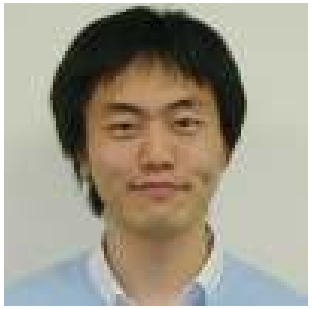
# IETF94報告会
# dots WG

2015.12.08

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関連技術およびCGN
  関連技術の開発とIETF提案活動に従事
- 2015～ ISOC-JP プログラムチェア



NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

# dots WG

- **DDoS Open Threat Signaling (dots)**
- **設立：2015-06**
- **Chairs: Roman Danyliw(CERT)**

**Tobias Gondrom（OWASP, Huawei)**

- 新しいWG(BoF:IETF92 / Meeting:IETF93,94)
- DDoS対策を効率的に実現するために、DDoSに関連した情報のリアルタイムでのシグナリングを規格化する
  - 自動化
  - より大規模な防御システム
  - ベンダ独自なソリューションからの開放

# Charter(-01)

- 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.

# IETF94 Agenda

1. Note well, logistics and introduction (chairs, 5 min)
2. Use Case Discussion (50 min)
   - draft-ietf-dots-use-cases-00 (Roland Dobbins, 30 min)
   - draft-nishizuka-dots-inter-domain-usecases-00 (Kaname Nishizuka, 10 min)
   - Additional use cases discussion (10 min)
3. Requirements Discussion (30 min)
   - draft-ietf-dots-requirements-00 (Andrew Mortensen, 20 min)
   - Additional requirements discussion (10 min)
4. Additional Drafts (40 min)
   - draft-reddy-dots-transport-01 (Prashanth Patil, 10 min)
   - Discussion (5 min)
   - draft-fu-dots-ipfix-extension-00 (Frank Xia Liang, 10 min)
   - Discussion (5 min)
5. Closing (5 min)

# ユースケースに関する議論

- 00versionのWGドラフト
  - draft-ietf-dots-use-cases-00
  - 用語の定義
  - 現状で使われているDDoS対策における構成の列挙

- 個人でユースケースのドラフトを投稿
  - draft-nishizuka-dots-inter-domain-usecases-00
  - WGドラフトでは足りていないインタードメインのユースケースをカバー
  - ベンダ依存性をより排除

