IETF100報告会
DOTS WG + Hackathon

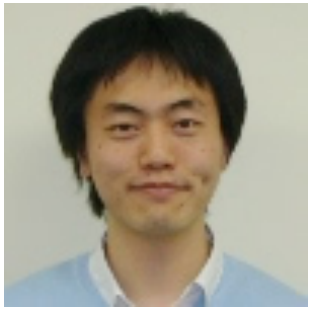
2017.12.15

Kaname Nishizuka@NTT Communications
@__kaname__

NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

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
- メインフィールド
  - トラフィック分析
  - DDoS対策ソリューション
  - IPv4枯渇対策関連技術
- IETF提案活動
  - DOTS WG
- JPNIC「IPv6教育専門家チーム」



NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

IETF100@シンガポール
DOTS 関連報告

3

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～)
- 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

IETF100におけるDOTS関連進捗まとめ

☺よかった点

- IETFハッカソンにおいて、OSS実装(go-dots)とベンダ実装(NCC)の間で最初の相互接続試験が実施された
  - シグナルチャンネルについて、実際に実装間で通信ができる(=DDoS攻撃を防御するアクションができる)ことが確認できた
  - 試験時に問題となった部分は、仕様への要求事項として、WGのミーティングにてフィードバックされ、反映された
- プロトコルへの要求事項(requirement)をまとめたドラフトがWGLCとなった(12/8)
  - これは、dots WGとしてWGLCとなった最初のドラフトである
- プロトコル仕様に関する詰めの議論が、IETF100以降もML上で積極的に交わされている

☹悪かった点

- DOTS WGの参加者が前回より少なかった

DOTS WG ミーティング – 11/14

Tuesday, November 14, 2017
13:30-15:30, Afternoon session I
Room: Olivia

Co-Chairs: Roman Danyliw and Tobias Gondrom

1. Note well, logistics and introduction (chairs, 5 min)

2. Use Case Discussion (15 min)
  - draft-ietf-dots-use-cases-08 (Roland Dobbins*, 10 minutes)
  - Use case discussion (5 min)

3. Requirements Discussion (15 min)
  - draft-ietf-dots-requirements-07 (Andrew Mortensen*, 10 minutes)
  - Requirements discussion (5 min)

4. Architecture Discussion (25 min)
  - draft-ietf-dots-architecture-05 (Andrew Mortensen*, 10 min)
  - draft-boucadair-dots-multihoming-02 (Mohamed Boucadair*, 10 min)
  - Additional architecture discussion (5 min)

5. Protocol Discussion (55 min)
  - Hackathon activity report (Kaname Nishizuka, 15 min)
  - draft-ietf-dots-signal-channel-07 (Mohamed Boucadair*, 30 min)
    draft-ietf-dots-data-channel-07
  - draft-boucadair-dots-server-discovery-03 (Mohamed Boucadair*, 10 min)

6. Closing (chairs, 5 min)

* remote presentation

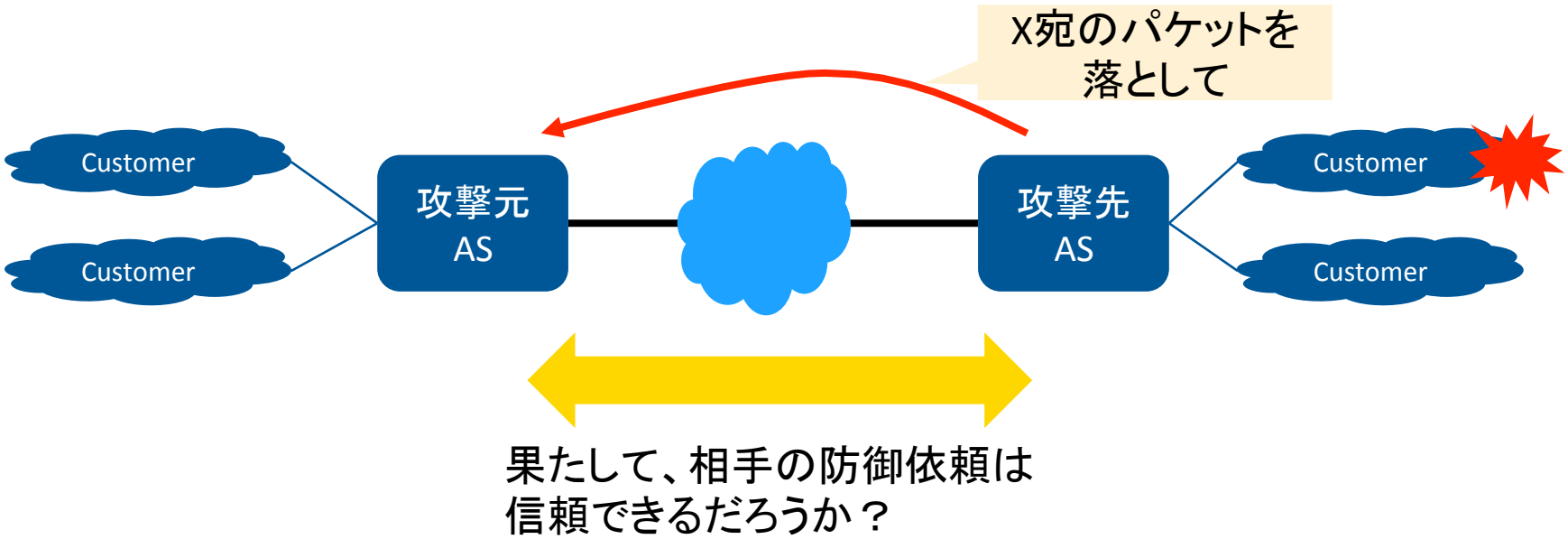
リモート発表が多かった
(デザインチームミーティングも
開催されなかった)

