Operators' Life with no-Sampling Flow Data:

お客様に優しいDoS対応
～差分抽出による攻撃トラフィックの自動特定～

近藤　毅

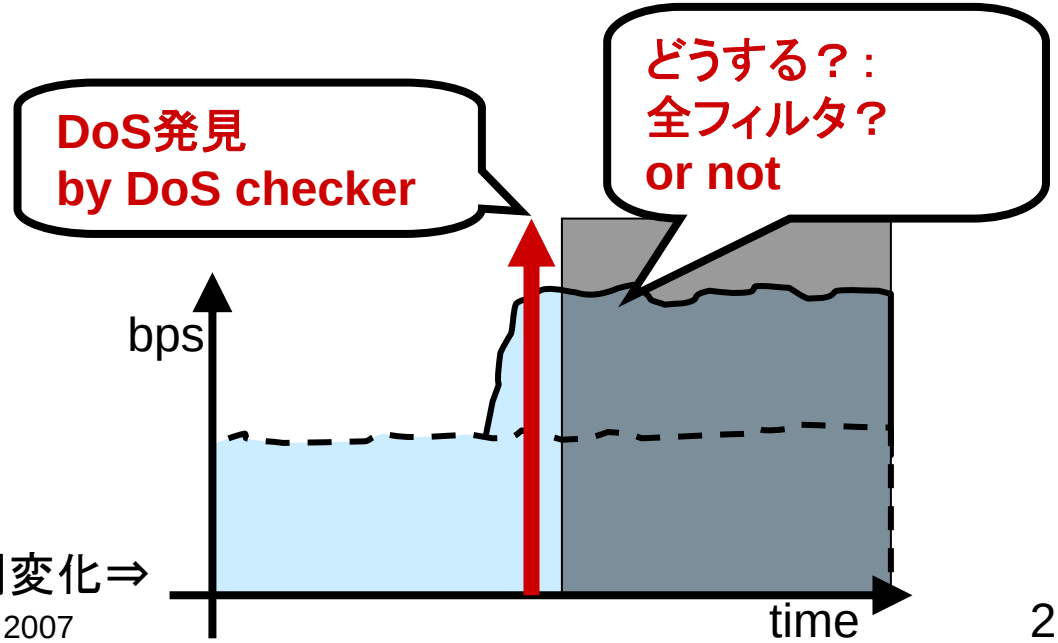
kondoh.tsuyoshi@lab.ntt.co.jp

NTT 情報流通プラットフォーム研究所
Flow Inspection Project

DoS CheckerでVictimは検出できる

- Dst_ip毎のトラフィック量変化を監視するため
- but, **VictimのIP addressだけでは,**
  全部止めるか，手動で追加分析するか，放置するか
  - 全部止めると，結局DoS成立