発表時スライド

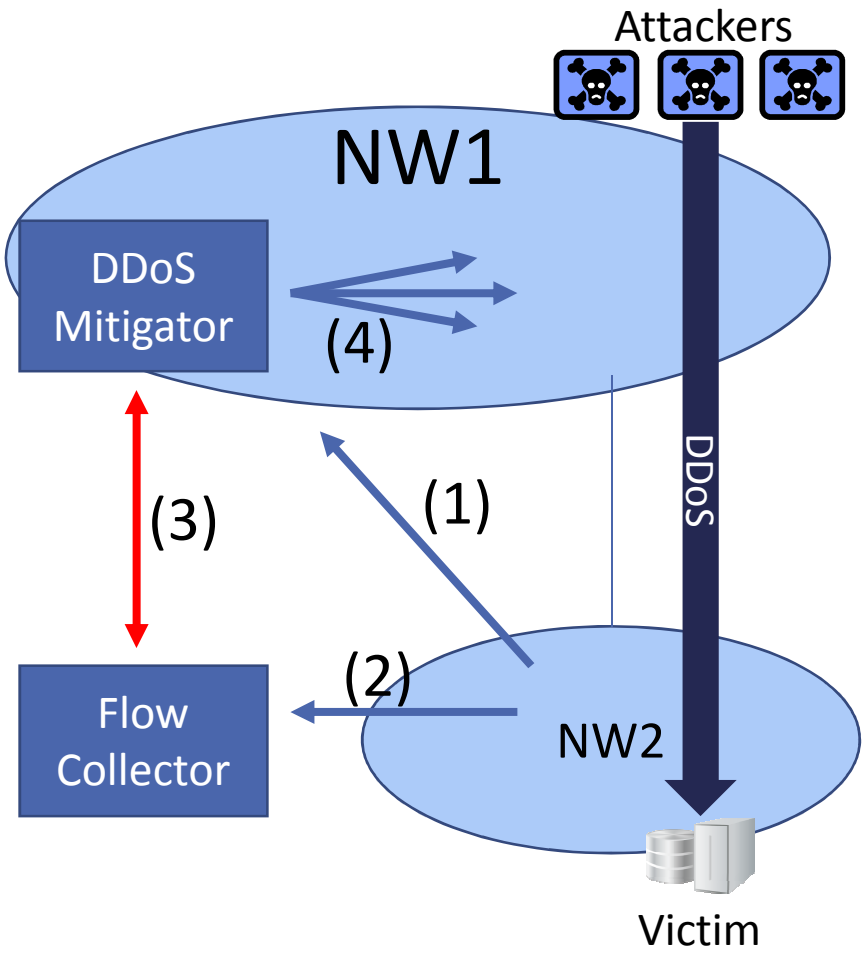
# Inter-Domain DOTS Use Cases

draft-nishizuka-dots-inter-domain-usecases-00

Kaname Nishizuka, NTT Communications
Nov. 2015 IETF94@yokohama

発表時スライド

# Scenario Overview




(1)Provisioning stage

Provisioning of DDoS protection capability

