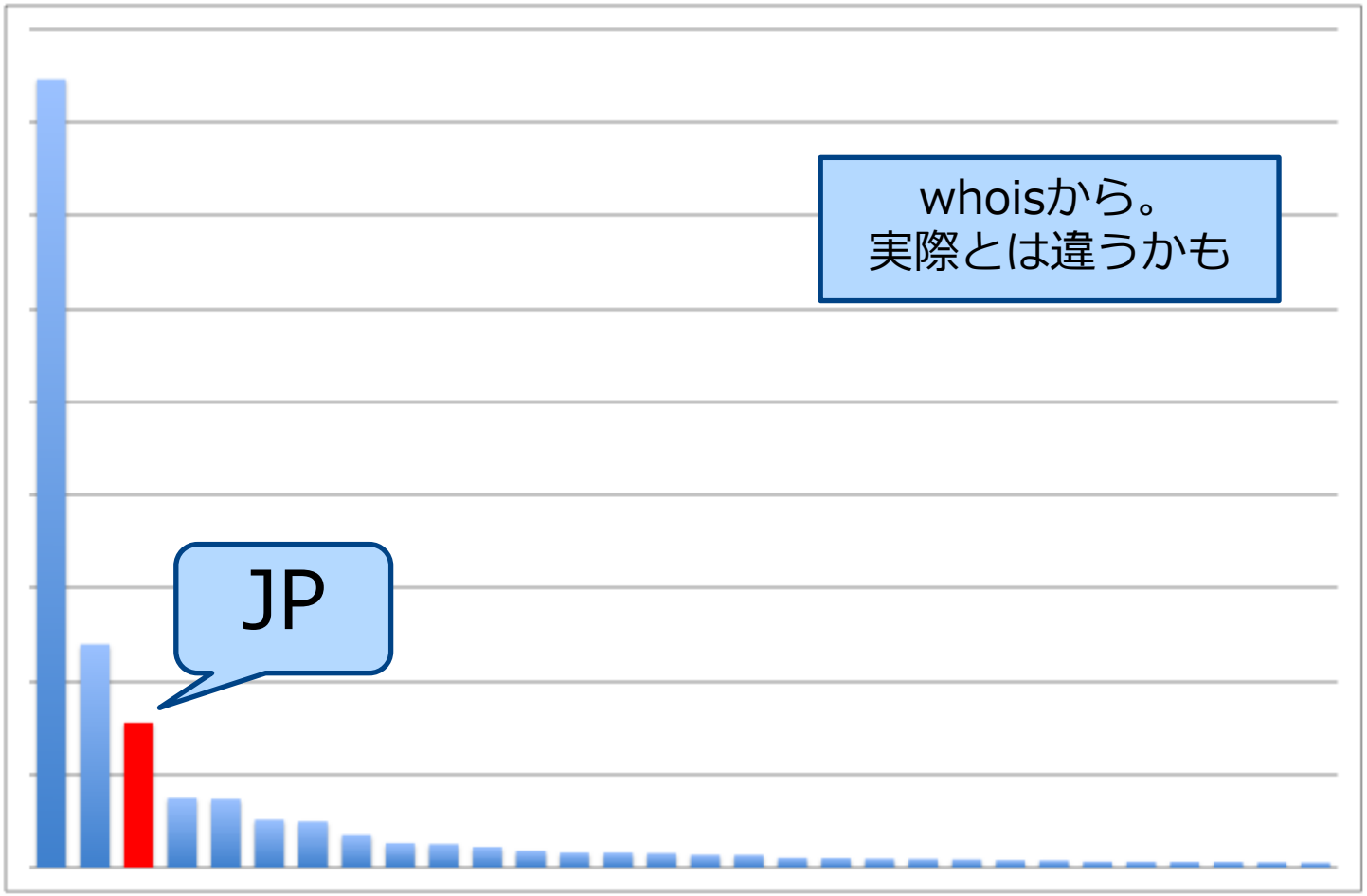
OpenNTPProject.org

- http://OpenNTPProject.org/
  - 不適切な設定のNTPサーバがどれくらいあるのか?
  - IPv4インターネット上をUDP/123でスキャン、リスト化
  - 検索サービスを提供
    - ✓ /22まで。/22より広い検索要求には拒否
  - こちらの統計情報から2枚

