日本でのオープンループ

2018/1/24
JANOG41
NTTコミュニケーションズ 西塚要
kaname@nttv6.jp

自己紹介：

- 西塚要(にしづか かなめ)

- 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の運用サービスを担当。現在は研究開発組織にて、トラフィック分析などISPの課題に関する研究開発に従事。
- メインフィールド
  - DDoS対策
  - トラフィック分析
  - IPv4枯渇対策関連技術

- 社外活動
  - IETF DOTS WG (2015年～)
  - JPNIC「IPv6教育専門家チーム」

標準化のアンチパターン：

go-dots

- 標準化過程と利用者との断絶
  - IETF: 「私、作る人」
  - 運用者: 「僕、使う人」

- 標準化されたプロトコルを誰も使わないアンチパターン
  1. ニーズがないプロトコルを作ってしまった
  2. 不要かつ複雑怪奇な仕様で使いたくない
  3. 利用しにくい他のプロトコルに依存している
     ※利用しにくい=良いライブラリが無いなど
  4. 時期を逸してしまった(すでにプロプライエタリな実装でエコシステムが出来上がった)

今日のテーマ: どちらかといえば運用出身の私自身が、IETFでどのような活動をしているかを紹介

IETFとは

IETF(Internet Engineering Task Force) ：

- インターネット技術の標準仕様(プロトコル)を議論策定する団体
  - 1986年にIABにより設置
  - MLによる議論を中心とし年3回のミーティングを開催
- 代表的なプロトコル
  - IP (RFC791), TCP (RFC793), FTP (RFC 956)…
- RFC (Request for Comments)による仕様公開
  - 現在，RFC8313まで公開
- 特徴
  - “Open”な参加・標準化過程・標準仕様
  - “Rough Consensus, Running Code”を重視

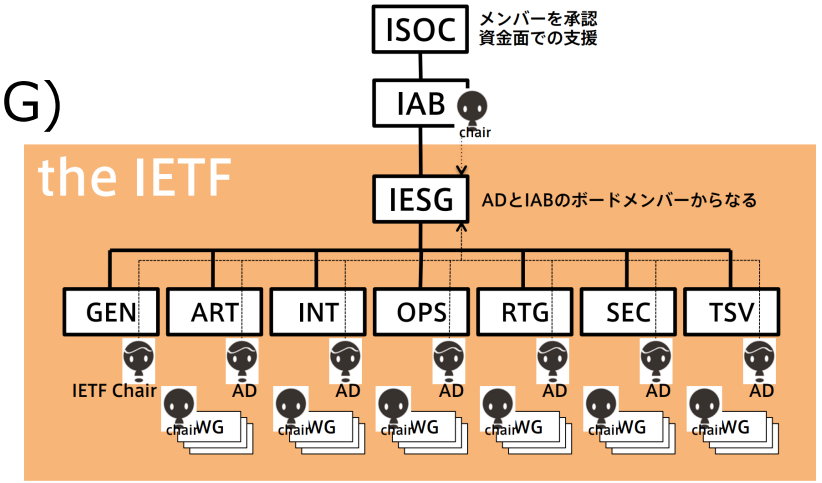
"We reject kings,presidents and voting. We believe in rough consensus and running code"