やりたいこと：攻撃トラフィック“だけ”の制御



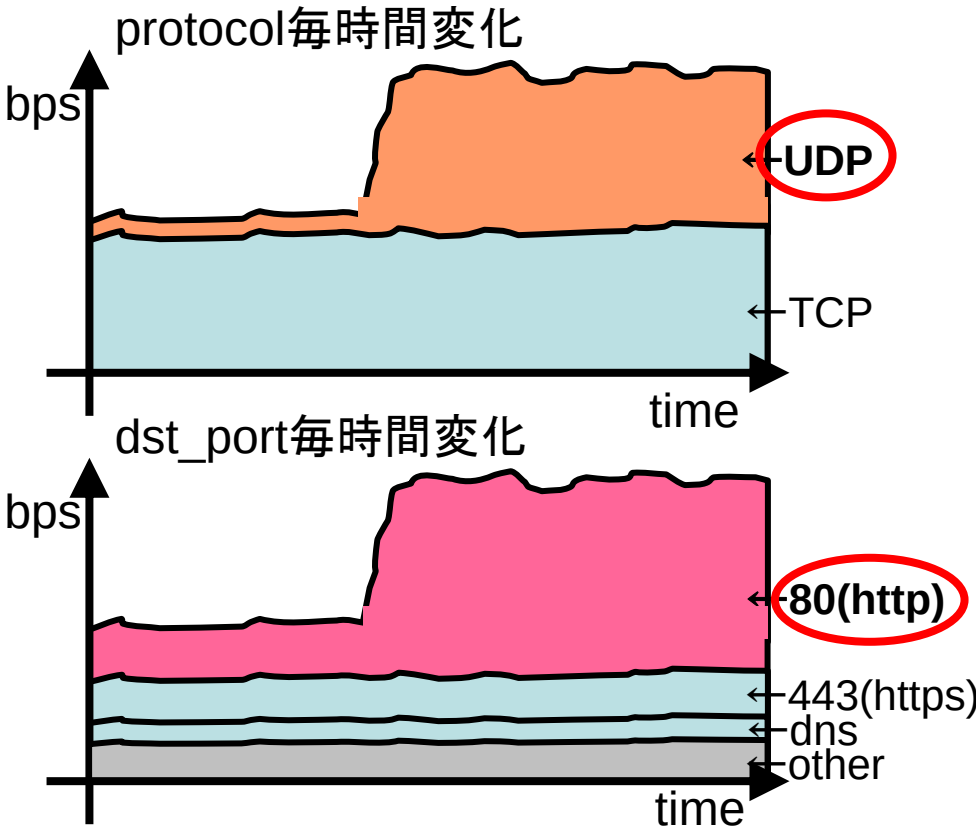
あるdst_ip宛てトラフィック量の時間変化⇒

現状のflow分析：手動ドリルダウン（1）

- トラフィック量の時間変化をいろんな次元で見る
  - protocol毎時間変化
  - dst_port毎時間変化
  - etc…

⇒徐々に絞り込む

  - 人間が手動で
  - ドリルダウン＝試行錯誤

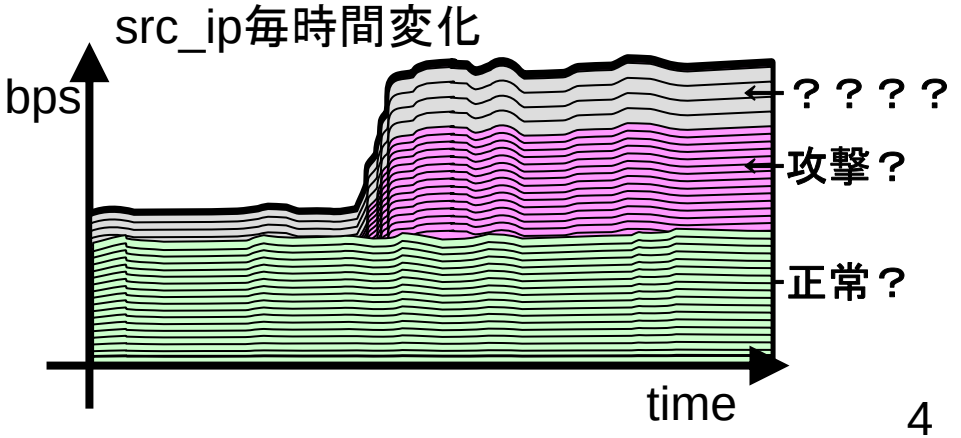


