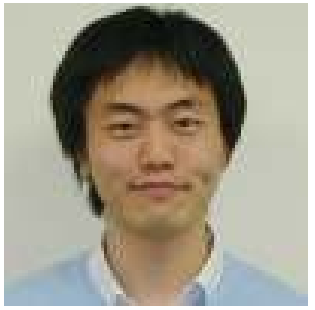
IETF93報告会
dots WG

2015.08.27

Kaname Nishizuka@NTT Communications

自己紹介

- 2006年 NTTコミュニケーションズ入社。
- OCNアクセス系ネットワークの設計に従事した後、
  大規模ISP向けのトータル保守運用サービスを担当。
- 現在、DDoS対策ソリューションの開発および、
  CGN関連技術のIETF提案活動に従事
- ISOC-JP プログラムチェア



【社外活動】

- JANOG28 実行委員長
- JANOG30 会場運営委員長
- JANOG32 「HTTP 2.0のインパクト」登壇
- HTML5 Conference 2013 NWチーム
- Interop2014「IPv6ホットトピックス」登壇

dots (SEC area)

3

dots WG

- **DDoS Open Threat Signaling WG**
- **設立：2015年(IETF93より)**
- **Chairs: Roman Danyliw (CERT)**
  Tobias Gondrom (Cisco)

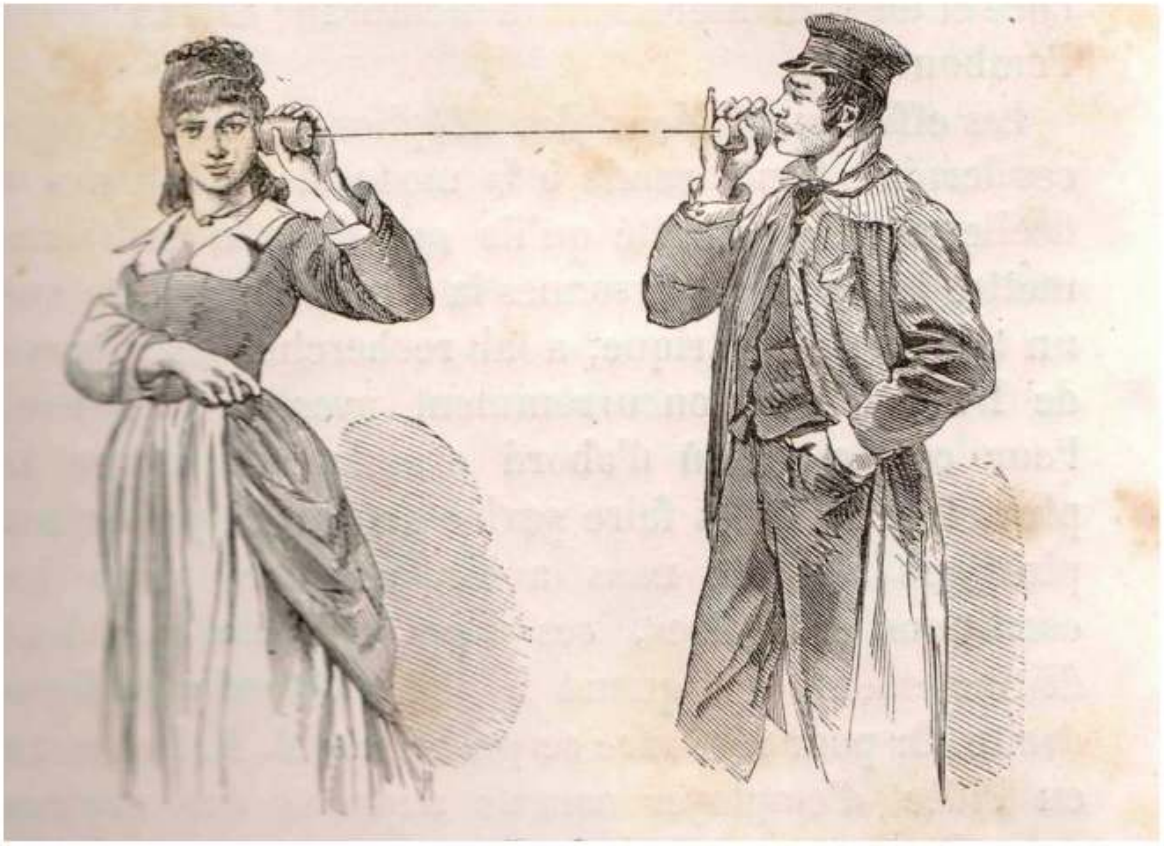
- DDoS対策に関連する情報のシグナリングの標準化を扱う
- 経緯：
  - IETF92：BoF
    - ✓ http://www.isoc.jp/wiki.cgi?page=IETF92Update
  - 2015.06.27 WG化

Charter

- Dots WGの目的
  - DDoSに関連したテレメトリ情報・脅威情報・対策の要求をリアルタイムにシグナルする標準的な手法を開発する
    - ✓ DDoS攻撃の検知
    - ✓ 分類
    - ✓ 攻撃元情報
    - ✓ Mitigation情報
- エレメント
  - On-premise DDoS mitigation platforms
  - Service provider DDoS mitigation platforms
  - Other network elements and services
- 関連WG
  - M3AAWG, SACM, MILE, SUPA, I2NSF et.al.

