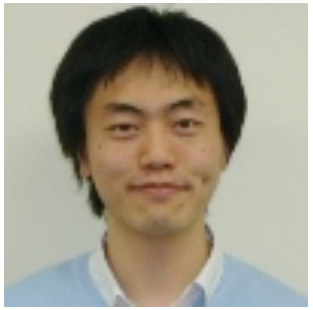
IETF99報告会
Hackathon & DOTS WG

2017.09.01

Kaname Nishizuka@NTT Communications
@__kaname__

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.

IETFハッカソンとは

3

IETFハッカソン – イベントの定着

- 2015年 IETF 92 から開始
  - 今回で8回目
- IETFミーティングの直前の2日間(土日)
- IETFで策定されているプロトコルについて実装を作ることが目的
  - "rough consensus and running code”

- 参加者やプロジェクト数は増加傾向
  - 参加者: 199名(初参加:89名)
  - プロジェクト数: 25

IETFハッカソン – 参加のメリット

- 参加者同士の議論の場
  - 興味のある人同士でグループが作られる
- 相互接続テストの場
- IETF参加者への露出
  - プロトコルやプロジェクトの知名度向上
- WGでの実装報告
- Bits-n-Bites(懇親会) でのデモ権の獲得
- Tシャツ
- 3食+間食 完備
  - スポンサーは Cisco

IETFハッカソン – 風景

[Running Code is King at IETF 99 in Prague]

IETFハッカソン – 参加までの流れ

- MLをサブスクライブ
  - https://www.ietf.org/mailman/listinfo/hackathon
- 次回ハッカソンのページが出来上がる
  - https://ietf.org/hackathon/100-hackathon.html
- 参加登録
  - 参加者と興味のある分野のリストが閲覧可能
- Wikiに情報が集まり始める
  - https://www.ietf.org/registration/MeetingWiki/wiki/100hackathon

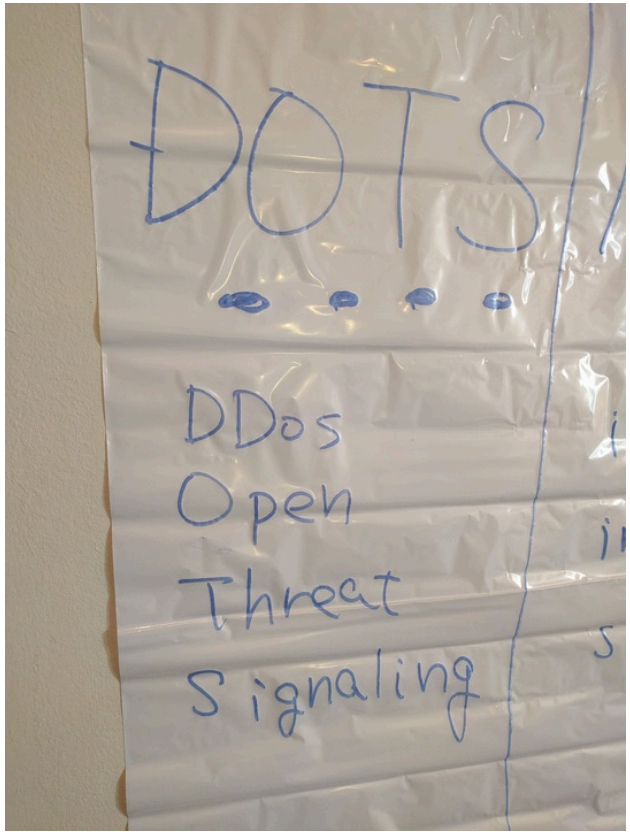
IETFハッカソン – プロジェクトの主催

参加の仕方は2つ

- 既存のプロジェクトに参加する
  - DNS, HTTP 2.0, NETVC, OpenDaylight, ONOS, VPP/FD.io, RiOT, SFC, TLS 1.3, WebRTC, YANG/NETCONF/RESTCONF
- 自らプロジェクトを主催する=Champion になる
  - Wikiを編集して、プロジェクトを追加
  - MLにプロジェクトの簡単な紹介を流す