絞り込むほど，攻撃トラフィックだけを制御できる
（正常トラフィックへの影響を減らせる）

現状のflow分析：手動ドリルダウン（2）

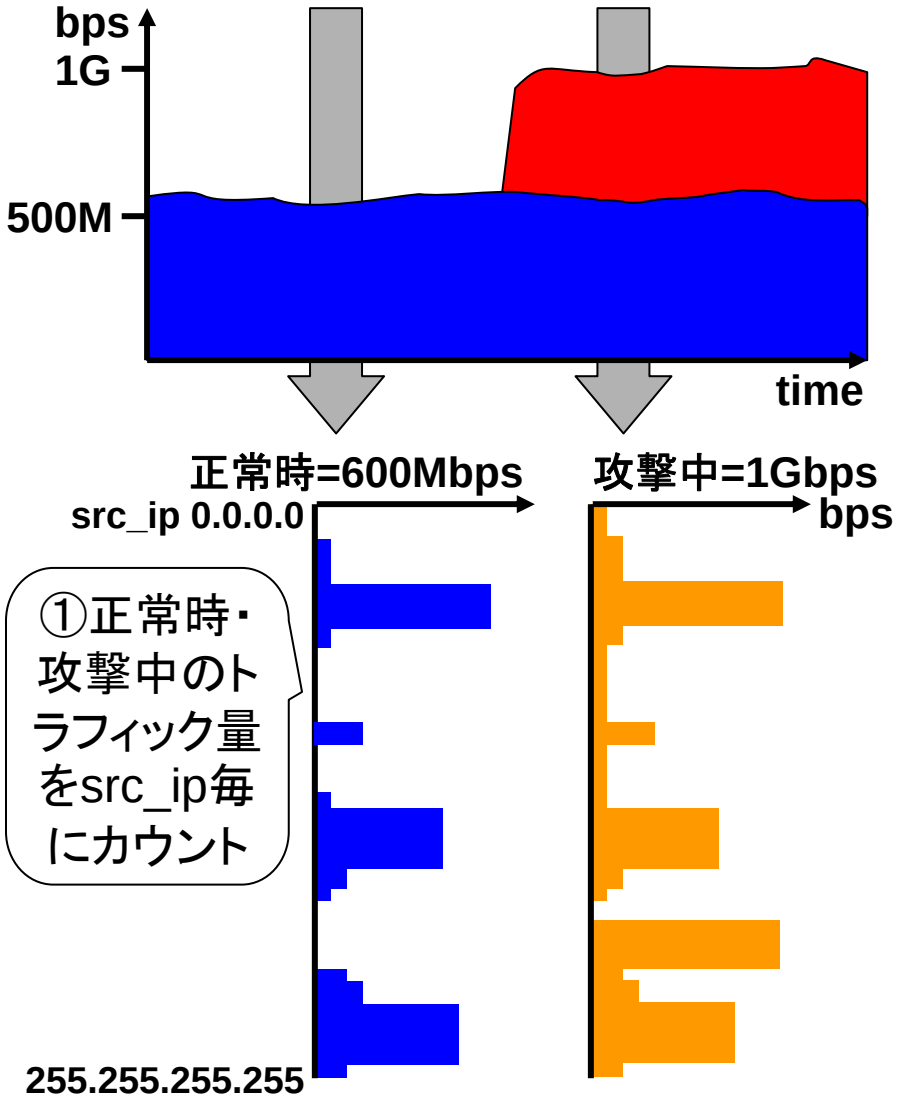
- DDoSでは攻撃元（src_ip）絞り込みが困難
  - 数千？～2^32（理論上限）の出現src_ip
  - src_ip毎の時間変化はグラフに描けない，人間も見られない
  - prefixで表現しないとACLも書けない