(2) DDoS Detection

- Automatic detection
- Automatic/manual trigger of DDoS protection

Scope of Dots

(3)Signaling stage

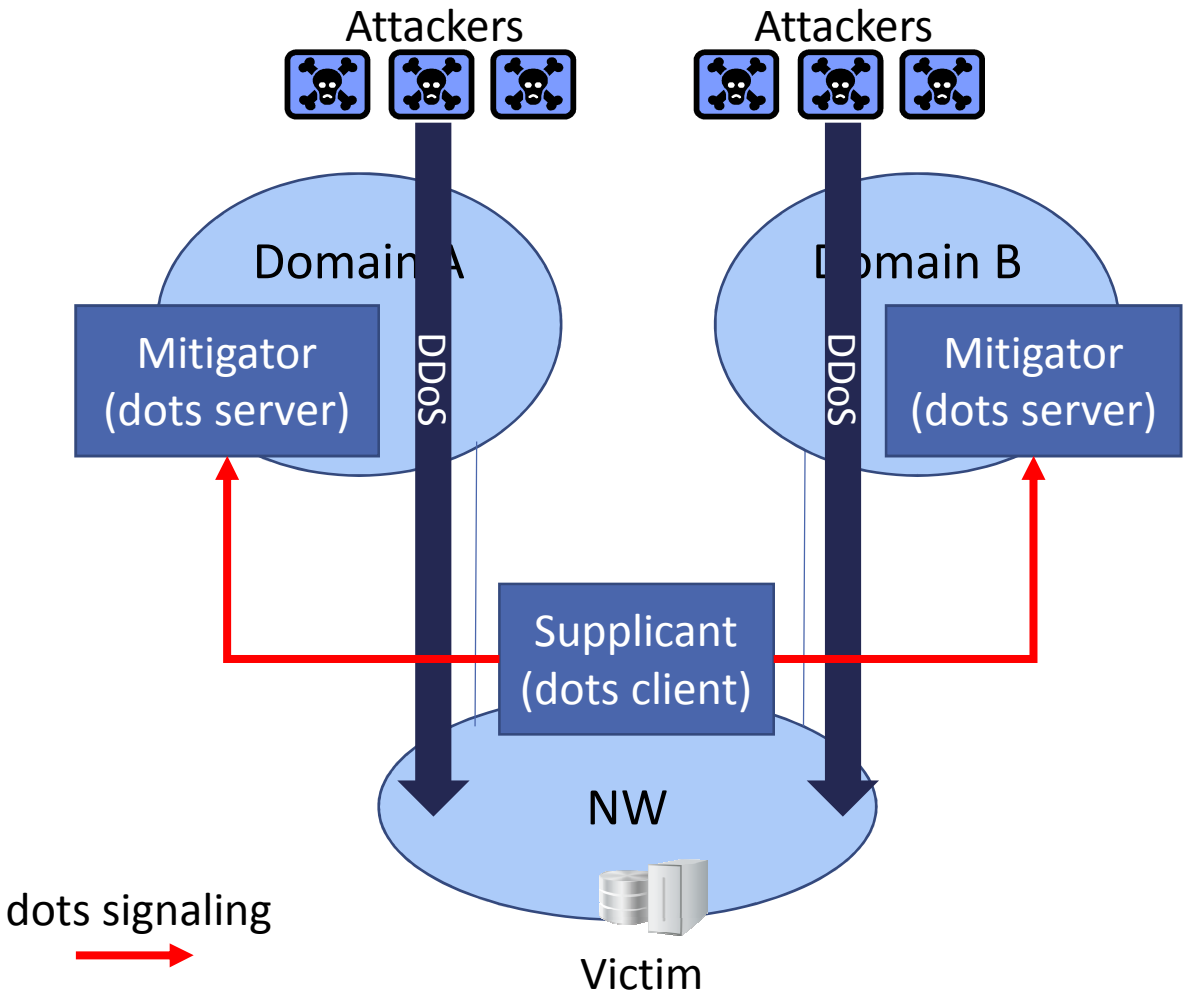
"Call for help" signaling from supplicant (=flowcollector, in our case) to DDoS mitigator