ユースケースドラフト

- draft-ietf-dots-use-cases-08
  - ユースケースの筆者同士で、編集の主導権の綱引きが継続
    - ✓ 一方は、一つのユースケースを詳細に記述したい
    - ✓ 他方は、網羅的にユースケースを列挙したい
  - 上記の理由により、内容に整合性が失われてしまっている状況でWGLCにはまだ至っていない

(少し報告から離れますが) DOTSの利用シーンについて

■ 防御依頼と相互信頼



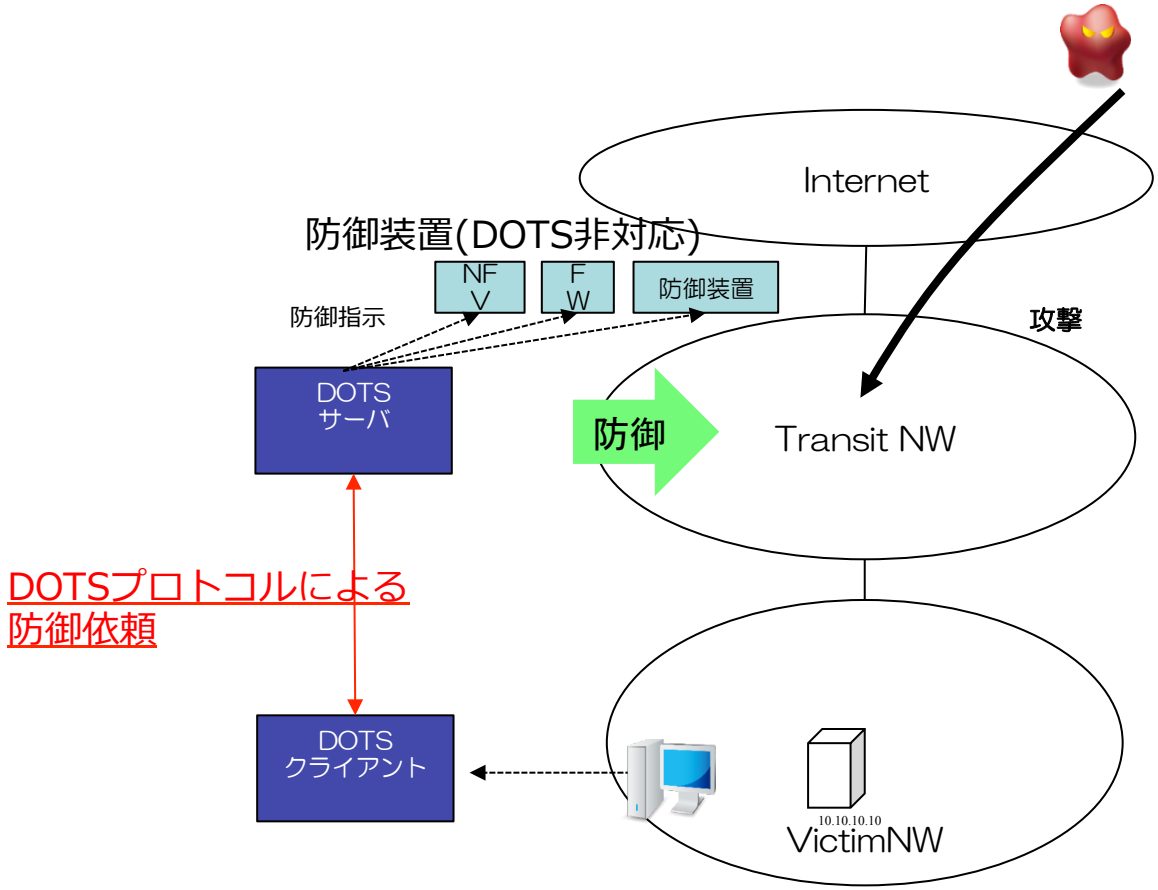
■ **パケットフィルタアウトローシング**と**セキュリティオートメーション**を、**相互信頼のもと**で実現する技術として、DOTSプロトコルが注目されている