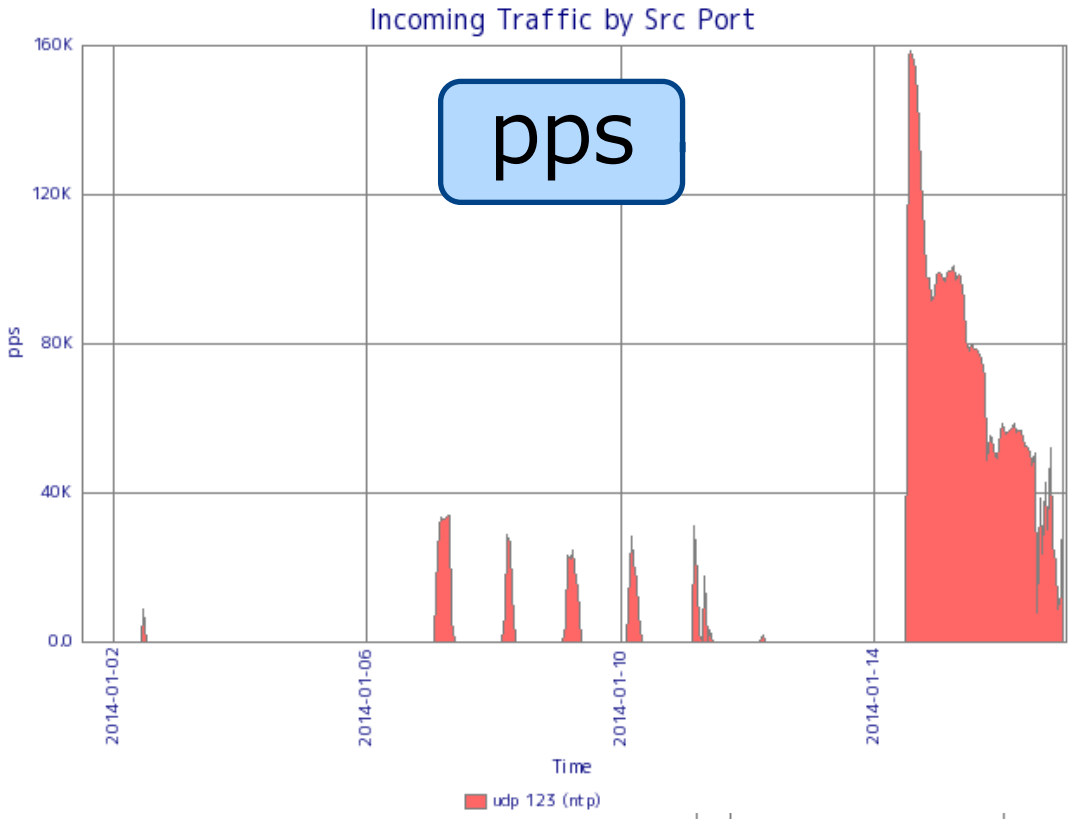
リフレクトサイズ集計



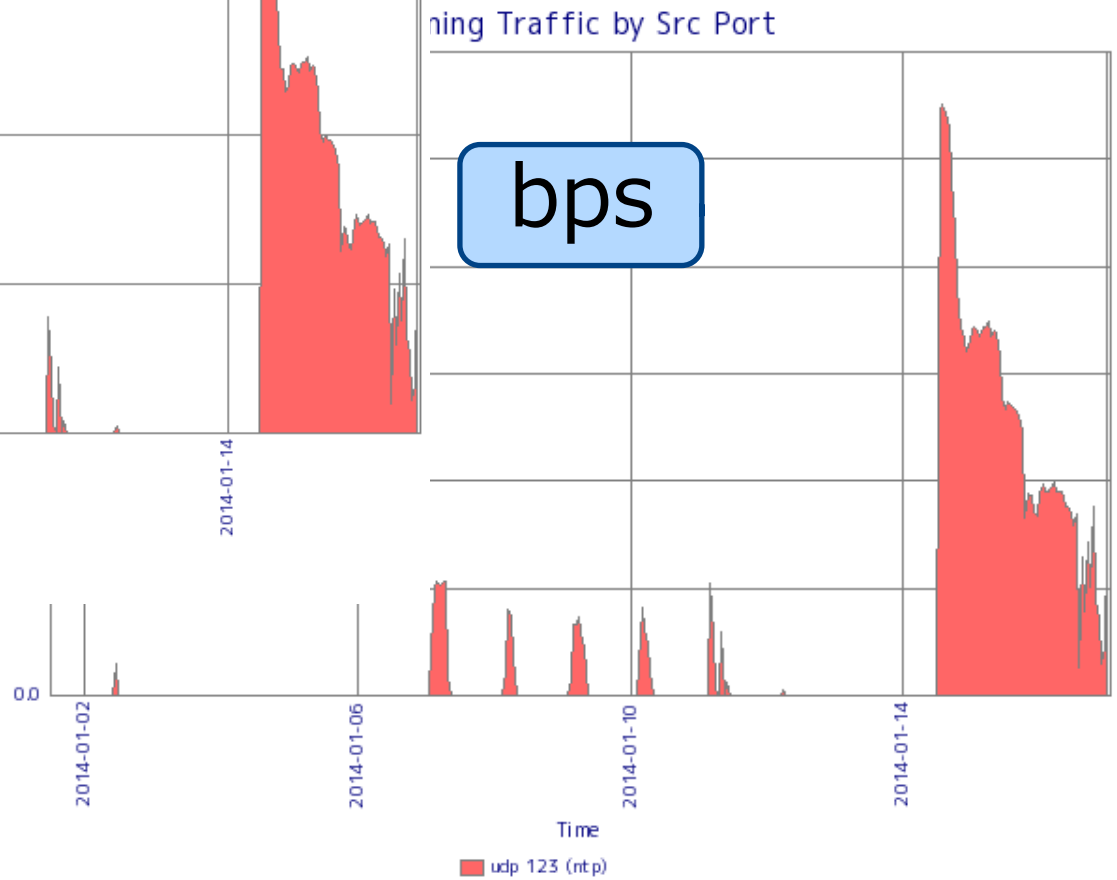
国別集計 (トップ30)