攻撃元を，prefix/lengthで自動特定したい



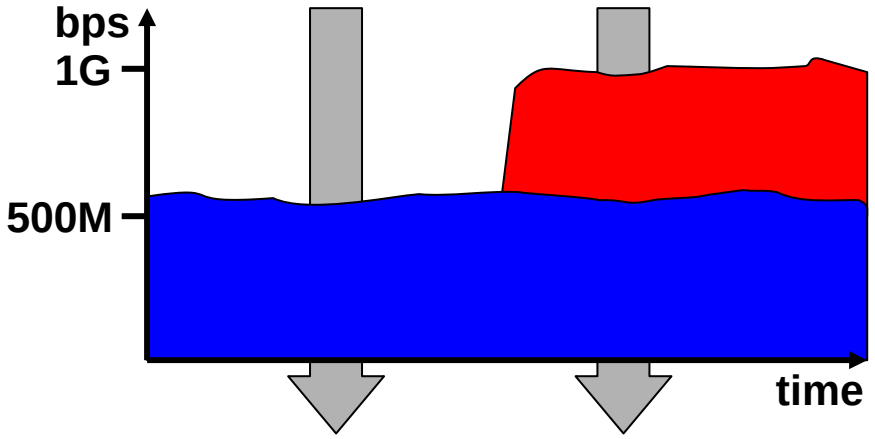
あしたのflow分析：
差分抽出による攻撃トラフィックの自動特定

- トラフィックの送信元（src_ip）の変化に注目して自動特定



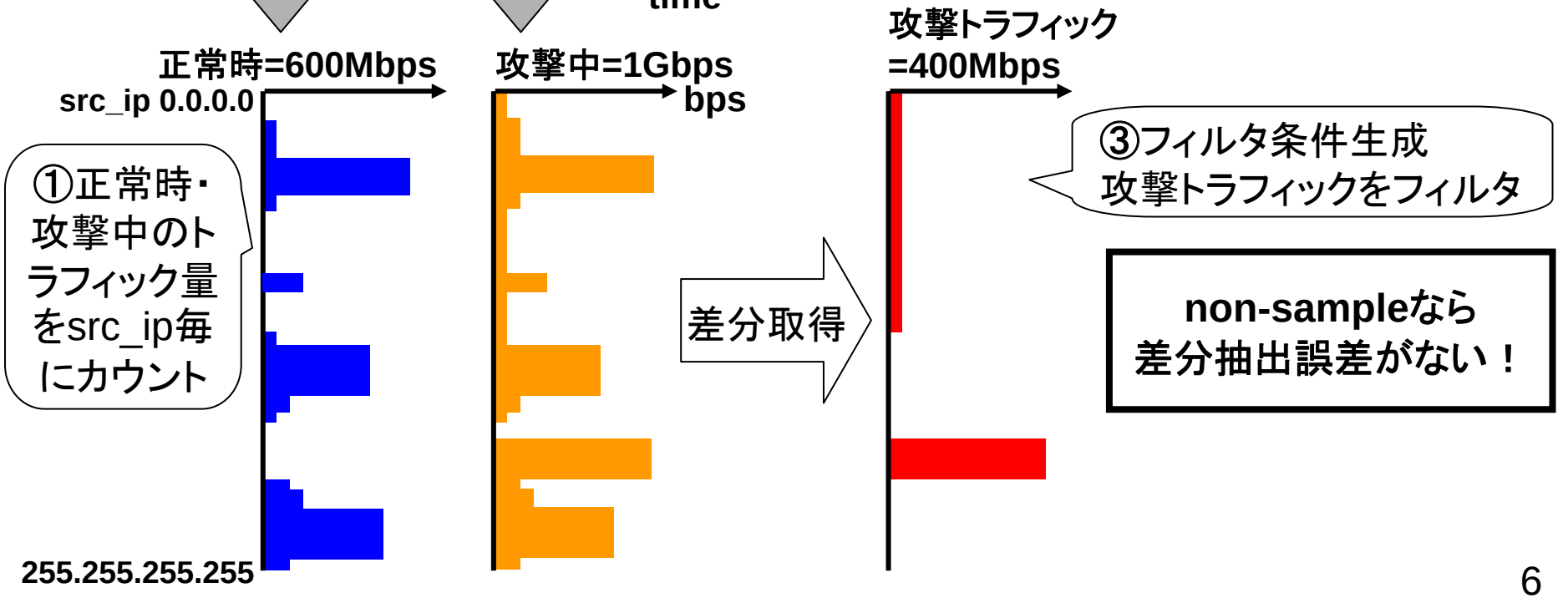
On Filtering of DDoS Attacks Based on Source Address Prefixes
Gary Pack, Jaeyoung Yoon, Eli Collins, Cristian Estan
SecureComm, August 2006

あしたのflow分析：
差分抽出による攻撃トラフィックの自動特定



On Filtering of DDoS Attacks Based on Source Address Prefixes
Gary Pack, Jaeyoung Yoon, Eli Collins, Cristian Estan
SecureComm, August 2006