By David Clark, MIT

IETFミーティングの中身：

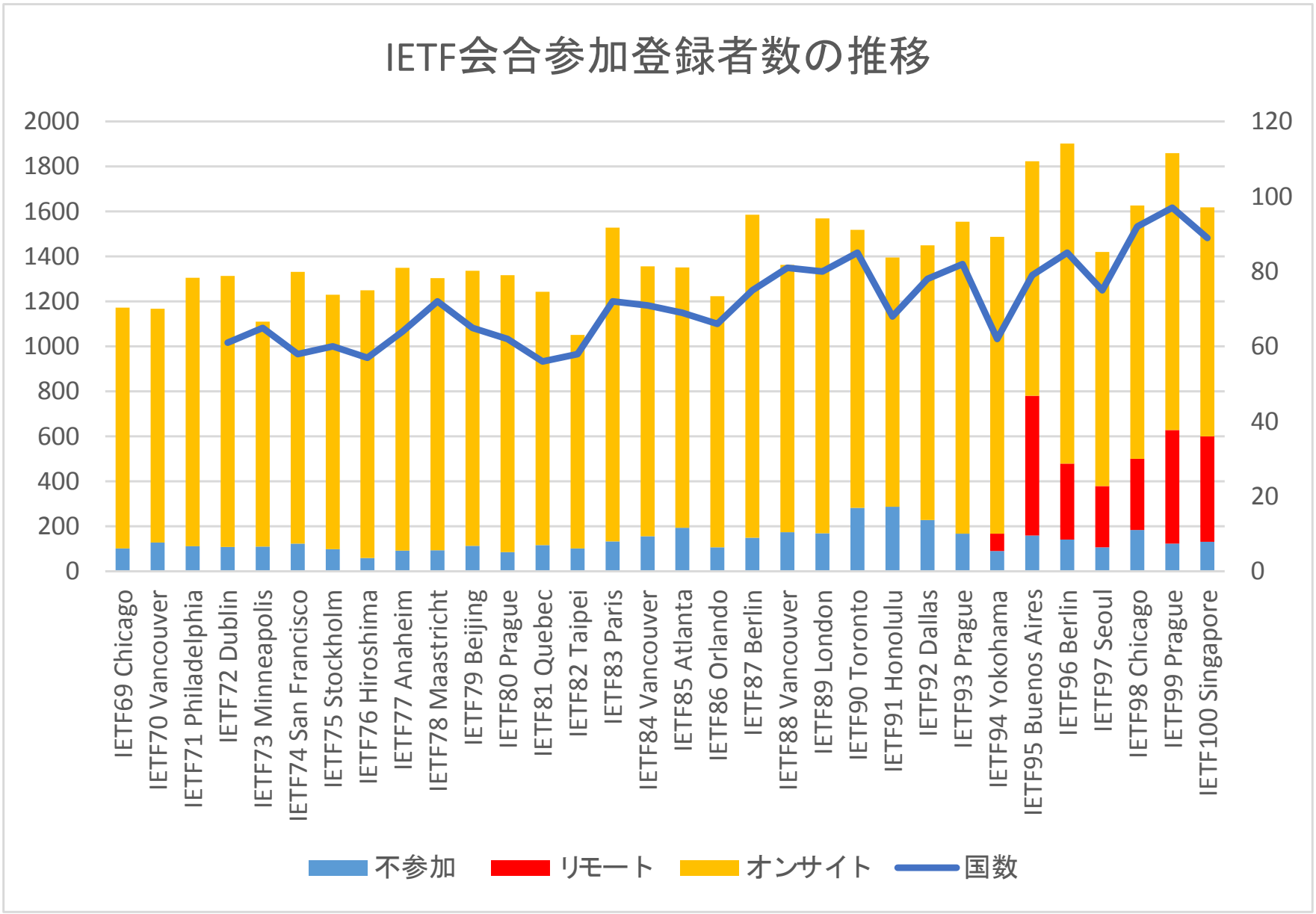
1000から1500人のIETF参加者が集まるミーティング(約1週間)が年に３回開催される

- 公式イベント:
  - Working Groupセッション (約130 WG)
  - Birds of a Feather (BoF) セッション
  - エリア全体セッション
  - IETF全体ミーティング
  - チュートリアル & ランチ セッション
  - Social Event
  - IETFハッカソン
  - 非公開のビジネス会議（例: IAB, IESG, IAOC, NOMCOM）