DOTSプロトコルの動作とメリット

- DOTSプロトコルの動き方
  - 利用者側のDOTSクライアントから提供者側のDOTSサーバに対して、攻撃を受けているIPアドレスなどの情報とともに防御を依頼
  - 依頼を受けたDOTSサーバ側は、認証および防御依頼のバリデーションを実施した上で、DDoS対策を実施
- DOTSプロトコルのメリット
  1. 人間を介さない防御受付のインタフェースが規定されることで、DDoS対策の自動化が可能になる
  2. 複数の対策事業者に対して共通のプロトコルで防御依頼をすることができるようになる
  3. 別の対策事業者に防御依頼をするような事業者間連携を実現できる

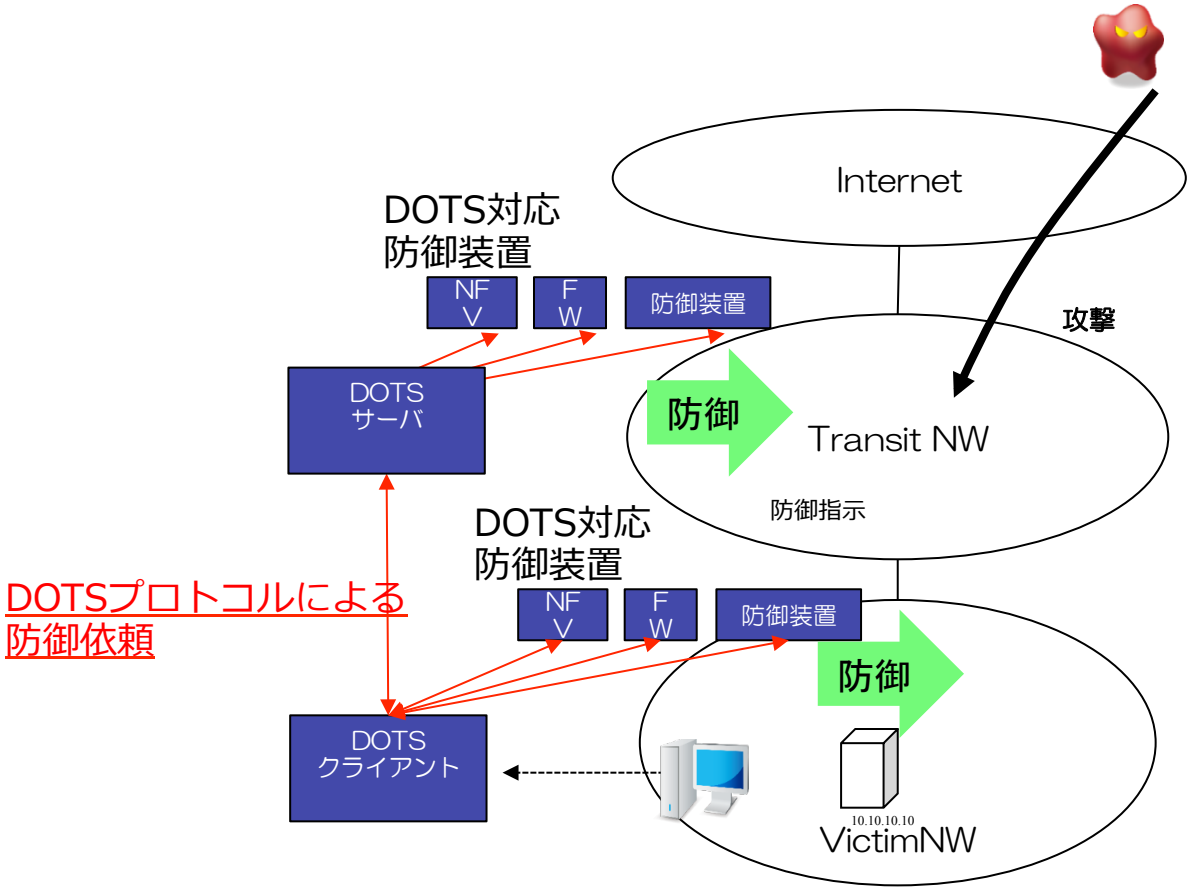
DOTS利用シーン その1

■ 人間を介さない防御受付インタフェースによるDDoS対策自動化



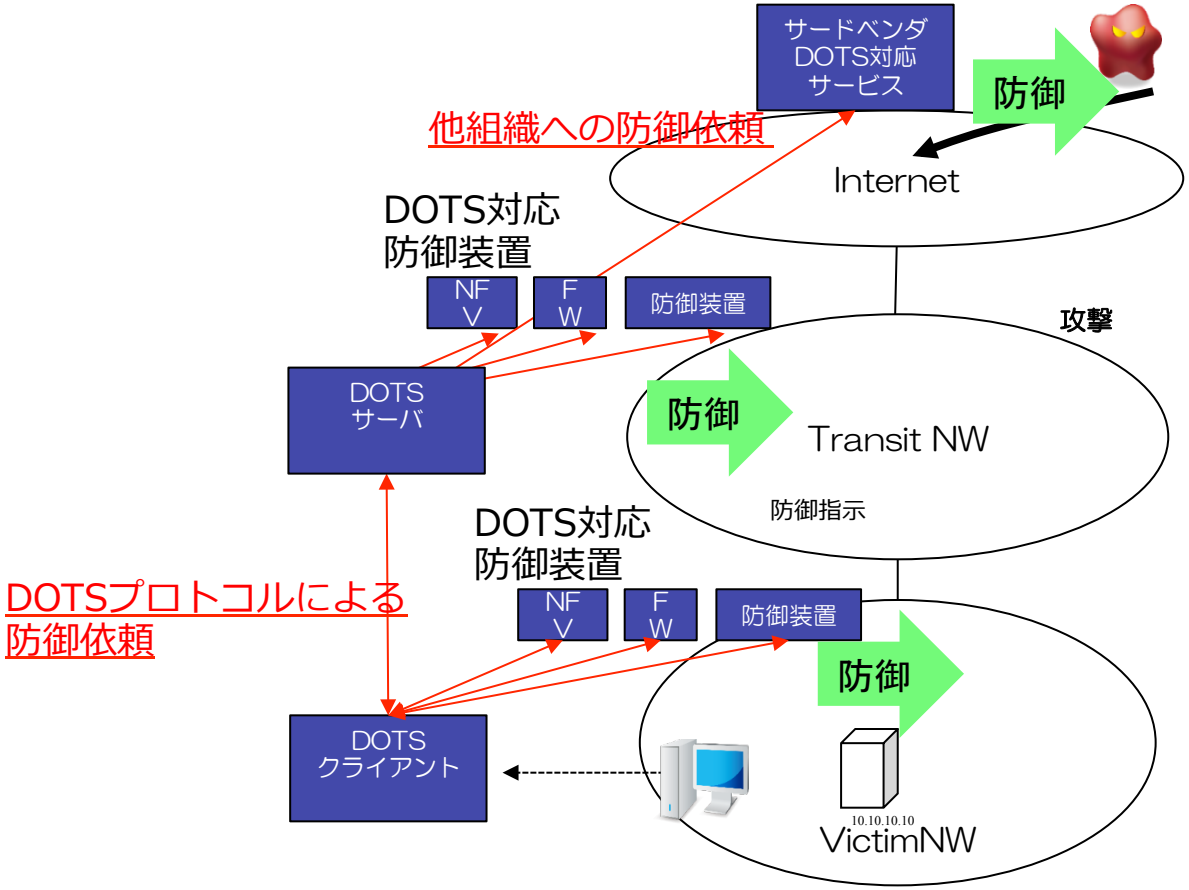
DOTS利用シーン その2

■ 防御装置(DOTS対応)への防御依頼の共通化



DOTS利用シーン その3

■ キャパシティオーバの際に別の対策事業者に防御依頼をするような事業者間連携が実現できる



ユースケースドラフト(に戻って)

- ユースケースドラフトでは、上記で紹介した利用シーンに加えて、以下の点が考慮されている
- 様々なDOTSクライアントのパターン