(4)Mitigation action from the mitigator to NW elements

- BGP injection(RTBH/Diversion)
- Controlling multi-vender mitigation box
- Changing ACL of routers
- Flowspec advertisement

発表時スライド

# Inter-domain usecase1: Multi-home model

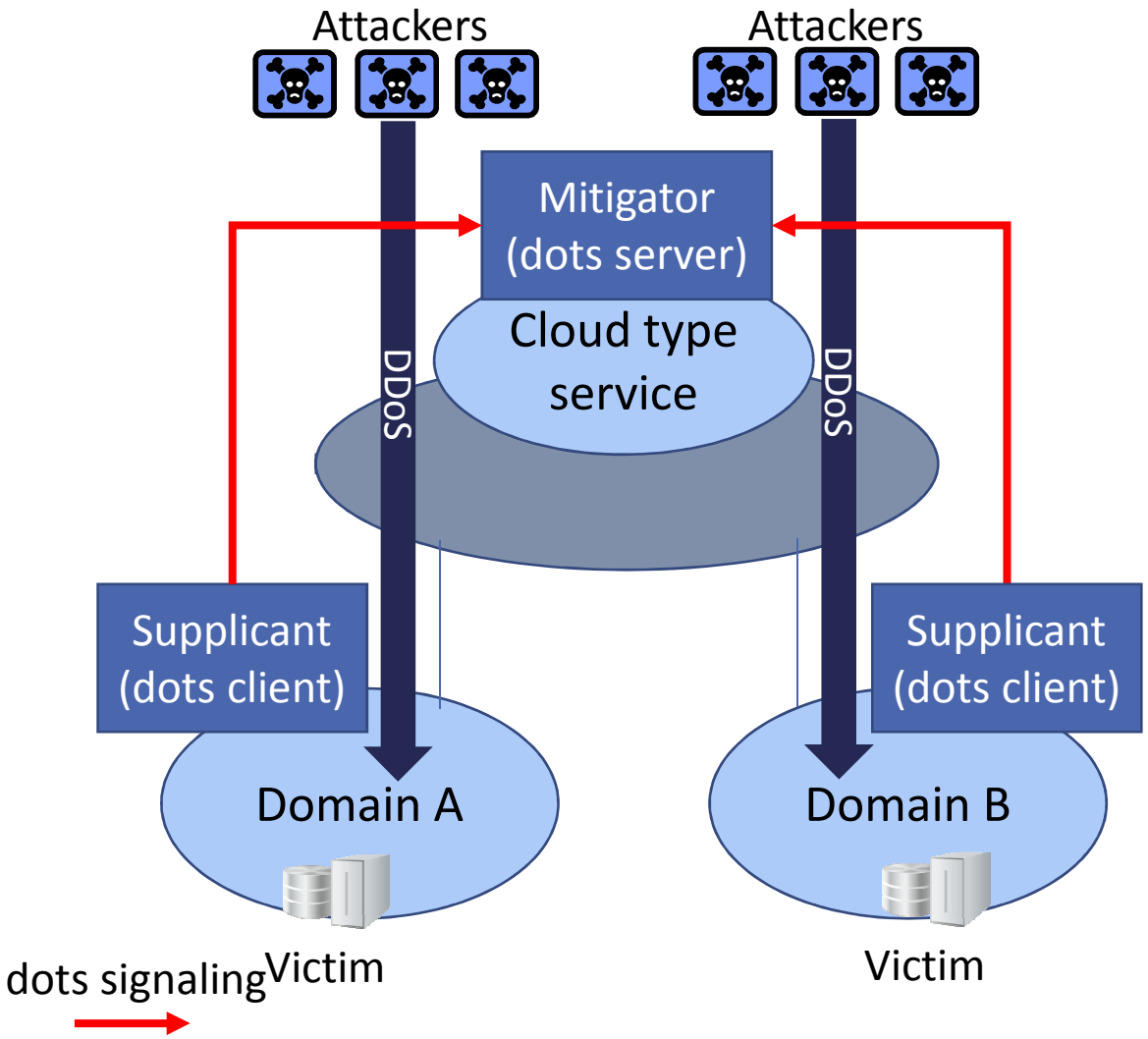



- one supplicant
- multi mitigators

- The common signaling protocol can protect a service in one-stop by protecting both links connected to different domain.

