NTT

IETF100調査報告
&
これから初参加される方に向けて

ネットワークサービスシステム研究所
転送サービス基盤プロジェクト
転送サービスシステムDP
林　裕平
@iehuuy
2017/12/15

もくじ

もくじ

自己紹介

◆名前　林　裕平　(@iehuuy)
◆年齢 27歳
◆所属
2008年～　東京工業大学
2014年～　ネットワークサービスシステム研究所
転送サービス基盤プロジェクト


※入社時の写真

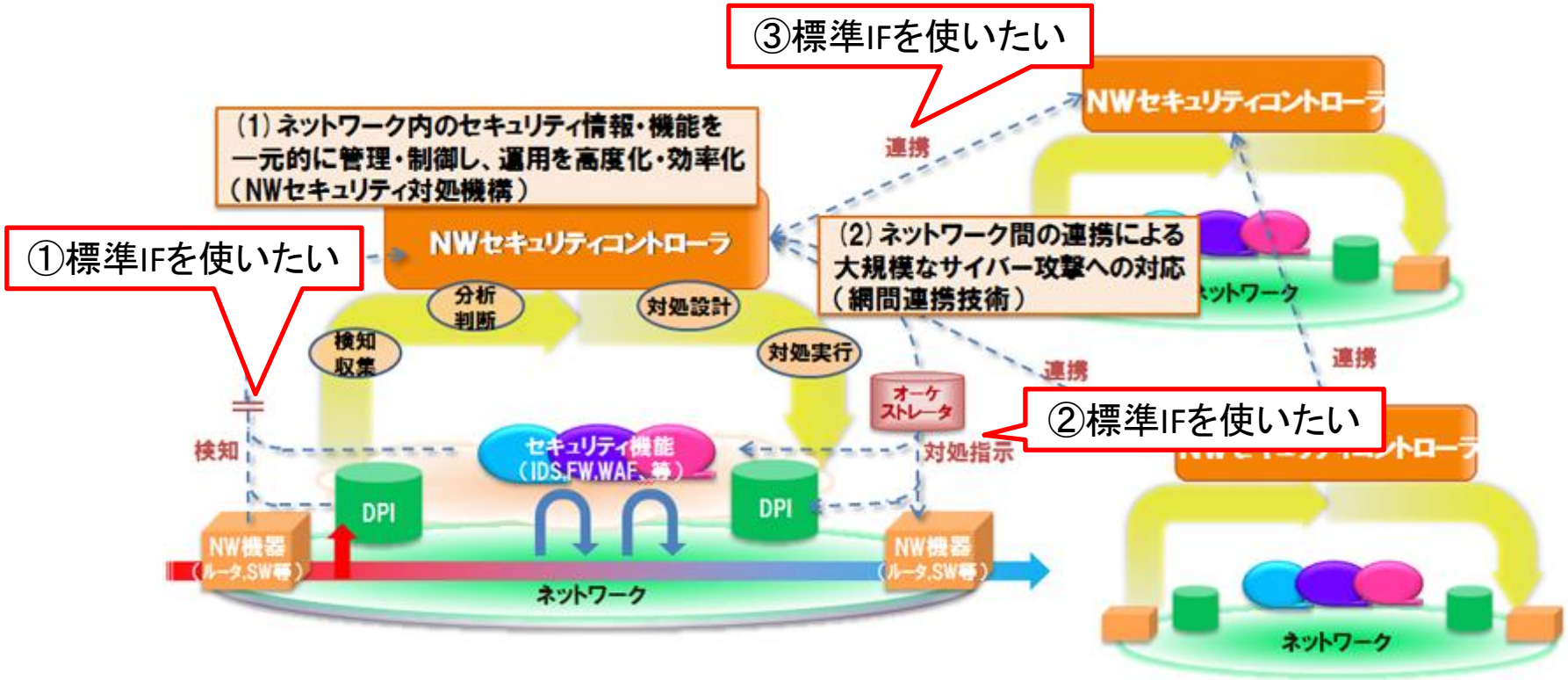
◆主な検討領域
NWにおける経済的なDoS対策技術
ルータとサーバの連携によるDoS検知技術
多様なプロトコルが存在するNWでのDoS検知技術