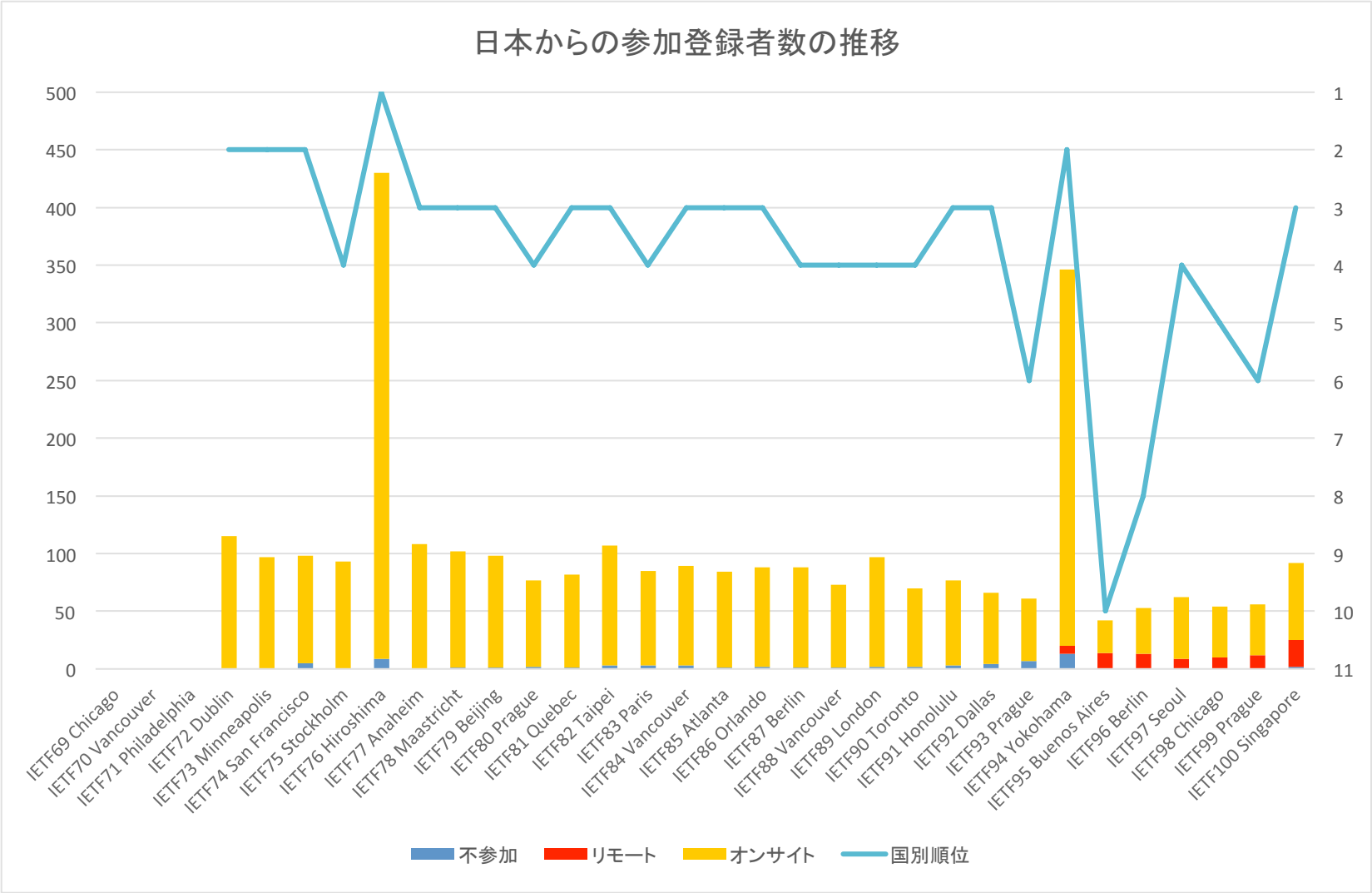


- 非公式イベント:
  - Bar BoF
  - PechaKucha

IETF参加者数：


IETF会合参加登録者数の推移
2000
1800
1600
1400
1200
1000
800
600
400
200
0
120
100
80
60
40
20
0
IETF69 Chicago
IETF70 Vancouver
IETF71 Philadelphia
IETF72 Dublin
IETF73 Minneapolis
IETF74 San Francisco
IETF75 Stockholm
IETF76 Hiroshima
IETF77 Anaheim
IETF78 Maastricht
IETF79 Beijing
IETF80 Prague
IETF81 Quebec
IETF82 Taipei
IETF83 Paris
IETF84 Vancouver
IETF85 Atlanta
IETF86 Orlando
IETF87 Berlin
IETF88 Vancouver
IETF89 London
IETF90 Toronto
IETF91 Honolulu
IETF92 Dallas
IETF93 Prague
IETF94 Yokohama
IETF95 Buenos Aires
IETF96 Berlin
IETF97 Seoul
IETF98 Chicago
IETF99 Prague
IETF100 Singapore
不参加
リモート
オンサイト
国数