IETFハッカソン – 初日の動き

- 8:00 – 9:00 早めにきて、ポスターを準備する
- 9:00 なし崩し的になんとなく始まった雰囲気になる
- 9:30頃 キックオフ
  - 2日間のおおよその流れが説明される
- ～21:00 ひたすら開発
  - ポスターを見て、興味を持って話しにきてくれる人の対応がちょくちょく入る



IETFハッカソン – 2日目の動き

- 9:00 開始
- 13:30 作業終了のアナウンス
  - プレゼンの準備をするように言われる
  - 資料は github にて収集
- 14:00 プレゼンテーション
  - プロジェクトあたり3分程度
  - ジャッジから質問される
    - ✓ 何人がプロジェクトに参加していたか
    - ✓ 実際にこの2日間で達成したことは何か
    - ✓ WGはどこで、標準化のステータスはどのくらいか
- 15:30 結果発表・表彰

発表の様子

IETFハッカソン – IETF99 受賞プロジェクト

- Best New Work - HTTP error code 451
- Best University Work - Interface to Network Security Functions (I2NSF) Framework
- “NEAT”est Work - NEAT/TAPS
- Best Interop Work – QUIC Interop
- Best Continuing Work - SCHC implementation and test SCTP
- Best Name - Waiting for go-dots
- Best Overall - SDN Apps for management of microwave radio link via IETF YANG Data Model

IETFハッカソン – プロジェクト一部紹介

- Best New Work - HTTP error code 451
  - クローラ(js)とコレクタを作る
  - 451を返すWordpressプラグインを作る
  - 451を解釈するブラウザプラグインを作る


```
$ node index.js --mode reddit http://redditlist.com/nsfw

{"date":"2017-07-16T11:45:41.273Z","creator":"block-crawler","version":"0.1","u
rl":"http://reddit.com/r/twinks","status":451,"statusText":"Unavailable For
Legal Reasons","blockedBy":{"rel":"blocked-by","url":"https://reddit.com"}}
```

IETFハッカソン – プロジェクト一部紹介

- Best Interop Work – QUIC Interop
  - First Implementation の相互接続試験

client ↓ | server →	Minq	Mozquic	Quicly	Quant	ngtcp2	NGINX+ngtcp2	mvfst
Minq	HDC	HDC	HD	H	H		
Mozquic	HDC	HDC	HD	H		H	
Quicly	HD		HD	H	H		
Quant	H	H	H	H(D)C			
ngtcp2	H		H		HC	H	
mvfst							NONE
	Legend:						
	self-test	interop	known broken	unknown	N/A		
To Test:	H = Handshake						
	D = Stream Data (encrypted)						
	C = Close						

Plus 1 new issue for the Working Group and many editorial clarifications

IETFハッカソン – 日本からの現地参加

- MILE
  - Managed Incident Lightweight Exchange (MILE) の実装を行う
    - ✓ NICT:高橋健志氏,鈴木未央氏
- Best Name - Waiting for go-dots
  - DDoS Open Threat Signaling(DOTS) の実装を行う
    - ✓ 私と株式会社レピダム:岡田耕司氏
  - ハッカソンに合わせて、PoC開発したソフトをOSSとして公開し、現地で改良
  - だ洒落で、ベストネーム賞をいただく…

IETFハッカソン – デモ

- 木曜日に開催される懇親会にてデモブースを持つ機会が得られる
  - スペースは限られているため、早いもの勝ち

IETF99@プラハ
DOTS 関連報告

17

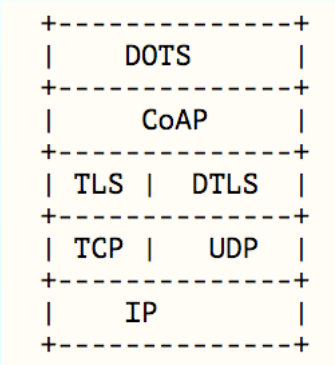
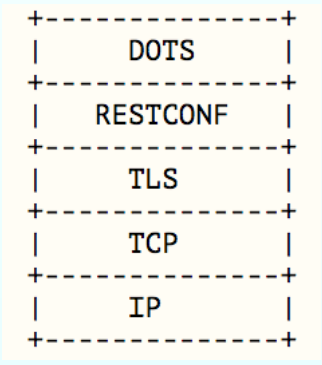
dots WG