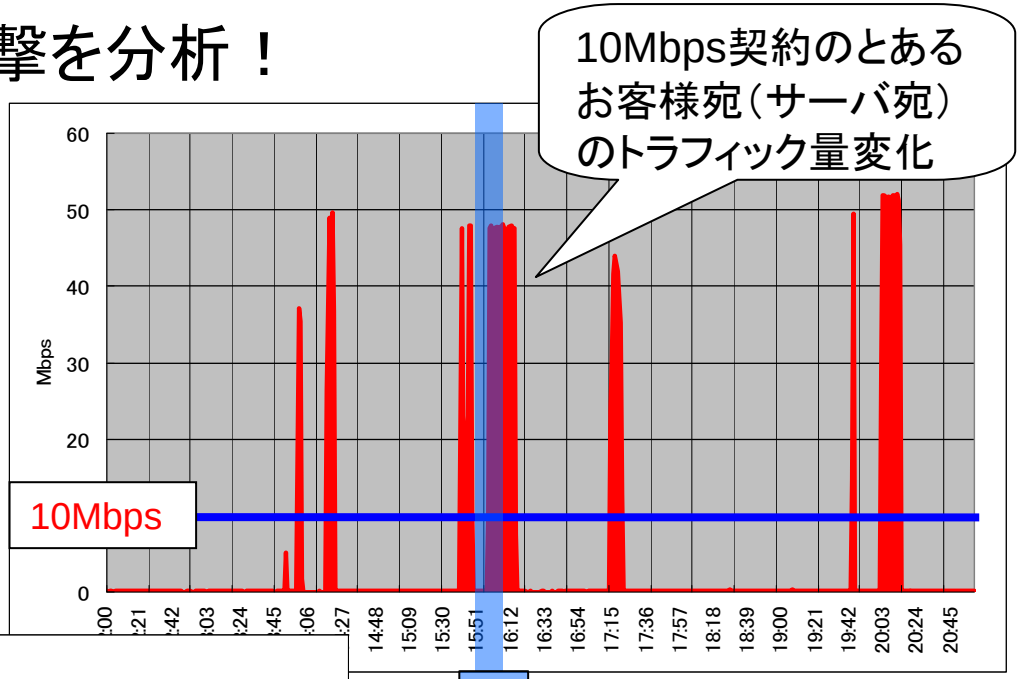
②攻撃中－正常時＝攻撃トラフィック
src_ip毎の攻撃トラフィック量を特定

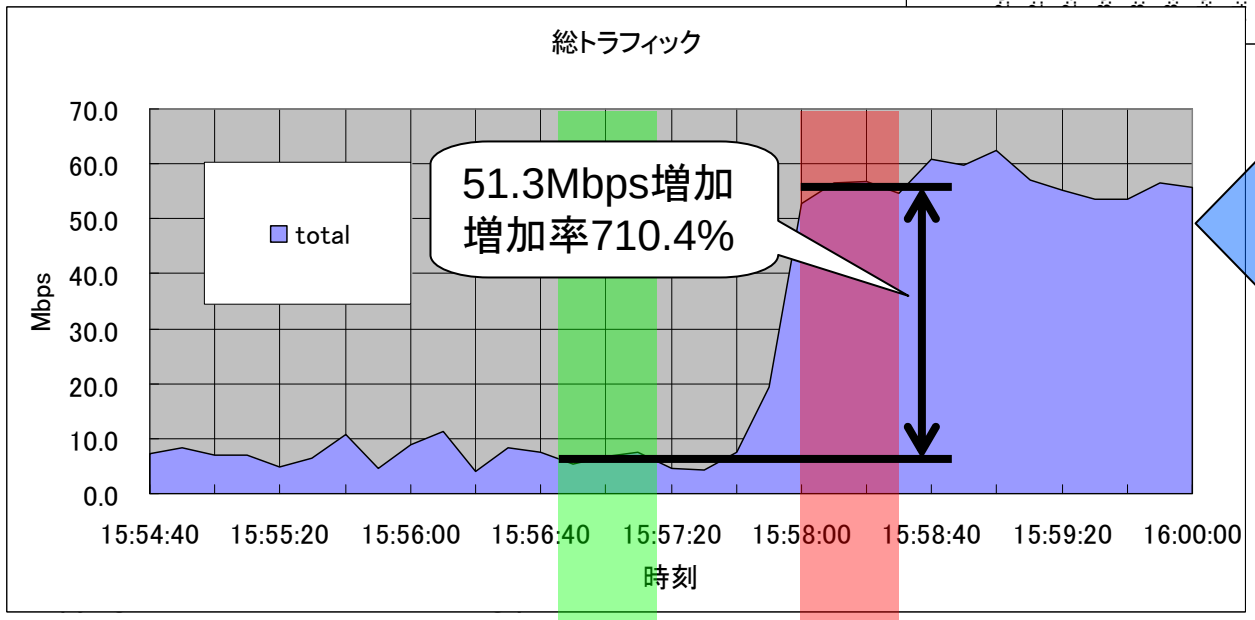


non-sampleなら
差分抽出誤差がない！

試しに実装して試験してみました：ターゲット

- DoS Checkerで検知した攻撃を分析！
- **緑と赤との比較して増加分のトラフィックを抽出**
  - 緑＝変化前
  - 赤＝変化中





この区間を拡大
（その他のお客様の
トラフィックも含む）