  - DDoS対策アプライアンス装置, DDoS検知システム(flow collectorなど), CPE, サーバアプリケーション, 運用者のモバイル端末
- 様々な組織間の関係性
  - 組織内で完結するケース(Intra-organization/domain)
  - 組織間のケース(Inter-organization/domain)
    - ✓ 複数の上流組織が存在する場合
    - ✓ 防御依頼がカスケードされる場合

リクワイヤメントドラフト

- DOTSプロトコルに対する要求事項を列挙
- issueはだいぶ片付けられた
  - 残りの issue
    - ✓ NAT 越えに関する記述
    - ✓ ACL が競合したときに順番に関する記述

- 記述を整理した形で、12/8にWGLCに

アーキテクチャドラフト

- DOTSのアーキテクチャの概要を記述
  - 内容も充実しており順調
  - 更新の頻度が低いせいか、今回の会場では読んでいる人が少数であったため、WGLCは見送られた
    - ✓ 十分WGLCの完成度はあると思うので残念…

IETF100@シンガポール
ハッカソン関連報告

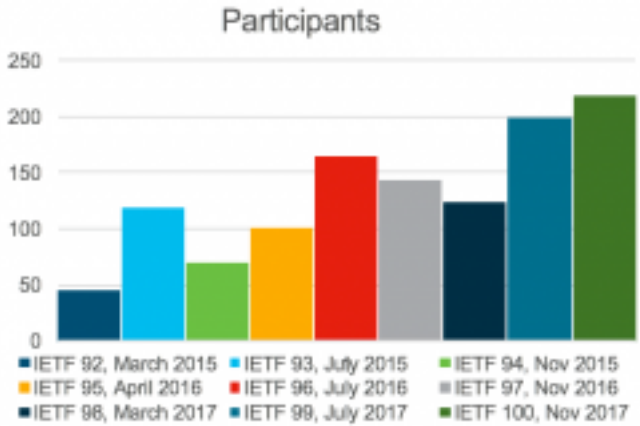
16

IETF100ハッカソン

- IETF100 ハッカソン
  - 本会議の前の土日に開催
  - 200人以上の参加者(IETF100参加者の約22%)
  - IETF技術領域における20のプロジェクトが参加