- **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

DOTS プロトコルスタック

	Signal Channel	Data Channel
スタック		
アプリケーション	CoAP	RESTCONF
セキュリティ	TLS/DTLS	TLS
トランスポート	TCP/UDP	TCP
目的	(攻撃を受けているときに) 防御を依頼するチャンネル	(攻撃を受けていないときに) 防御をセットアップするチャンネル
クライアント→サーバ	・防御依頼(開始/停止) ・攻撃を受けているIPアドレス・プレフィックス ・防御状況の確認	・ネットワーク情報の登録 ・テレメトリ情報
サーバ→クライアント	・防御状況の報告	・テレメトリ情報

Interim Meeting – 6/8

- DOTS WGでは、IETFミーティングの約1ヶ月前に毎回 Interim Meetingを実施
  - 次のIETFまでに何をすればいいのかが明確化される
  - ドキュメントの精査がこの間に進む

- Virtual Interim Meeting 6/8
  - Usecase Discussion
  - Requirements Discussion
    - ✓ Homenet Usecase の扱いの議論
  - Architecture Discussion
    - ✓ マルチホーム環境の議論
  - Service Discovery
    - ✓ CPEでどのようにDOTS Serverを見つけるか

Design Team Meeting – 7/18

- DOTS WGでは、IETF期間中にデザインチームミーティングを少人数で開催

- デザインチームミーティング 7/18
- ユースケース関連
  - A社の著者が、ドラフトを一つ前の文面に revert したため紛糾
  - 読みやすさと、網羅性の両立が困難
  - 読者をナビゲートするような文面にすべきとなったが、果たして…
- プロトコル関連
  - ハッカソンで見つけた議論すべき点をフィードバック(後述)
  - 事前にこの場で説明することで、他のメンバに議論点の重要性を認識させることができたのが非常に有用だった

DOTS WG ミーティング – 7/20

DDoS Open Threat Signaling (DOTS) WG Agenda

THURSDAY, July 20, 2017
15:50-17:50, Afternoon Session II
Berlin/Brussels

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-07 (Roland Dobbins, 10 minutes)
   - Use case discussion (5 min)

3. Requirements Discussion (15 min)
   - draft-ietf-dots-requirements-06 (Robert Moskowitz, 10 minutes)
   - Requirements discussion (5 min)

4. Architecture Discussion (25 min)
   - draft-ietf-dots-architecture-04 (Nik Teague, 10 min)
   - draft-boucadair-dots-multihoming-01 (Mohamed Boucadair, 10 min)
   - Additional architecture discussion (5 min)

5. Protocol Drafts (55 min)
   - IETF 99 Hackathon Activity (Kaname Nishizuka, 10 min)
   - draft-ietf-dots-signal-channel-02 (Nik Teague, 20 min)
   - draft-ietf-dots-data-channel-02 (Nik Teague, 15 min)
   - draft-boucadair-dots-server-discovery-02 (Mohamed Boucadair, 5 min)
   - draft-francois-dots-ipv6-signal-option-02 (Jer?me Fran?ois, 5 min)

ユースケースドラフト

- 前日のデザインチームミーティングを受け、直前で内容をマージして -07 として提出
  - 直前すぎて読んでいる人が少ないため、議論が深まらず
  - (戦術なのか、天然なのか)
  - github にも反映されておらずドキュメントの編集状況が不透明

- エリアディレクター(AD)からのマージ要請
  - ADとして、Informational な RFC を複数出したくない
    - ✓ 似た内容が含まれていたりして、読む方も編集する方も大変
  - リクワイヤメント/アーキテクチャドラフトとマージしては？
  - これに対しては、2人のチェアが明確にNO！
    - ✓ それぞれのドラフトが独自の有益なコンテンツを含んでいる
    - ✓ これまでの経緯を重視