発表時スライド

# Inter-domain usecase2: Cloud model

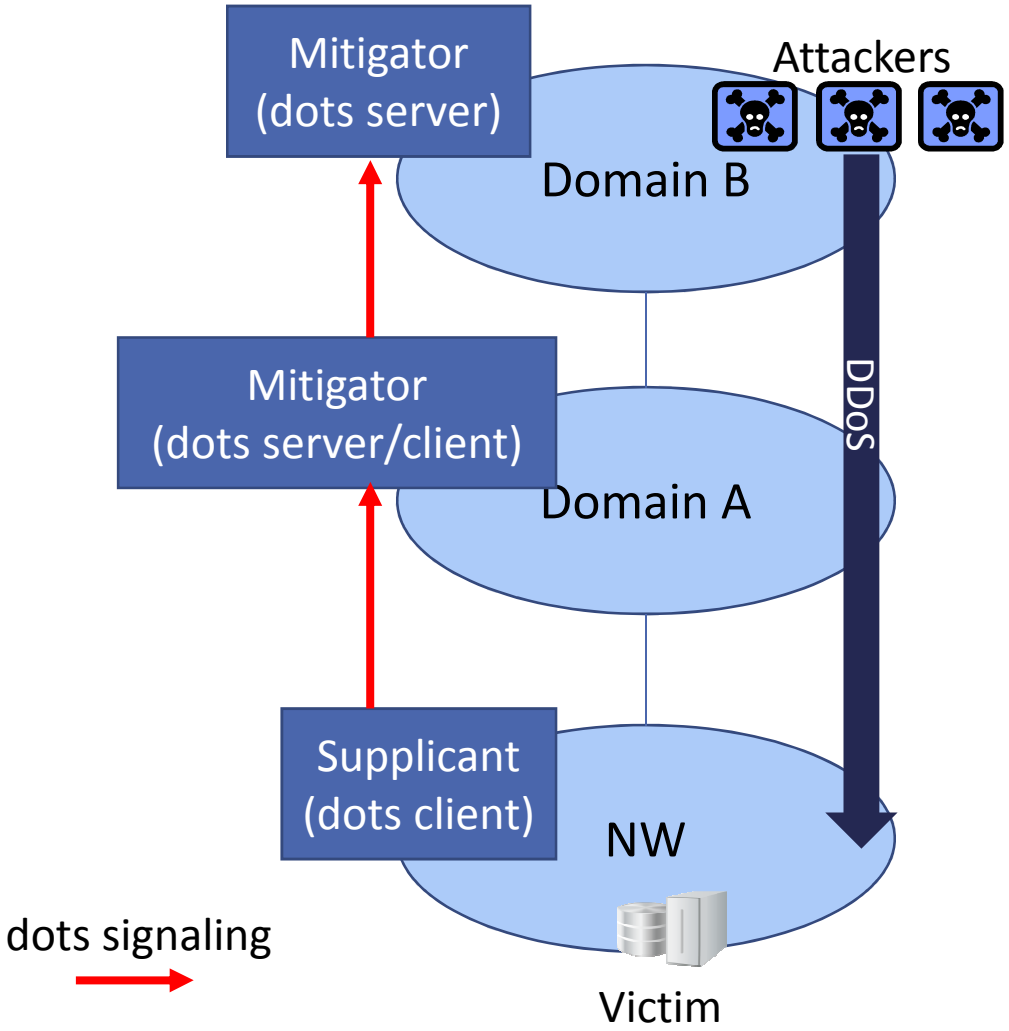



- multi supplicants
- one mitigator

- Cloud type of DDoS mitigation service provides common signaling interface, so any services in different domain can use the mitigator.