IETF92

IETF100



ハッカソンイベントの発展

■ ハッカソンイベントの発展
- 今回からついに公式イベントに(IETFの開催期間が土曜日からになった)
- 今後、スポンサーである Cisco Devnet の個別イベントではなく、IETFとしてサポートしていく
- 木曜日には、Cisco D.Ward氏による” Topic: 3 years on: Open Standards, Open Source, Open Loop” というタイトルの講演があり、IETFのプロセスを構成する重要な要素として、IETFハッカソンへの期待が語られた

■ ハッカソンへの参加の仕方や、ハッカソン中の流れは、前回IETF99報告会資料をぜひご参照ください

ハッカソンへの参加経緯

- IETF99において、DOTSプロトコル実装(go-dots)の公開(OSS化)と合わせて、実装の改善をテーマに初参加
  - ドラフト版の仕様を実際に実装し、プロトコルとして有効に動くことを証明
    - ✓ 実際に動くことを示して、標準化のスピードアップを狙う
    - ✓ 問題点は仕様にフィードバック
  - Best Name賞をいただく
- NCCグループが、自前の実装をすでに持っていることを表明
- IETF100においては、NCCグループとの相互接続試験をテーマに参加
  - 異なる実装間でも通信ができ、動作することを証明
    - ✓ 実際に相互接続ができたことを確認
    - ✓ 問題点は仕様にフィードバック
  - Best Open Source Project賞をいただく

IETFハッカソン – IETF100 受賞プロジェクト

- Best Overall：DNS
- Best Input for the Scotch BoF：IPv4-IPv6 Transition Technology Interop and NAT64 testing
- Best Student Project：I2NSF
- Best Long-Term Work: YANG/NETCONF/RESTCONF
- Best Remote Participation：TLS
- Best Open Source Project：DOTS Interop
- Best Cross Area Work: SACM
- Best Interoperability Testing: QUIC

DOTS
First Interoperability Test

IETF 100 Hackathon Report

Kaname Nishizuka/NTT Communications
Jon Shallow/NCC Group
Liang Xia/Huawei

DOTS is now working!

- DOTS WG is aiming to make it standardized in this year
- Now we have several individual implementations
  - go-dots (open-sourced project) from NTT
  - NCC Group's proprietary implementation
- This first interoperability test at the hackathon is a giant step for proving it works.

What happened in the Hackathon

- 3 active projects with 7 participants
  - include 3 remotely from Tokyo, London, Nanjing
- 3 Projects are:

1. First Interoperability test of 2 individual implementations
2. Adding new features and extensions to the open-sourced implementation
3. (Integration with a detection system of Mirai botnet)

We won an award!

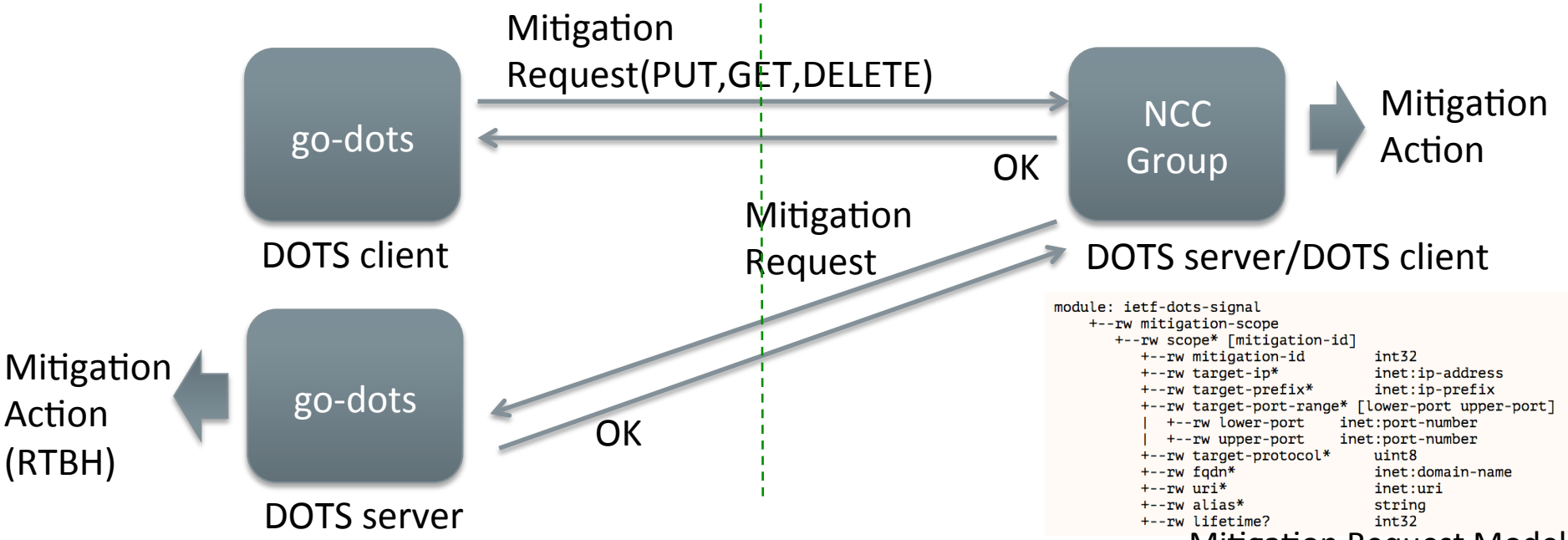
- Best Open Source Project

1. First Interoperability test of 2 individual implementations
   - go-dots (open-sourced project) from NTT
     - Kaname Nishizuka, Takahiko Nagata(Remote)
   - NCC Group's proprietary implementation
     - Jon Shallow(Remote)