リクワイヤメントドラフト

■ 新しい参加者からの質問が増加
- そもそもの前提のクラリフィケーションなど
  - ✓ クライアントからの情報と、サーバ側の判断どちらを優先するか
  - ✓ DOTSの仕様は後者
- 参加者層や注目度が上がっている

■ 今後
- 引き続きイシューを受付中
- 近日中に次のバーションに

アーキテクチャドラフト関連

- アーキテクチャドラフト(WGドラフト)
  - 内容も充実しており順調

- マルチホームアーキテクチャドラフト(New)
  - draft-boucadair-dots-multihoming
  - インタリムミーティングで議論が出て、マルチホーム環境について考慮(仕様への重要な改変)が必要かどうかを判断したい
  - 著者は、ありうるマルチホーム環境を列挙
    - ✓ しかし、微に入りすぎていている感あり
  - 結論としてマルチホーム環境にどのような問題があるかが不明瞭のため引き続き議論
    - ✓ 結果がでたら、WGドラフトに吸収されるべき(by Chair)

ハッカソンレポート

■ ハッカソンでの実装結果と、気づきをフィードバック

- 次ページからは発表資料

Go implementation of DOTS

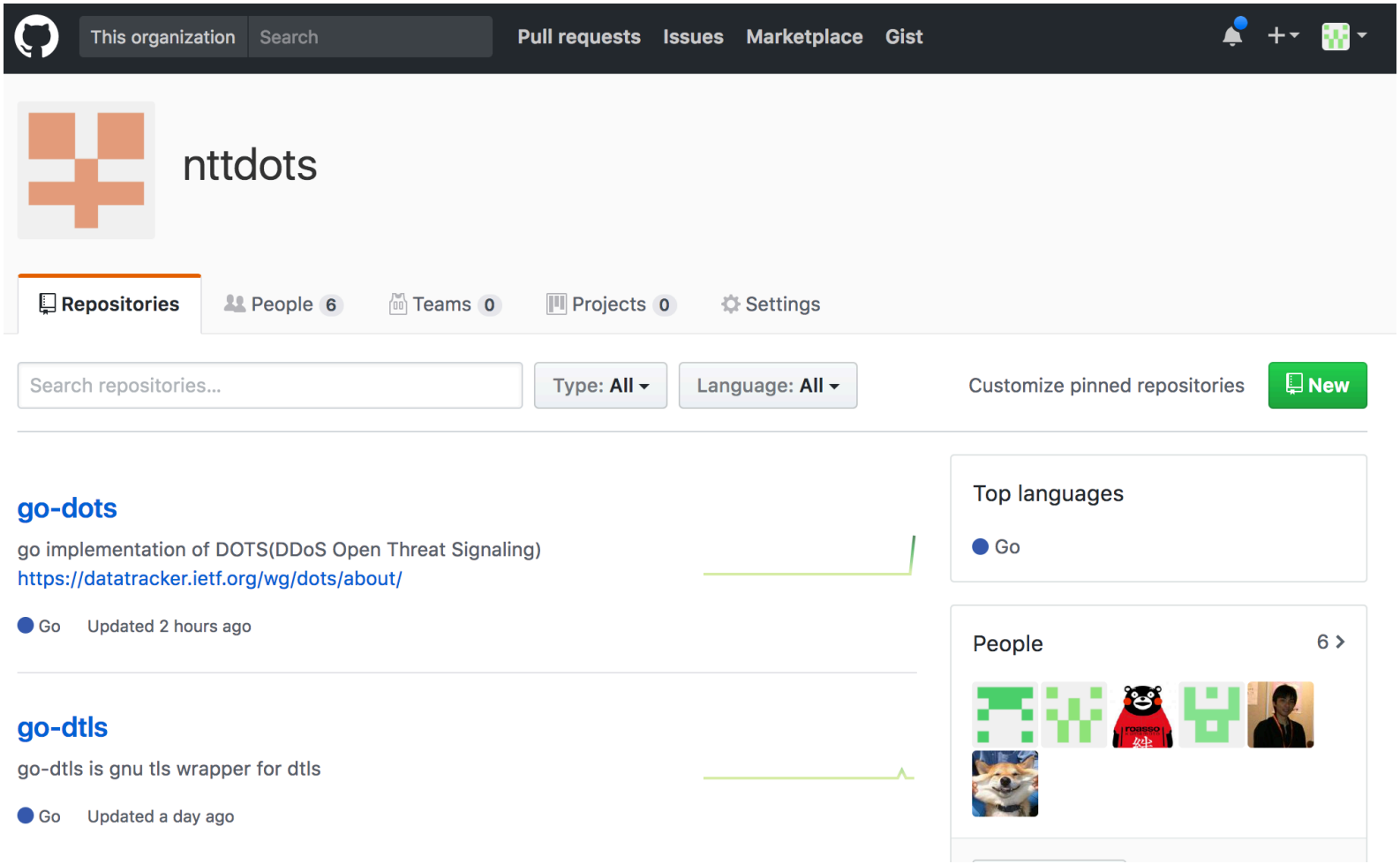
DOTS WG

2017.07.20

Kaname Nishizuka
(NTTCommunications)

We opened the code !!

- https://github.com/nttdots



What was developed in hackathon

- made the code easy to be deployed in various environments
  - made docker-compose files for each services
  - refined configuration part

- clarified the documents
  - for newcomers to this field

Demos and Interests

- made a demonstration of one user scenario
  - on a portable docker environment
  - triggering “blackhole routing” from victim side