IETF参加者数(日本)：


日本からの参加登録者数の推移
500
450
400
350
300
250
200
150
100
50
0
1
2
3
4
5
6
7
8
9
10
11
IETF69 Chicago
IETF70 Vancouver
IETF71 Philadelphia
IETF72 Dublin
IETF73 Minneapolis
IETF74 San Francisco
IETF75 Stockholm
IETF76 Hiroshima
IETF77 Anaheim
IETF78 Maastricht
IETF79 Beijing
IETF80 Prague
IETF81 Quebec
IETF82 Taipei
IETF83 Paris
IETF84 Vancouver
IETF85 Atlanta
IETF86 Orlando
IETF87 Berlin
IETF88 Vancouver
IETF89 London
IETF90 Toronto
IETF91 Honolulu
IETF92 Dallas
IETF93 Prague
IETF94 Yokohama
IETF95 Buenos Aires
IETF96 Berlin
IETF97 Seoul
IETF98 Chicago
IETF99 Prague
IETF100 Singapore
不参加
リモート
オンサイト
国別順位

DOTS WGに関わるまでの経緯

初めてのインターネットドラフト(2013)：

- 総務省 平成24年度「IPv4アドレスの枯渇に伴う情報セキュリティ等の課題への対応に関する実証実験の請負」
  - 実証実験の成果をドラフトにまとめて投稿
  - CGN導入における考慮事項をまとめたドラフト
  - 内容は評価されたが、タイミングが悪かったため自主的にExpire
- Lessons Learned
  - ドラフト投稿はやればできる
  - 内容が技術的な知見にきちんと基づいていれば、議論の場に乗せてくれる
  - 特にオペレータからの意見は貴重とみなされる
  - 受け皿となるWGを持つことが重要

以降、「自分の考えはIETFにドラフト投稿して、作る側に回ってしまえばよい」というマインドに。

DOTS WG立ち上がり(2015) :

- DOTS: DDoS Open Threat Signaling
  - 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標準化する
  - IETF92 BoF → IETF93 WG化

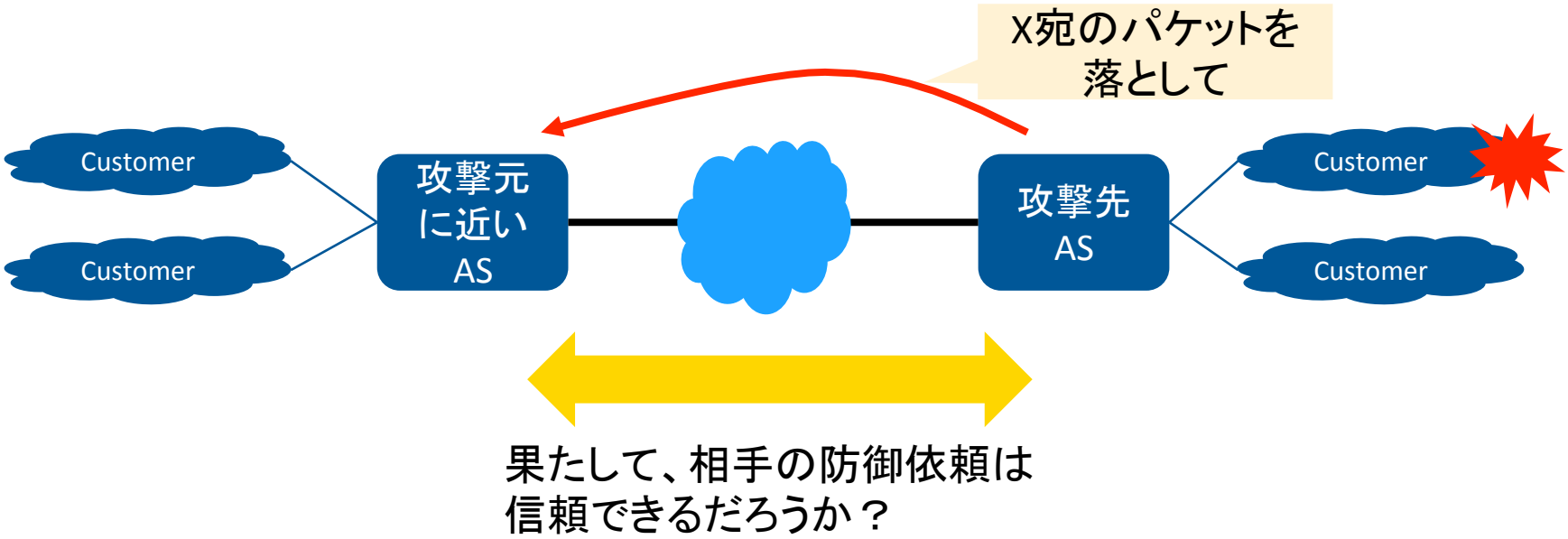
- 最初は、スコープも定まらない状況
  - どのような情報をどのようにやり取りするか、をこれから決める状況