Result of the Interop Test

Purpose: Check interoperability of the messages on the signal channel							
			Interop Testing (client -> server)		Internal Testing		
Item #	Messages	CoAP Method	go-dots -> ncc	ncc -> go-dots	ncc	go-dots(ntt)	huawei
1	Mitigation Request	PUT	✅	✅	✅	✅	✅
2	Mitigation Request Withdraw	DELETE	✅	⚠	✅	✅	✅
3	Mitigation Request Status	GET	✅	⚠	✅	✅	✅
4	Mitigation Request Status All	GET	✅	⚠	✅	✅	✅
5	Mitigation Status Notify	observe	-	-	✅	-	-
6	Efficacy Update	PUT	-	-	✅	-	✅
7	Session Configuration	PUT	✅	⚠	✅	✅	✅
8	Session Configuration Delete	DELETE	⚠	⚠	✅	✅	✅
9	Session Configuration Retrieve	GET	✅	⚠	✅	✅	✅
10	Heartbeat	COAP ping	-	-	✅	-	-

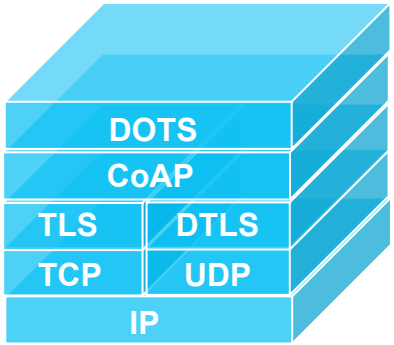
What we proved in the Interop




```
module: ietf-dots-signal
    +--rw mitigation-scope
       +--rw scope* [mitigation-id]
          +--rw mitigation-id          int32
          +--rw target-ip*             inet:ip-address
          +--rw target-prefix*         inet:ip-prefix
          +--rw target-port-range* [lower-port upper-port]
          |  +--rw lower-port     inet:port-number
          |  +--rw upper-port     inet:port-number
          +--rw target-protocol*       uint8
          +--rw fqdn*                  inet:domain-name
          +--rw uri*                   inet:uri
          +--rw alias*                 string
          +--rw lifetime?              int32
```

Mitigation Request Model

- We can start and handle a mitigation from each client over DOTS signal−channel (CoAP over DTLS)
- Plus, NCC Group's implementation can act as a DOTS relay (gateway), so we proved that relayed mitigation requests can work over multiple organizations.



DOTS Signal Channel Layers

General Feedback to DOTS WG

- Implementation Experiences
  - For example most of the code modification was related to encode/decode of CoAP mapping
  - there were many implicit specifications we need to figure out and agree on
- Need more description of the content and code
- approx. 60% of the signal-channel spec has been proved to work
  - The rest will be done at/by the next IETF

go-dots Feedback to DOTS WG

- Preparation for the interop test
  - Agree on port number(-06) and URI path(-07)
  - Fixed CBOR mapping
  - Updated data models
- Code Updates during Hackathon
  - Omit empty(NULL) entries in requests
  - Fixed response body
- Test scenarios should be listed and shared
  - to get every patterns of request/response type and see normal/error behavior
  - unintended behavior can be found only by interop

NCC Group Feedback to DOTS WG (Pt 1)