発表時スライド

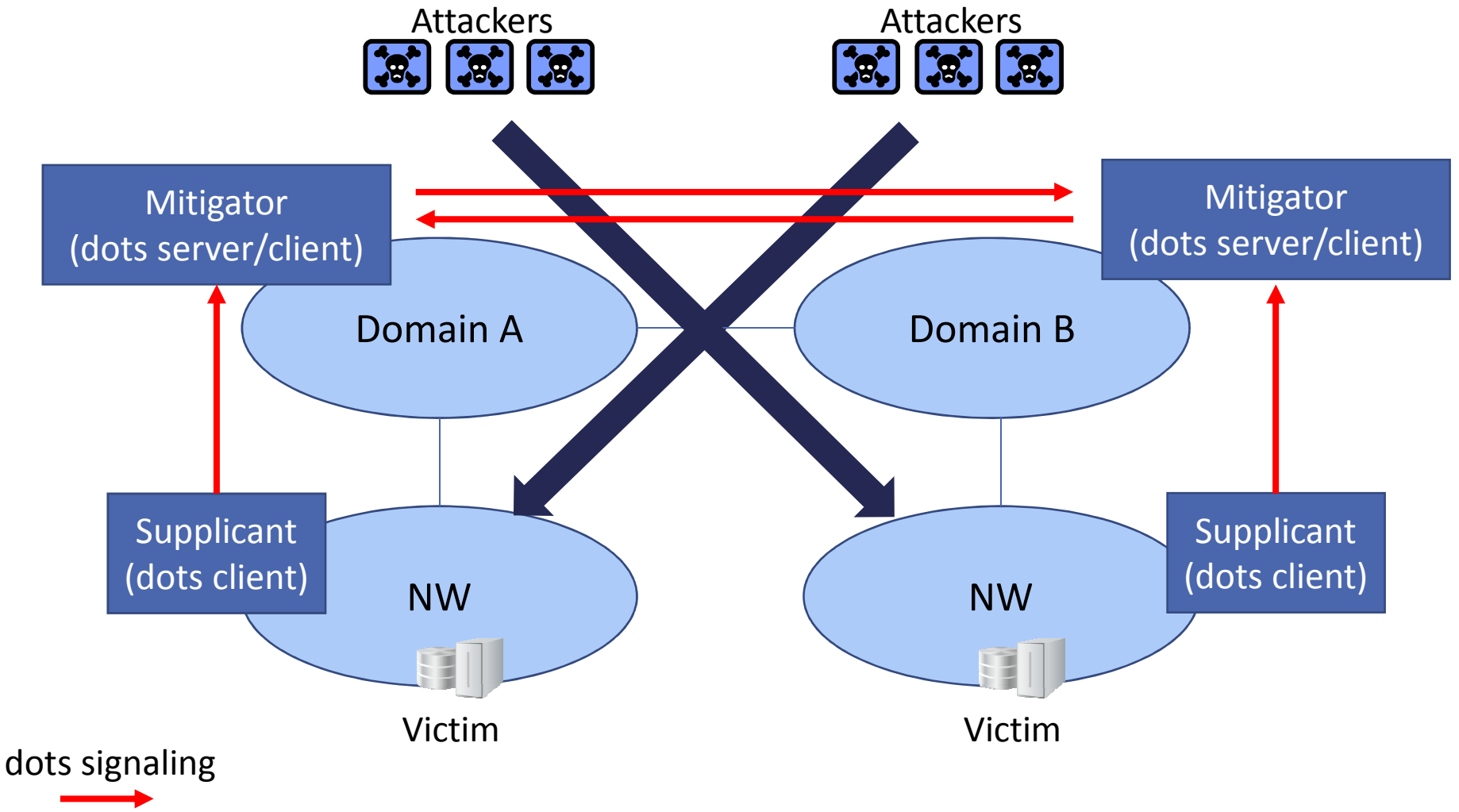
# Inter-domain usecase3: Delegation model




- a mitigator can be supplicant and vice versa.
- The mitigator in a domain can delegate the burden of protection to other domains by dots signaling.

発表時スライド

# Cooperative DDoS Mitigation with DOTS Signaling



# ユースケースに関する議論

- inter-domain-usecasesドラフトに関して
  - 用語の統一を十分にケアしてほしい
  - WGドラフトに組み込むことができるので検討してほしい
    - ✓ WGとしては一つのユースケースドラフトを目指す
    - ✓ 個人的には、単純なマージには難しさを感じている
- dots WGとして、どこまでがdotsのスコープなのか、というコンセンサスあるとは言い切れない
  - Clarifyの質問が多数
- ユースケースのあとは、シグナリング部分の、スキーマとデータモデルに注力する予定

# リクワイヤメントに関する議論

- 00versionのWGドラフト
  - draft-ietf-dots-requirements-00

- シグナリングチャンネルに対する要求事項の議論が紛糾
  - 攻撃されている間は回線が輻輳しているのではないか、という前提
  - 最初のCharterではIPFIXが例示されているが、IPFIX一択ではない
  - 既存のプロトコルを再利用する
    - ✓ tsv WGに対して、どのプロトコルが適しているか質問

- Requirementsに関して、IETF94が開催されるまではMLの流量が少なかったが、一部のメンバが集中して書き上げた状態であったため、IETF94では意図を明確化(確認)する質問が集中
  - IETF期間中にMLでRequirementsに関する議論が活発化
  - 11月中旬まで続いて、今はひとまず沈静

# まとめ

- Usecaseドラフト
- Requirementドラフト
  - WGとして一つにまとめる
  - 用語の整理の重要性
  - 前提のコンセンサス

## 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

- スキーマやデータモデルの定義については、オペレータからの意見が必要とされる
  - ベンダロックインの回避
  - 使える実装にできるかが重要
    - ✓ 既存のインプリの共有も