ppsとbps



pps



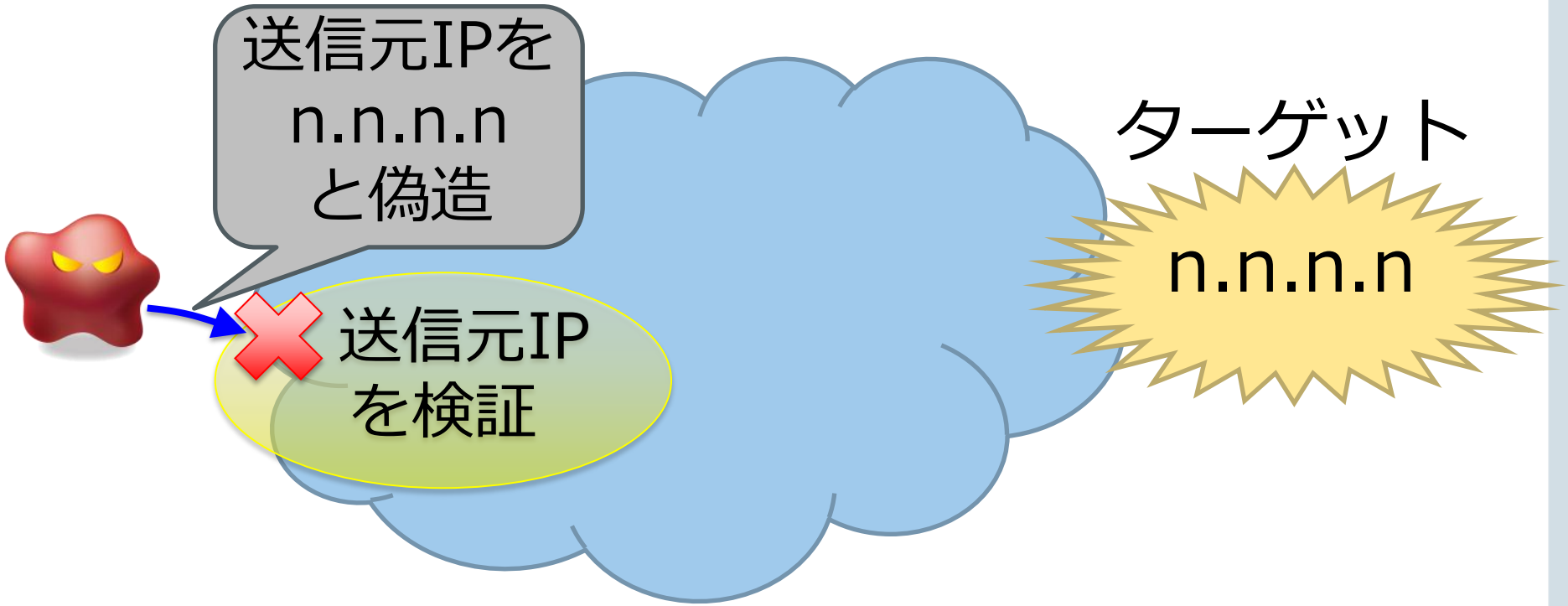
bps

対策

- ターゲット側では「お金で解決」な対策しか取れない

- 攻撃プラットフォーム側の対策をがんばるしかない
  - 攻撃者にとって魅力的でないようにしていく努力
  - 踏み台を減らす
    - ✓ 設定テンプレの普及
      - ✓ disable monitor
      - ✓ 適切なacl
    - ✓ 問題のある実装を撲滅
      - ✓ 古いNTPd
      - ✓ ホームルータ?
    - ✓ 「デフォルト設定」を安全側に倒す
      - ✓ 何もしなくても問題のない状態になっていること
  - BCP38