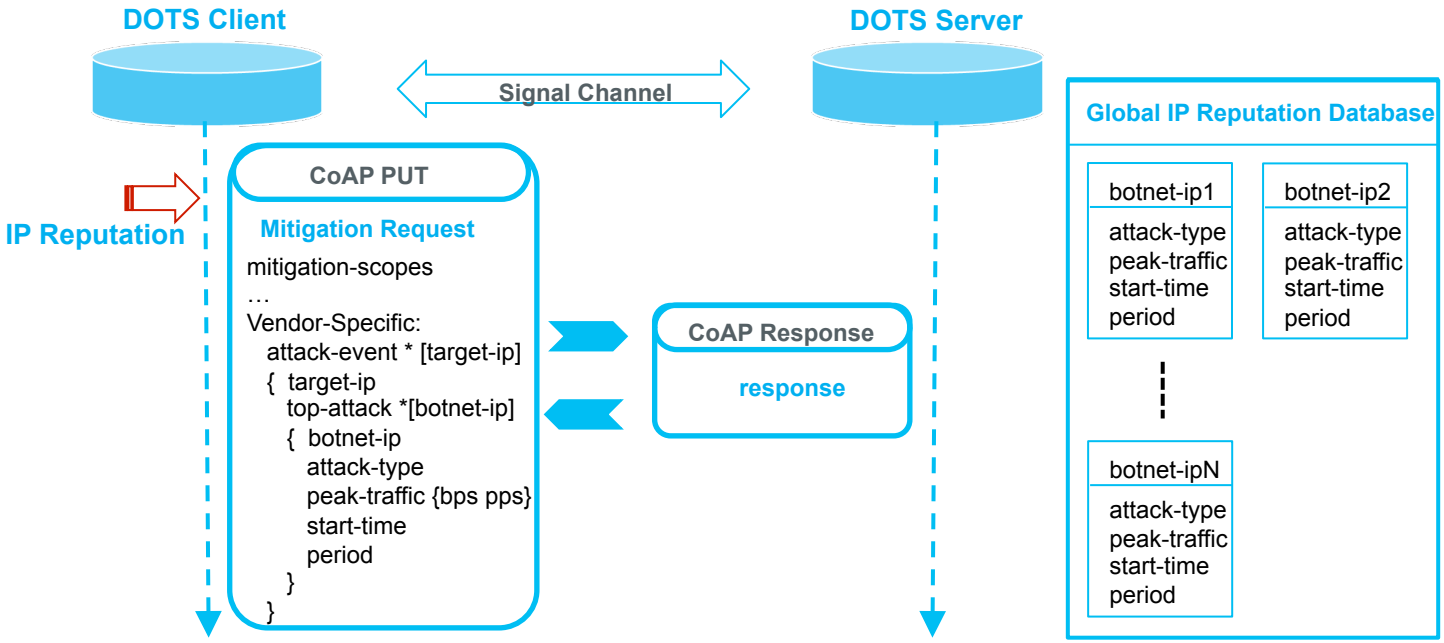
- Code Updates during Hackathon
  - CBOR <-> JSON mapping fixes for NULL entries
  - Remove NULL entries confusion and deleted NULL entries in any response
  - Added support for multiple mitigation requests within a single PUT
- NCC DOTS Client crashing go-dots DOTS server
  - Disabled Signal Configuration requests
  - Disabled Heartbeats
  - Still go-dots server issues handling NCC client requests - to be worked on

NCC Group Feedback to DOTS WG (Pt 2)

- Outstanding NCC Group to be fixed
  - DOTS Client handling bad CoAP Ping responses
  - Support of GET empty requests that are not CBOR encoded
- Questions
  - Should NULL entries be allowed ?
  - Should a NULL entry of type Object be allowed when definition is Array ?
  - What should happen when lifetime = 0 is requested ?
  - Should there be support for multiple mitigation requests within a single PUT ?

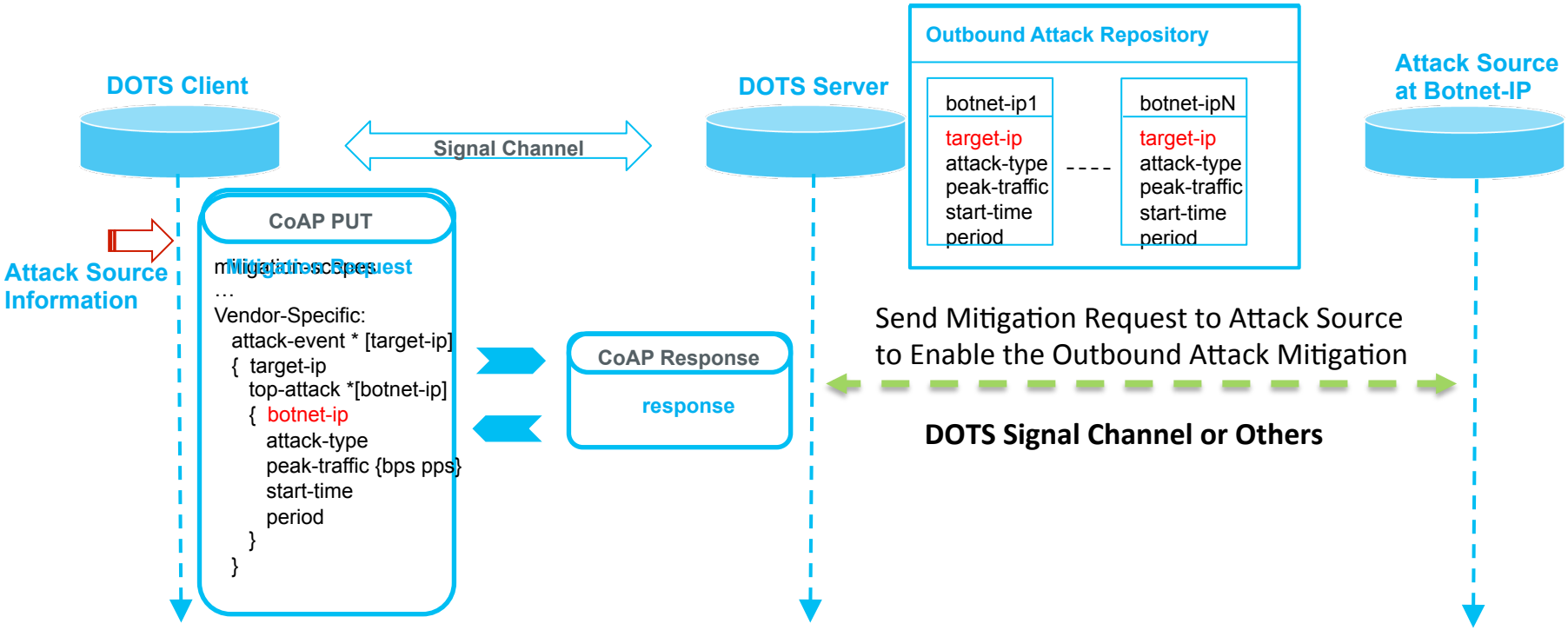
2. Adding new features and extensions to the open-sourced implementation