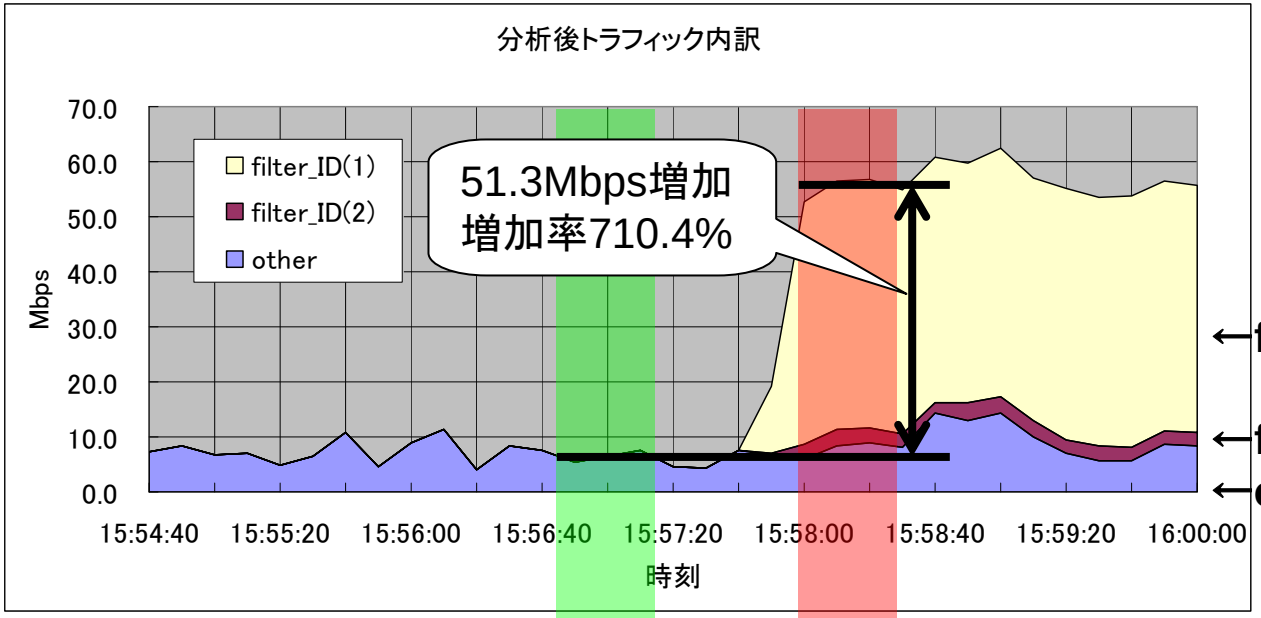
試しに実装して試験してみました：結果

- 分析結果

filter_ID	total=47.3Mbps					
	src_ip	dst_ip	proto	src_port	dst_port	
filter_ID(1)	XX.XX.162.247/32	XXX.XXX.17.99/32	*	low	low	**44.7Mbps (87.1%)**
filter_ID(2)	XXX.XXX.17.99/32	XXX.XXX.17.99/32	*	low	low	**2.7Mbps (5.3%)**