基本的な対策: Source Address Validation



誰からのmonlist
リクエストにも
答えるNTPサーバ

オープンリゾルバ

トラフィック可視化の重要性

- 自分のNWがどう使われているか、把握してますか?
  - ヘルスチェック
  - インシデント対応

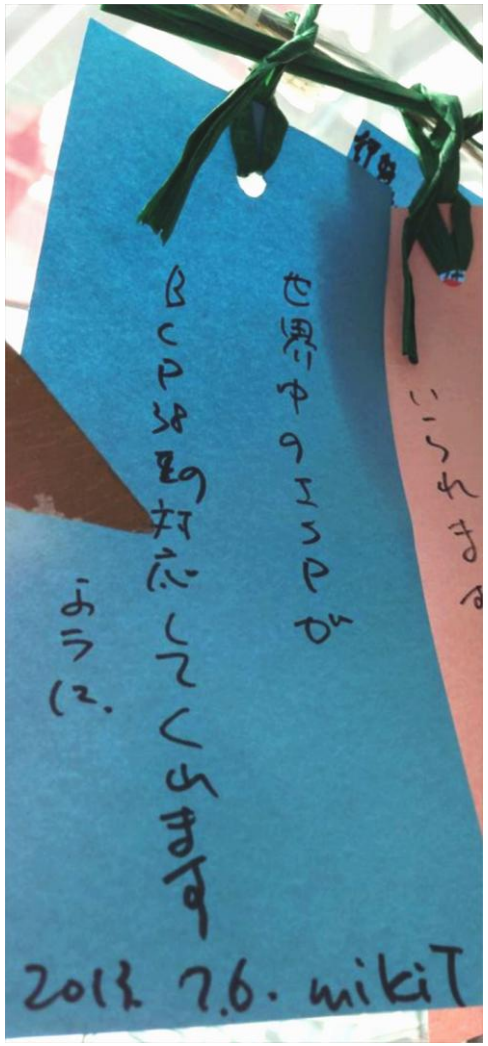
- 「今」どうなのか?
- 「過去」どうだったのか?
- 「未来」を予測するためにも重要

まとめ

- NTPヤバイ
- まずは現状把握しましょう

- テンプレを流行らせたい
  - オープンリゾルバ対応のように、日本語で。。
  - 「NTP担当」っていませんよね
  - WGやってみますか?

- もうひとつ、
- BCP38がんばろう!



参考資料(1)

- Hackers Spend Christmas Break Launching Large Scale NTP-Reflection Attacks
  - http://www.symantec.com/connect/blogs/hackers-spend-christmas-break-launching-large-scale-ntp-reflection-attacks
- NTP reflection attack
  - https://isc.sans.edu/forums/diary/NTP+reflection+attack/17300
- NTP DoS reflection attacks
  - https://cert.litnet.lt/en/docs/ntp-distributed-reflection-dos-attacks
- New DoS attacks taking down game sites deliver crippling 100Gbps floods
  - http://arstechnica.com/security/2014/01/new-dos-attacks-taking-down-game-sites-deliver-crippling-100-gbps-floods/
- 設定テンプレ集
  - https://www.team-cymru.org/ReadingRoom/Templates/secure-ntp-template.html
  - https://www.team-cymru.org/ReadingRoom/Templates/secure-endrun-template.html

参考資料(2)

- JPCERT/CC
  - https://www.jpcert.or.jp/at/2014/at140001.html
  - http://jvn.jp/cert/JVNVU96176042/
- @Police
  - https://www.npa.go.jp/cyberpolice/detect/pdf/20140117.pdf

- Amplification Hell: Revisiting Network Protocols for DDoS Abuse
  - Christian Rossow. 2014 Network and Distributed System Security Symposium, NDSS 2014, San Diego, CA, USA
  - http://www.internetsociety.org/ndss2014/programme#session1
    - ✓ We revisit 14 popular UDP-based protocols of network services, online games, P2P filesharing networks and P2P botnets, all of which are vulnerable to amplification DDoS attacks. We leverage traffic analysis to detect attack victims and amplifiers, showing that attackers already started to abuse amplification-vulnerable protocols other than DNS.