Using DOTS Vendor-Specific Attributes for Global IP Reputation Sharing




```
mysql> select * from ip_reputation;
+----+-------------+---------------+-------------+-------------+---------------------+---------------+---------------------+---------------------+
| id | customer_id | botnet_ip     | attack_type | peak_traffic | start_time          | attack_period | created             | updated             |
+----+-------------+---------------+-------------+-------------+---------------------+---------------+---------------------+---------------------+
|  1 |           2 | 10.136.157.111 | udp flood   |          100 | 2017-11-3 10:48:56  |          1800 | 2017-11-08 14:54:20 | 2017-11-08 14:54:20 |
|  2 |           2 | 10.136.157.115 | udp flood   |           50 | 2017-11-3 10:49:24  |          1700 | 2017-11-08 14:54:20 | 2017-11-08 14:54:20 |
|  3 |           2 | 10.136.157.112 | tcp flood   |          333 | 2017-10-31 09:51:44 |           444 | 2017-11-08 14:54:20 | 2017-11-08 14:54:20 |
|  4 |           2 | 10.136.157.113 | ack flood   |          156 | 2017-10-31 09:51:43 |           666 | 2017-11-08 14:54:20 | 2017-11-08 14:54:20 |
|  5 |           2 | 10.136.157.114 | syn flood   |          233 | 2017-10-31 09:51:42 |           888 | 2017-11-08 14:54:20 | 2017-11-08 14:54:20 |
+----+-------------+---------------+-------------+-------------+---------------------+---------------+---------------------+---------------------+
5 rows in set (0.00 sec)
```

Using DOTS Vendor-Specific Attributes for Outbound Attack Mitigation




```
mysql> mysql> select * from outbound_attack;
+----+-------------+---------------+---------------+-------------+-------------+---------------------+---------------+---------------------+---------------------+
| id | customer_id | botnet_ip     | target_ip     | attack_type | peak_traffic | start_time          | attack_period | created             | updated             |
+----+-------------+---------------+---------------+-------------+-------------+---------------------+---------------+---------------------+---------------------+
|  1 |           2 | 10.136.157.111 | 192.168.90.101 | udp flood   |          100 | 2017-11-3 10:48:56  |          1800 | 2017-11-08 14:54:20 | 2017-11-08 14:54:20 |
|  2 |           2 | 10.136.157.115 | 192.168.90.101 | udp flood   |           50 | 2017-11-3 10:49:24  |          1700 | 2017-11-08 14:54:20 | 2017-11-08 14:54:20 |
|  3 |           2 | 10.136.157.112 | 192.168.90.102 | tcp flood   |          333 | 2017-10-31 09:51:44 |           444 | 2017-11-08 14:54:21 | 2017-11-08 14:54:21 |
|  4 |           2 | 10.136.157.113 | 192.168.90.103 | ack flood   |          156 | 2017-10-31 09:51:43 |           666 | 2017-11-08 14:54:21 | 2017-11-08 14:54:21 |
|  5 |           2 | 10.136.157.114 | 192.168.90.104 | syn flood   |          233 | 2017-10-31 09:51:42 |           888 | 2017-11-08 14:54:21 | 2017-11-08 14:54:21 |
+----+-------------+---------------+---------------+-------------+-------------+---------------------+---------------+---------------------+---------------------+
5 rows in set (0.00 sec)
```

次回IETF101に向けて

- 発表は好評
  - 問題点はつつがなく仕様に反映された

- チェアが会場に、「早く他にも Interop に出す実装を持ってきてほしい」「早く市場に展開させたい」と発言
  - 以下の2点を気にしていたので、IETF101では改善し、標準化が一気に進むことに期待
    - ✓ 今回はドラフトの著者がほとんどリモートだったこと
    - ✓ 他の主要なWGとのコンフリクトで参加人数が少なかったこと

まとめ

■ ハッカソン出場の意義
- 標準化プロセスを早めることができる
- WGでの発表や懇親会でのデモなど、数多くのアクティビティの機会をゲットできる
- WGでの発言力を強化できる

■ DOTSの進展
- MLにて議論が活性化中
- 我々の戦略として
  - ✓ 引き続きNCCグループとは Interop を実施
  - ✓ さらに Interop に参加する実装を集めたい

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.