- DDoS対策システムの開発の知見を活かし、スコープを定めるところから議論に入る

DOTSプロトコルとは

DOTSのスコープ：

■ 防御依頼と相互信頼



■ **パケットフィルタアウトソーシング**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プロトコルの動作
  - 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
  - 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
  - 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
  - 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

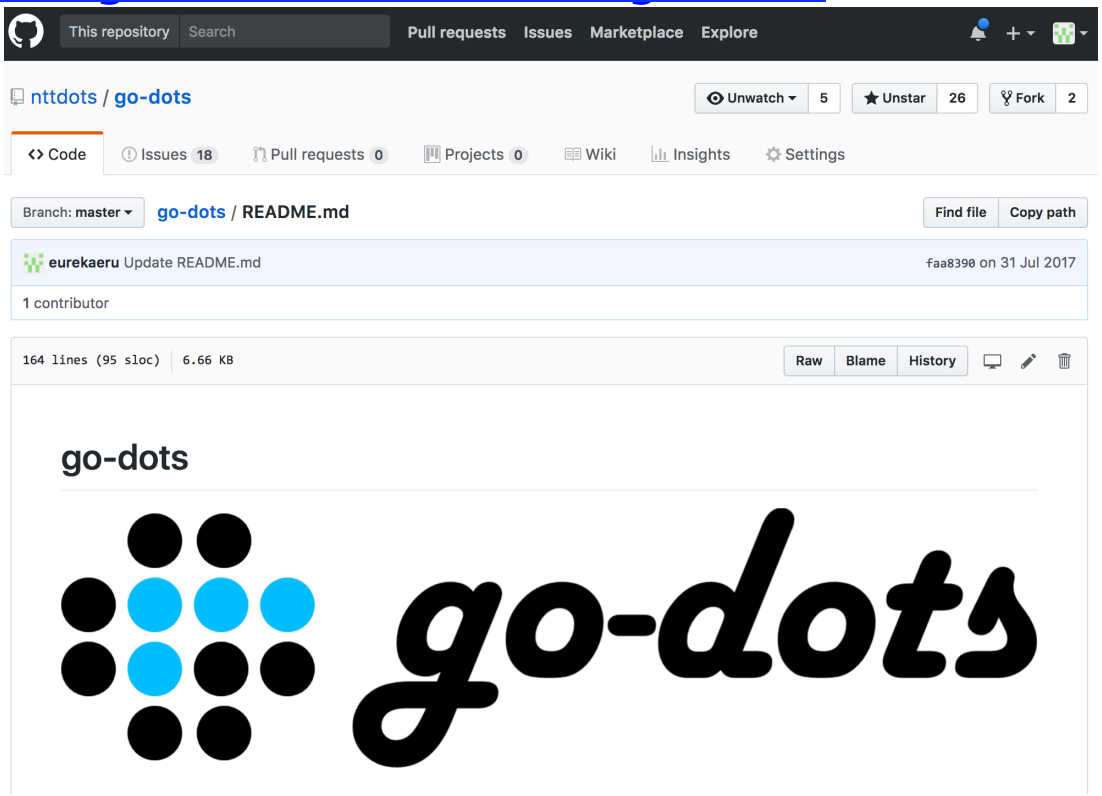
DOTS WGでの活動

DOTS WGでの活動(1/3)：ドラフトの投稿

- 2015年12月: ユースケースドラフトを投稿
  - draft-nishizuka-dots-inter-domain-usecases
  - WGアイテムのユースケースが組織間での防御依頼のユースケースをカバーしていなかったため、スコープを広げるために投稿
  - 後に、WGアイテムにマージ
- 2016年2月: 伝達する情報のモデルのドラフトを投稿
  - draft-nishizuka-dots-inter-domain-mechanism
  - 他の参加者との議論の結果、内容を整理しシンプル化したものを再提出し、WGドラフト化
- 2016年10月: テレメトリ情報に関するドラフトに連名
  - draft-doron-dots-telemetry
  - ベンダ(Radware社)がメインで執筆

DOTS WGでの活動(2/3)：リファレンス実装

- 2016年10月～
  - 仕様を決めたドラフトのWGアイテム化に合わせて、リファレンス実装となることを目的とした開発を開始
- 2017年7月: OSSとして公開
  - Go implementation of DOTS (go-dots)
  - https://github.com/nttdots/go-dots



DOTS WGでの活動(3/3)：ハッカソンへの出場

- 2017年7月: OSS公開に合わせて、IETF99ハッカソンに出場
  - 2日間のハッカソンで go-dots の改良
  - 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
  - Best Name賞を受賞(“Waiting for go-dots”)
  - 懇親会でデモブースをゲットし、デモを実施
  - WGに仕様上の改修すべき点をフィードバック
- 2017年11月: 相互接続試験のためにIETF100ハッカソンに出場