今のDDoS対策

How Can You Ask for Help Today?



Technology pioneered by Robert Hooke in 1667, only slightly improved!

NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

Agenda

1. Note well, logistics, charter introduction (chairs, 5 min)
2. Use Case Discussion (20 minutes)
   - draft-mglt-dots-use-cases-00 (Daniel Migault, 10 min)
   - draft-xia-dots-extended-use-cases-00 (Frank Xialiang 10 min)
   draft-fu-ipfix-network-security-01
3. Requirements Discussion
   - draft-mortensen-threat-signaling-requirements-00 (Andrew Mortensen, 10 min)
   - Chris Morrow and Roland Dobbins (10 min)
4. Discussion (10 min)
   - Way ahead for use case discussion
   - Way ahead for requirements discussion
   - Who is implementing?
   - Virtual Interim Meeting in September 2015
5. Summaries of Other Drafts (5 min)
   - draft-teague-open-threat-signaling-01 (Nik Teague)
   - draft-reddy-dots-transport-00 (Tiru Reddy)
   draft-reddy-dots-info-model-00

(1)

(2)

(3)どのようにまとめるかの議論

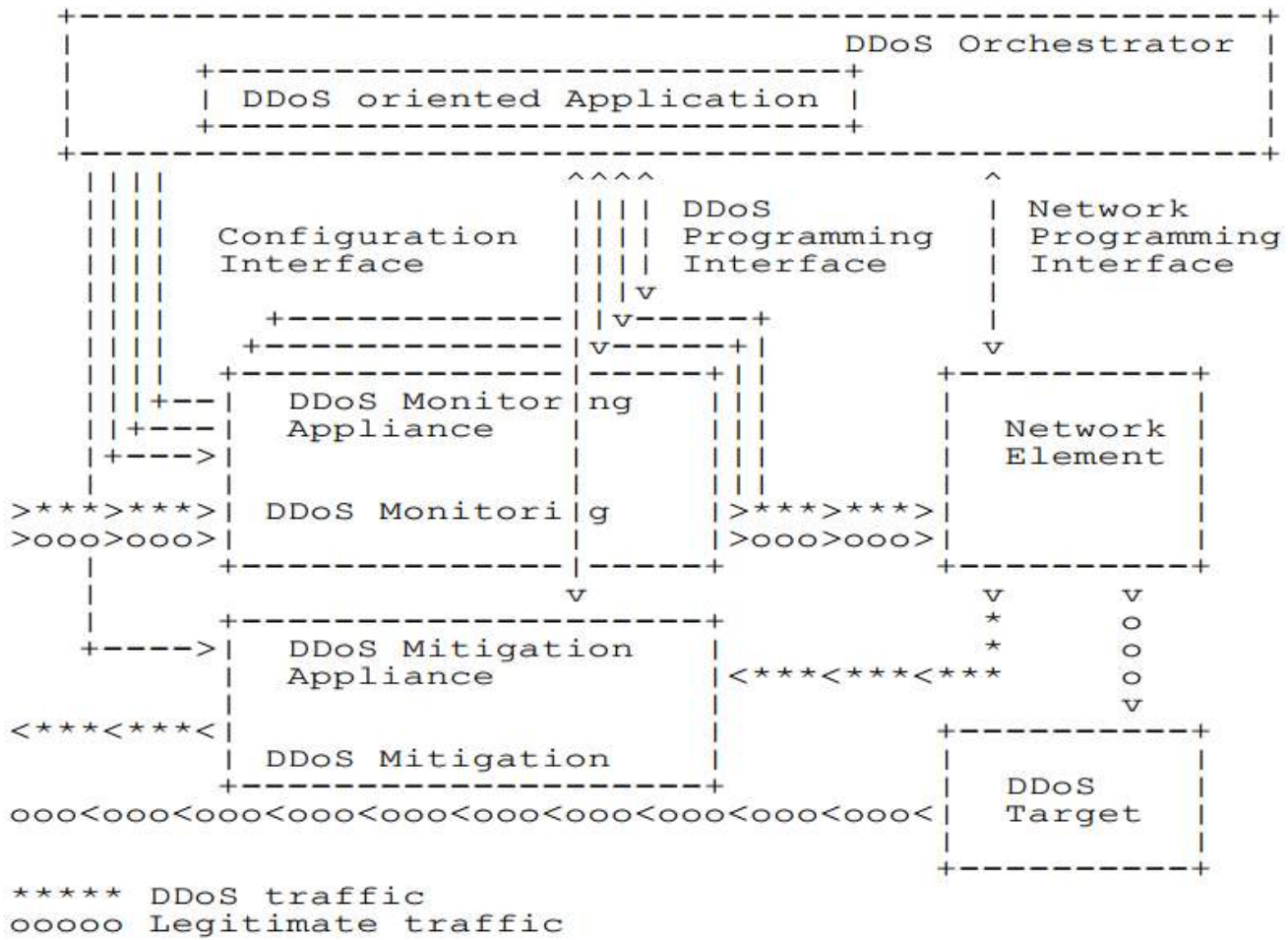
時間切れ

(1) Usecase draft 1(1/3)

- DDoS Open Threat Signaling use cases
  - draft-mglt-dots-use-cases-00
- dotsに期待すること
  - 個別のアプライアンスで実現してきたDDoS対策の拡張
  - Inter-domain DDoS monitoring
    - ✓ DDoS検知をより早く正確に
  - Inter-domain DDoS mitigation
    - ✓ 協力して効率のよい攻撃緩和
  - 複数の組織間でのモニタリング情報のシェア
  - サードパーティーへのDDoSのモニタリングと緩和のシェアまたは委譲

(1) Usecase draft 1(2/3)

On-Premise Asymetric (DOTS)



(1) Usecase draft 1(3/3)

- 会場での議論
  - DDoS Orchestratorとは何か？
    - ✓ 明確な答えはなし
  - DDoS Programming I/Fは、i2nsfの領域では？
    - ✓ 明確な答えはなし

- 現状のDDoS対策については、説明されているが、Dotsがどの領域を担うのか、ということについては不明確
- Usecaseについて議論する最初のきっかけとしては及第点

(1) Usecase draft 2(1/2)

- The Extended DDoS Open Threat Signaling Use Cases
  - draft-xia-dots-extended-use-cases-00
- 一つ目のUsecase Draftをうけてusecaseを追加

Use Case 1

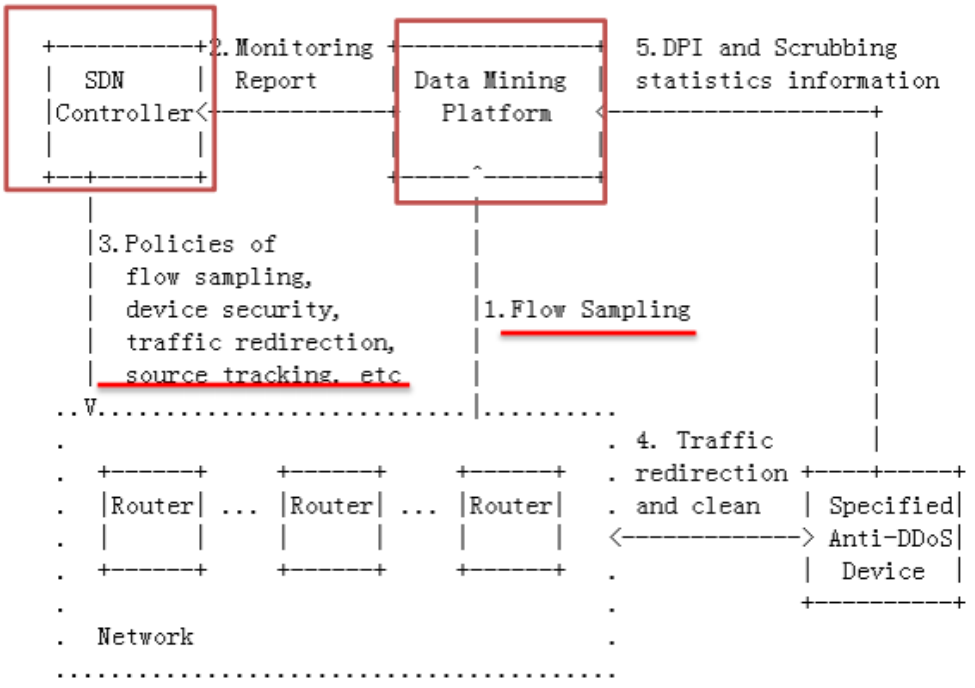


Figure 1. Data Mining and SDN Based Centralized Anti-DDoS Use Case

(1) Usecase draft 2(2/2)

- Inter-domainのイメージ

Use Case 3 (not yet in draft)