⇒原因トラフィック判明！

– フィルタを実施した場合の影響も判明

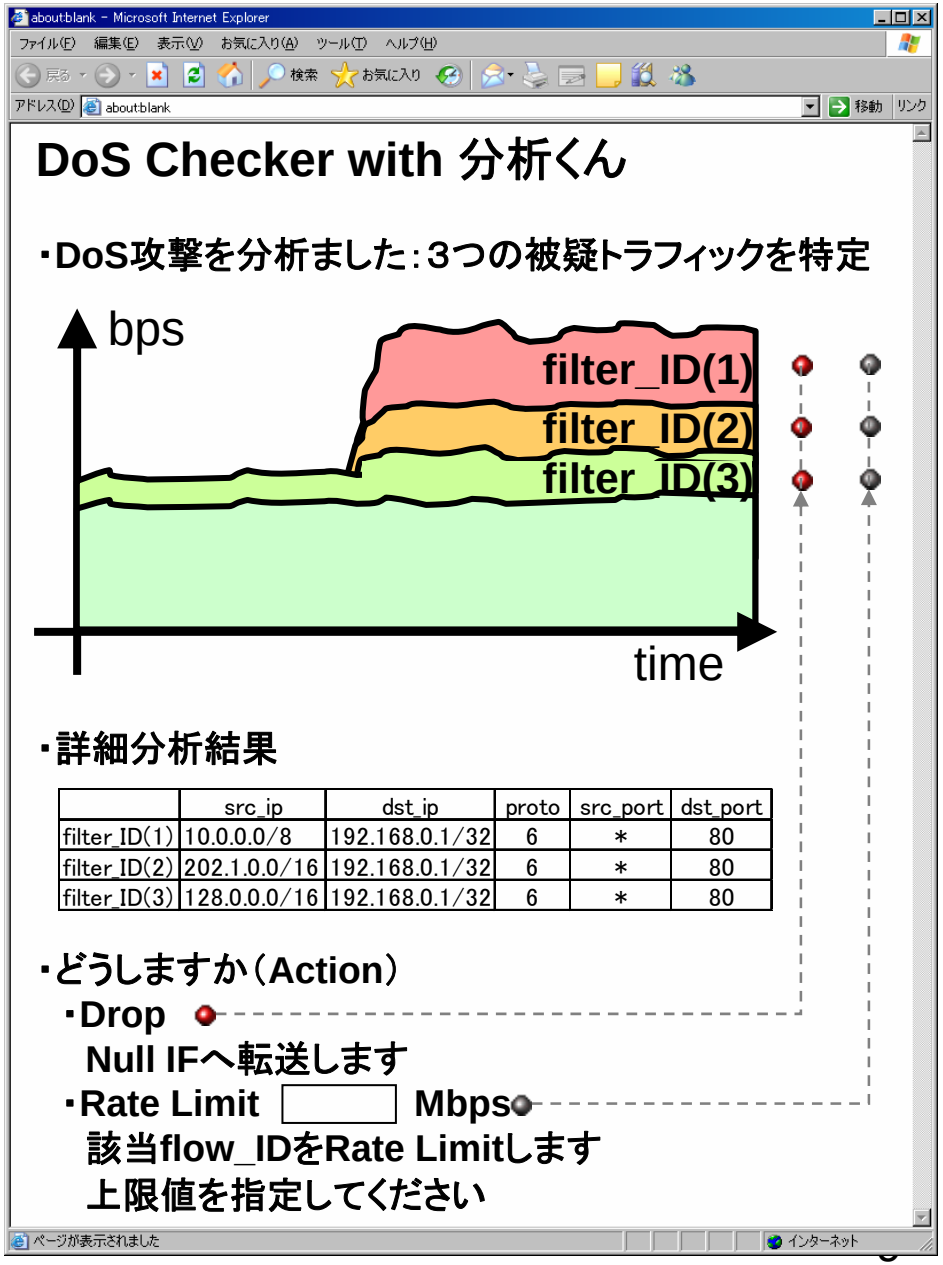


DoS Checkerと連携した未来

※画面は，はめこみ合成です

- 攻撃元を自動特定し，“お客様に優しい制御”を実施
  - dst_ip以外の制御条件も自動特定
    - src_ipも，protocolも．．．

⇒あとはActionボタンを押すだけでDoS攻撃だけをフィルタできる



	src_ip	dst_ip	proto	src_port	dst_port
filter_ID(1)	10.0.0.0/8	192.168.0.1/32	6	*	80
filter_ID(2)	202.1.0.0/16	192.168.0.1/32	6	*	80
filter_ID(3)	128.0.0.0/16	192.168.0.1/32	6	*	80

まとめ

- 手軽に攻撃トラフィックを特定できるアルゴリズムの紹介
  - 変化前との差に注目するため，攻撃トラフィックだけを分離
  - 必要ならばそのままACLを書ける

- その他の応用例
  - 攻撃に限らず分析可能：変化を引き起こした原因トラフィックを特定
    - ex. トラフィックシフト，トラフィック集中（Flash Crowd）
  - トラフィック量減少の原因を特定（居なくなったトラフィックの特定）
    - サイレント故障，トラフィックシフトの把握

- トラフィックモニタ・解析は大切
  - ただし，定常時にトラフィック弁別するのは難しい
  - 変化が起きたタイミングこそチャンス

参考文献（1）[SAPF]:
今回紹介した手法

- Gary Pack, Jaeyoung Yoon, Eli Collins and Cristian Estan, **“On Filtering of DDoS Attacks Based on Source Address Prefixes,”**
  SecureComm, August 2006
  - 送信元の変化に注目したDDoS攻撃軽減手法
  - 著者らの先行研究である[Automatically]の応用例として提案
  - 正常トラフィックを避け，異常トラフィックだけをフィルタするヒューリスティックな手法が提案されている
  - 後述の[Automtically]との差
    - [SAPF]は意図的に正常トラフィックの巻き添えを避けるようにフィルタ条件を生成する（[Automatically]では巻き添えを考慮しない）