  - NCCグループのプロプライエタリ実装との相互接続試験
  - 異なる実装間でも通信ができ、動作することを証明
  - Best Open Source Project賞を受賞
  - WGに仕様上の改修すべき点をフィードバック

ハッカソンでの発表の様子：

DOTS WGでの活動の目的

なぜ標準化に参加する必要があったのか：

WGへの参加の目的

1. 自分の望む仕様を実現するため
   - 使えないプロトコルを座して待つより、使いたいプロトコルを作る
2. 標準化のプロセスを早めるため
   - 待っているだけでは2年以上はかかる
   - しかし、DDoS対策の事業者連携は、今すぐにでも実現したい(ビジネスとしての戦略)

そのために、

- オペレータの視点で、欲しいものを明らかにする
- リファレンス実装を作って実際に動くことを実証する

なぜ実装をOSS化したのか：

go-dots

最初からOSS化を目的として開発を始める

- リファレンス実装となることを目的としているため

オープンなランニングコードを持つということ

- 端的にいえば、議論で”勝てる”
- WGへの継続的なフィードバックによって、自分たちが使いやすい仕様に変えていくことができる

IETFハッカソンに出場する意義：

- ハッカソン自体が、頭でっかち(議論重視)になっていたIETFを、Running Code(実装重視)にするための取り組み
  - 標準化前のプロトコルについて、実装をすすめることができる場所をIETFが提供する
  - オープンな場所で、相互接続試験を試すことができる

- 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獲得できる
  - IETFには数多くのWGがあり、実は他のWGの活動を把握できる機会は少ない

これからIETFを活動の選択肢の一つとするあなたへ：

- IETFにおける標準化の目的を常に考えること
  - 標準化自体が目的ではない
  - 使えるプロトコルを早く世に出し、それが広く使われることが目的
  - 自社にとってのビジネス面でのメリットをいつでも正しく言えるように
- どのようにして標準化を早めるか、そして使えるものを手にいれるか
  - オープンループをまわすのが今のベストプラクティス
- どのようにオープンループを回すのか
  - 実装をもつ。OSSで公開する
  - ハッカソンに参加する

JANOGとオープンループ：

こんなJANOG(er)だったらいいと思います

- 運用上の知見を、IETFにフィードバックしていく
  - NANOGは定常的できている(ループが回せている)
    (grow WG, idr WGなど)
  - JANOGももっとできるのでは？

- 運用で使っているOSSツールにガンガンコミットしていく
  - 例えば、JANOGハッカソンを開催する
    - 運用技術にフォーカスしてツールの開発・改良など