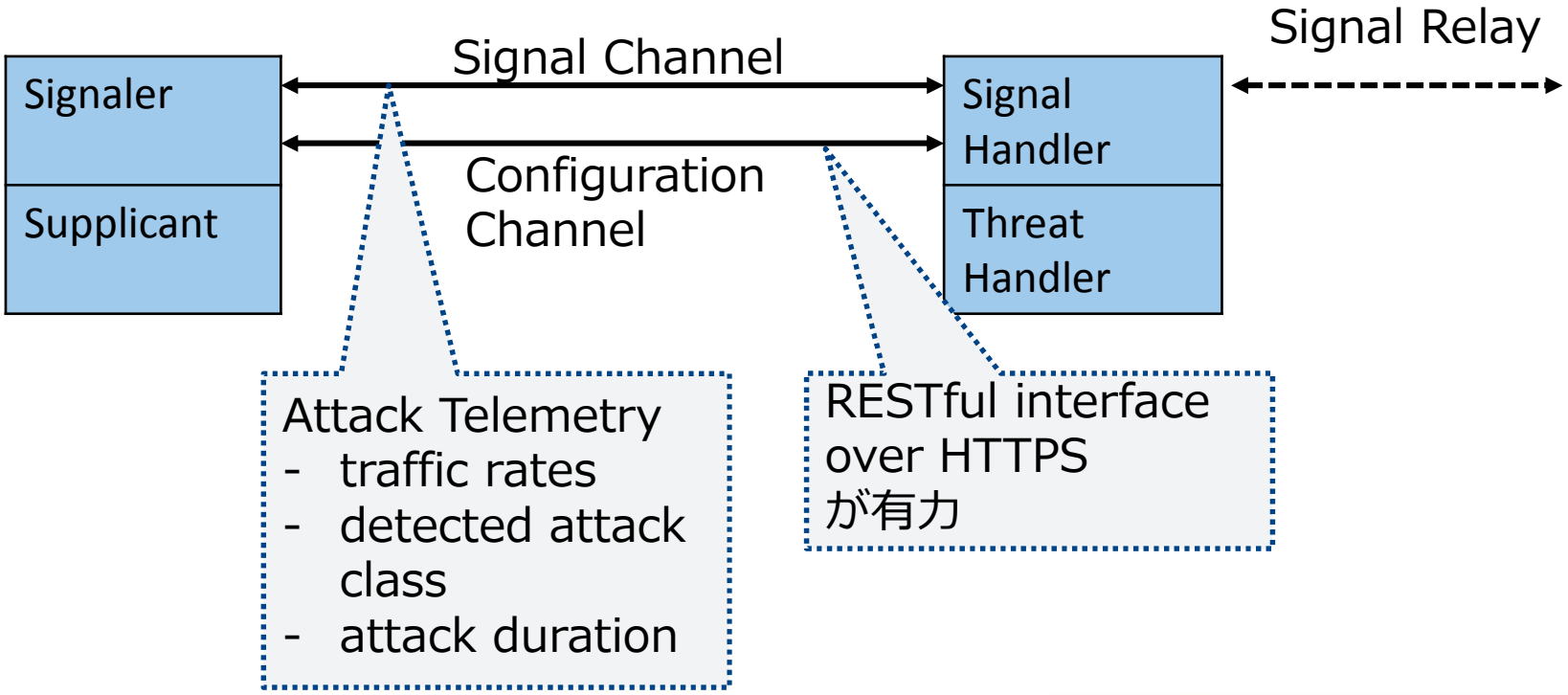
Inter-domain Anti-DDoS Coordination

Carriers and MSSPs unite to coordinate global mitigation resource to carry out near source mitigation.

① One of the alliance members mitigates traffic within the bandwidth, application-layer attacks using a local DDoS mitigation system and detects large-traffic attacks.
② When not being able to defend large-traffic attacks, the victim member sends cloud signal to the CCC (Cloud Coordination Center) request global near source mitigation.
③ The CCC notifies the corresponding alliance members to initiate near-source mitigation.

(2) Requirement draft

- DDoS Open Threat Signaling Requirements
  - draft-mortensen-threat-signaling-requirements-00
- 用語の定義



※IPFIXにはこだわらない

まとめ

- Usecaseドラフト
  - 一つにまとめる
  - エディターを募集中
- Requirementドラフト
  - 一つにまとめる
  - エディターを募集中
  - Usecaseドラフトとの整合性の整理が必要

Milestones

- Feb 2016 - **Requirements/use case** information document to IESG
- May 2016 - **Transport document** as proposed standard to IESG
- Jun 2016 - **Data model document** as proposed standard to IESG

- オペレータからの期待は高い
  - DDoS対策の協調(早さ/効率/キャパシティ)
  - ベンダロックインの回避
- そのため、文章の精度を上げてScopeを明確化することが急務
  →いっしょにやりませんか？