    - [Automatically]は5次元でトラフィックをプロファイリングするが[SAPF]は送信元(src_IP)に限定されること
  - http://pages.cs.wisc.edu/~estan/publications/DDoSfiltering.pdf （論文）

参考文献（2）[Automatically]: [SAPF]のベースとなった先行研究

- Cristian Estan, Stefan Savage and George Varghese, **“Automatically Inferring Patterns of Resource Consumption in Network Traffic,”** SIGCOMM, August 2003
  - トラフィックを多次元でとらえること手法を提案した有力な論文
    - トラフィックプロファイリング，トラフィッククラスタリングと呼ばれる手法の1つ
    - この論文では多次元として，src_ip, dst_ip, protocol, src_port, dst_portの5つのトラフィック属性（次元）を採用
  - オペレータへのトラフィックレポート作成を主眼としている
  - 求めたプロファイル間の差分抽出手法も提案されており，トラフィックの変化分を抽出することが可能

  - http://pages.cs.wisc.edu/~estan/publications/trafficclusters.pdf (論文)
  - http://pages.cs.wisc.edu/~estan/publications/trafficclusters.ppt (発表資料)

参考文献（3）[AutoFocus]: [Automatically]の実装例

- AutoFocus tool
  NANOG29 Oct. 2003で発表
  - [Autofocus]の実装例
  - 公開されていたがオフィシャルページはリンク切れ

  - http://ial.ucsd.edu/AutoFocus/ (official: リンク切れ)
  - http://pages.cs.wisc.edu/~estan/publications/autofocusnanog.ppt（発表資料）
  - http://www.caida.org/tools/measurement/autofocus/ (動作例)