◆主な業績
・Method for detecting low-rate attacks on basis of burst-state duration using quick packet-matching function，IEEE LANMAN 2017
・Applying per-node priority assignment to heterogeneous bandwidth flows environments，” IEEE PACRIM 2013
・A Method of Per-Node Priority Assignment for Live Streaming Flows，IEEE CQR 2013

もくじ

調査の動機

■NWセキュリティ運用の稼働の増加を抑えるためにコントローラによる自動化を検討.
■①コントローラとNW機器・セキュリティ機能間での情報収集のIF・②制御のIF,③NW間の攻撃対処依頼のIFとして，標準IFを活用することによりマルチベンダの装置を活用したい.
■NWのDoS対策自動化に関連があるDOTS及びI2NSFについて調査を実施.



http://www.ntt.co.jp/inlab/org/ns.html

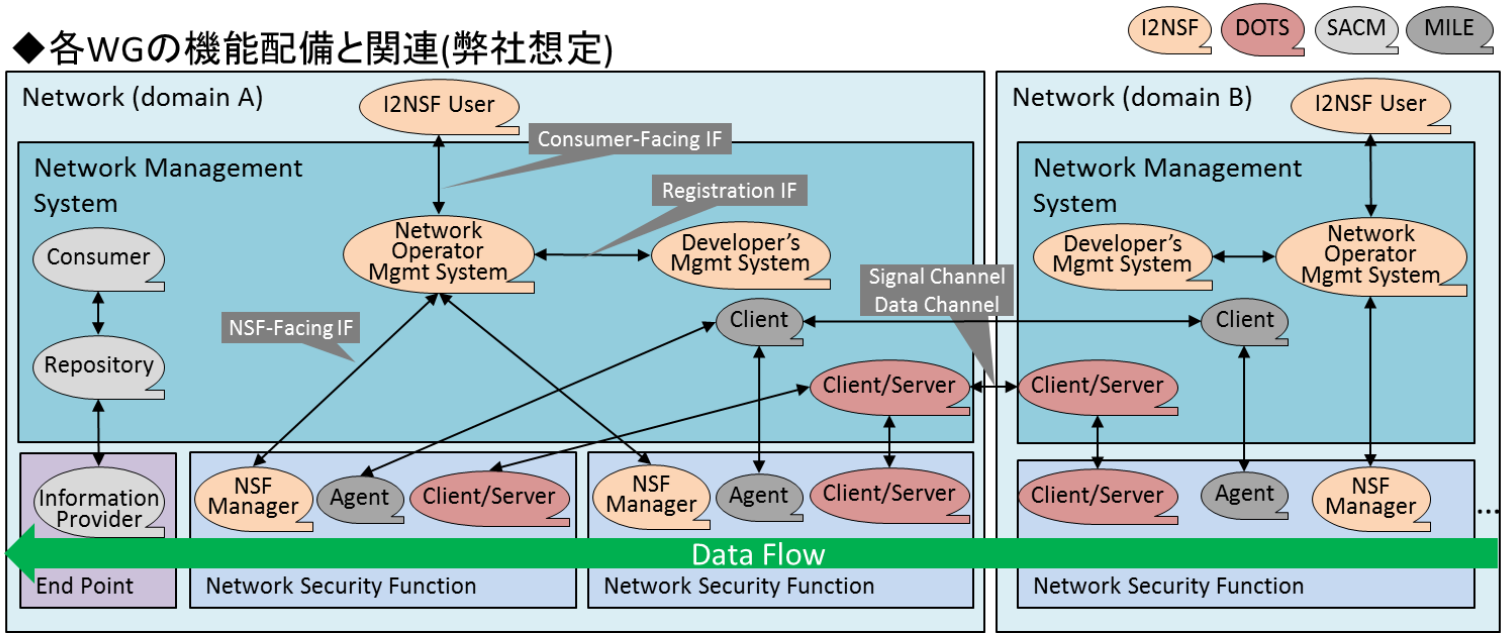
調査の観点

■NWのDoS対策自動化に関連があるDOTS及びI2NSFについて調査を実施.
-DOTSとI2NSFのステータスは?不足要件があった場合に標準に盛り込めそうか?
-各WGのモジュールのNWへの機能配備は?各WGで連携はあるか?
-DOTSとI2NSFの実装の兆しはあるか? 実装状況は?