- attracted 4 people and showed them demo

We do demo on Bits-n-Bites

- Today: 19:15-21:15
- Prosím, visit us on the site.

Demo: Go implementation of DOTS

Demo scenario:
Enabling DDoS Protection in an upstream network by DOTS protocol

https://github.com/nttdots/go-dots

DOTS is:

- **D**DoS **O**pen **T**hreat **S**ignaling
- Automation and Standardization of signaling for DDoS protection
- "ask for help!" from a victim to an upstream provider
  - inter-organization / including authN and authX in spec

What you can see in this demo:

- A DOTS client sends a mitigation request to a DOTS server over DOTS signal channel.
- The DOTS server receives and validates the request, then starts mitigation by kicking a blocker
- In this demo, the blocker is a gobgp server which triggers "blackhole routing" in a service operator's network

Signal Channel

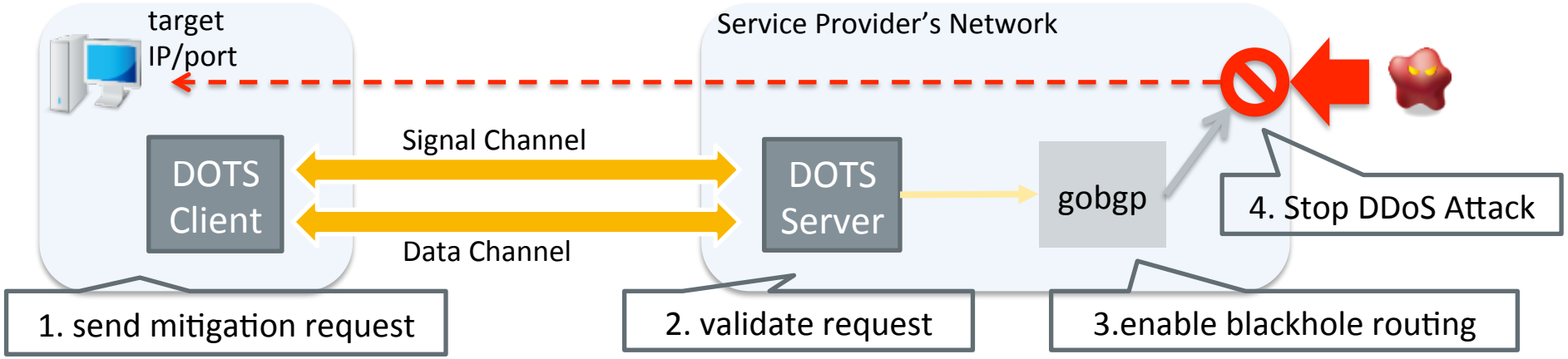
```
+--------------+
|     DOTS     |
+--------------+
|     CoAP     |
+--------------+
| TLS |  DTLS  |
+--------------+
| TCP |   UDP  |
+--------------+
|     IP       |
+--------------+
```