◆IETF Security Automation関連WG

WG	概要
DOTS (DDoS Open Threat Signaling)	Inter/intra-domainにてDDoSの検知情報等のシグナリング技術の標準化
I2NSF (Interface to Network Security Functions)	NSFの制御/監視のための情報・データモデルとソフトウェアIFの標準化
MILE (Managed Incident Lightweight Exchange)	セキュリティインシデント情報の交換技術の標準化
SACM (Security Automation and Continuous Monitoring)	エンドポイントのセキュリティ状態の監視と自動対応の技術の標準化

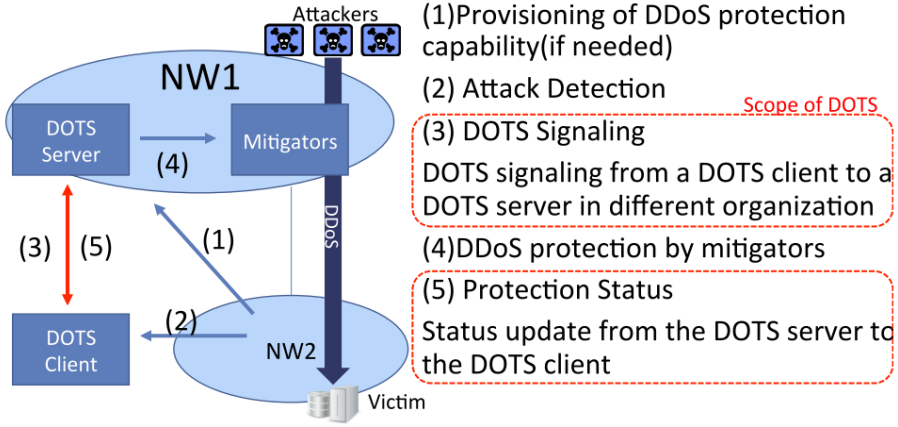
◆各WGの機能配備と関連(弊社想定)



もくじ

DOTS(DDoS Open Threat Signaling)概要

■Inter/IntraドメインにてDDoSの検知情報等のシグナリング技術の標準化を行うWG
■参加組織については，キャリアとベンダが半々．有力セキュリティベンダのArborも参画
キャリア：Comcast, Charter, Verisign, Orange, NTT Com
ベンダ：Arbor, Cisco, Mcafee, Ericsson, Huawei
■WGのステータスについては，主要ドラフトはWG-LCに向かっている勢い.
Requirement, Use case, Architecture, Data channel, Signal Channel→WG Draft
DOTS Multihoming, Server Discovery → Internet draft



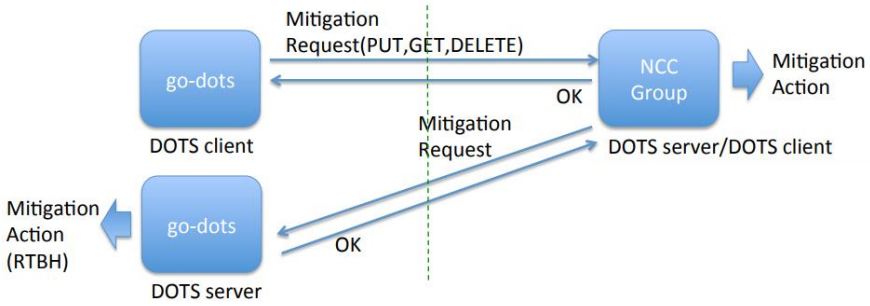
cf. slides-95-dots-6

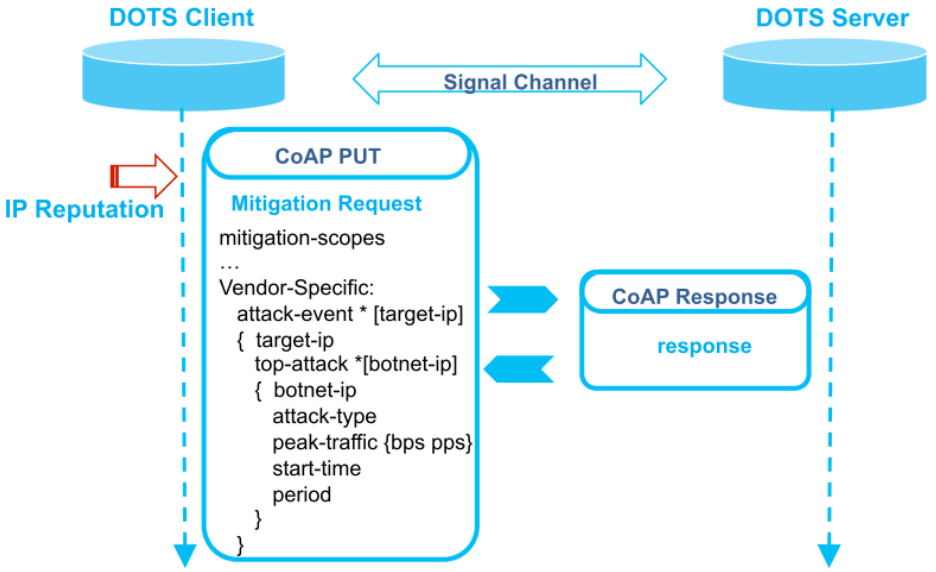
	Signal Channel	Data Channel
スタック	DOTS / CoAP / TLS | DTLS / TCP | UDP / IP	DOTS / RESTCONF / TLS / TCP / IP
アプリケーション	CoAP	RESTCONF
セキュリティ	TLS/DTLS	TLS
トランスポート	TCP/UDP	TCP
目的	(攻撃を受けているときに)防御を依頼するチャンネル	(攻撃を受けていないときに)防御をセットアップするチャンネル

cf. IETF98報告会 IPv6関連WG & DOTS WG

DOTSハッカソン

■今回のハッカソンでは西塚さん(NTTコム)のgo-dotsとNCCグループの独自実装の間でSignal channelの相互接続試験が実施された.
■6割の機能が動作することを証明.
■HuaweiによるVendor-Specificなメッセージ交換の実装も行われた.





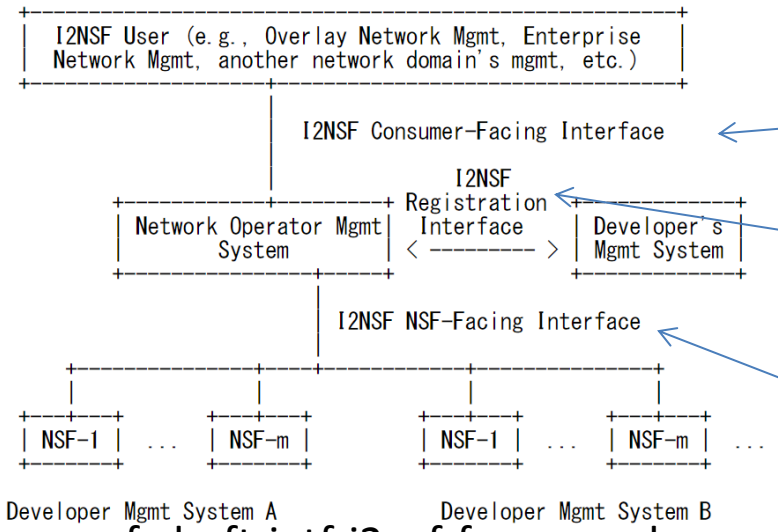
Result of the Interop Test

Purpose: Check interoperability of the messages on the signal channel				
			Interop Testing (client -> server)	
Item #	Messages	CoAP Method	go-dots -> ncc	ncc -> go-dots
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	-	-

cf. slides-100-dots-hackathon-and-interoperability-test-report

I2NSF(Interface to Network Security Functions)概要

■物理/仮想のNSF(Network Security Function)の制御/監視を行うための情報・データモデルとソフトウェアIFの標準化を行うWG
■参加組織については，ベンダ，キャリア，大学の順で多い.
キャリア：Korea Telecom, Telephonica, France Telecom, Bloomberg
ベンダ：Juniper, Nokia, vArmor, Huawei, Curveball, Dell
アカデミック：Sungkyunkwan University, University of Marucia
■WGのステータスについては，Problem Statement and Use CasesがRFC化.
FrameworkはWGLCがかかっているものの，多くのドラフトは未だ議論中.