Data Channel

```
+--------------+
|     DOTS     |
+--------------+
|   RESTCONF   |
+--------------+
|     TLS      |
+--------------+
|     TCP      |
+--------------+
|     IP       |
+--------------+
```

Mitigation Request Model

```
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
```



Lessons Learned(1/3)

1. Need more description on specification of mutual authentication
   - (D)TLS based-on client certificate
     - tend to use self-signed certification (in lab)
     - how can we bind the (D)TLS channel and customer (mitigation scope)
     - CN(or SNI) should be used? (it's not clearly documented)
   - what else for mutual authentication

Lessons Learned(2/3)

2. Still searching for good RESTCONF library
   - As an alternative, CoAP/DTLS can be used for data channel
   - but we want to implement it on RESTCONF, if we can.

Lessons Learned(3/3)

3. Zero heartbeat mode should be allowed
   - As a starting point of implementation in lab
   - Also there are several usecases (as discussed in the last IETF meeting)
   - “MUST” in REQ.SIG-003 should be relaxed?

IANA considerations

- need assignment for default port number
  - 4646/udp for signal channel (from draft-mortensen-dots-over-udp)
  - 4647 for data channel?

implementation specific problems

- Traffic data collection
  - traffic information should be returned from DOTS servers
    - incoming traffic / blocked traffic / passed traffic
  - need additional software component to collect those data from network equipment or mitigation boxes
    - very implementation specific but required
- Partially valid request
  - When a mitigation request includes valid scope and invalid scope at the same time, what is the appropriate behavior?
    - reject all? / pass valid request only?

Next Step

- As an OSS,
  - adopt to the various deployment scenario
  - keep going on the implementation of WG drafts and make feedback to the spec

- your feedback is welcome☺

DOTS is getting popular!

- We'd like to do interoperability testing at the next hackathon in IETF100
  - signal channel interop will be the 1st step

次回IETF100に向けて

- 発表は大変好評
- zero heartbeat の件も、リクワイヤメントに反映

- チェアが会場に、次回以降 Interop あるとしたらやりたい人を聞く
  - 5人が挙手
    - ✓ Arbor, Cisco, Huawei, Verisign, Checkpoint

その他のプロトコル関連ドラフト

- シグナル/データチャンネルドラフト(WGドラフト)
  - 順調
- サービスディスカバリ(New)
  - boucadair-dots-server-discovery
  - DHCPを提案
    - ✓ CPEのユースケースで使うのか？
    - ✓ サービスディスカバリ機能をMUSTとすべきではない、とフィードバック
- ipv6 signal option(New)
  - draft-francois-dots-ipv6-signal-option
  - WGドラフトが順調に進む中で、IPv6限定のチャンネルを提案(前は Hop-by-hop オプションの利用を提案)
  - 申し訳ないが筋が悪い

マイルストーン

- 2017年以内に現状のWGアイテムのラストコールを目指す
  - 下記のMilestoneは更新されていないが、11月がターゲットに設定されている

Milestones

Date	Milestone
Dec 2017	Data channel document as proposed standard to WGLC
Dec 2017	Signal channel document as proposed standard to WGLC
Sep 2017	Architecture document to WGLC draft-ietf-dots-architecture
Jul 2017	Use case document to WGLC draft-ietf-dots-use-cases
Jul 2017	Requirements document to WGLC draft-ietf-dots-requirements

各WGアイテムは github にて管理: https://github.com/dotswg

まとめ

- ハッカソン出場の意義
  - 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
  - OSS実装の露出
  - 参加人数/層が増え、注目を集めつつある
  - 今後の Interop に向けて、複数の実装が出てくる見込み