cf. draft-ietf-i2nsf-framework

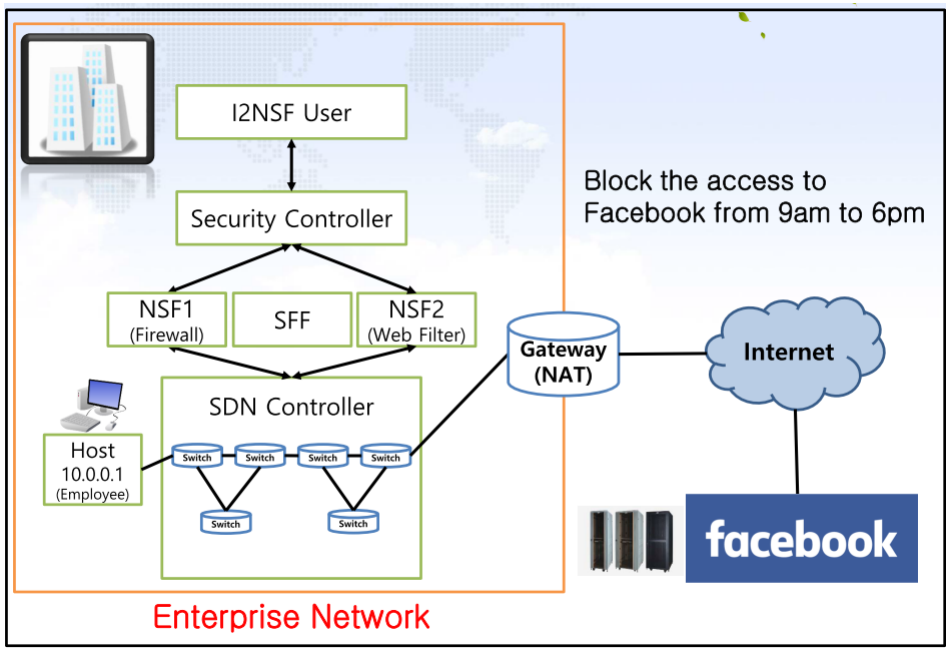
ユーザの抽象的な要求を受け付けるIF

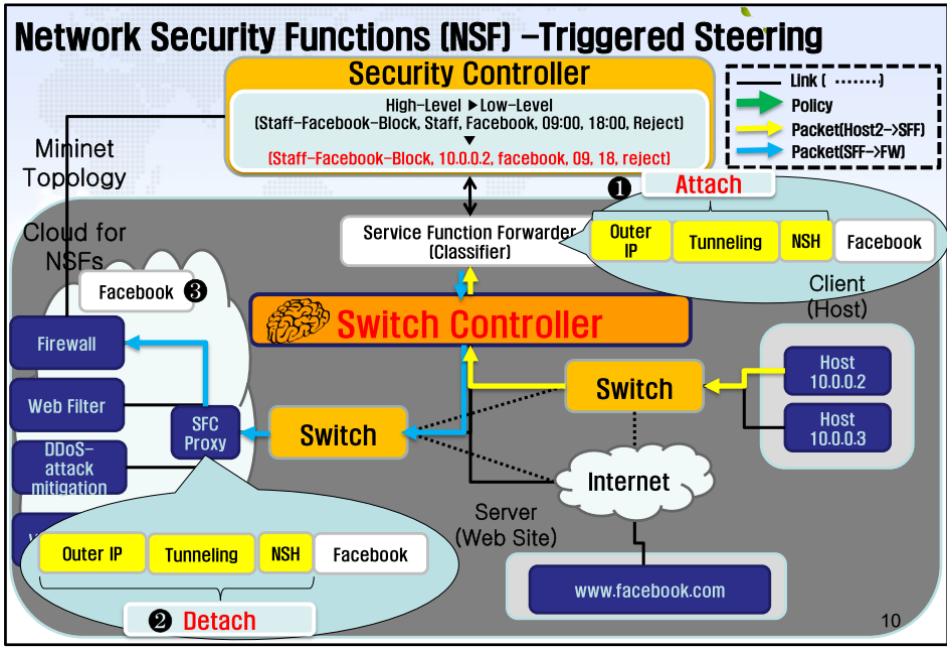
NSFのCapabilityを登録するIF

NSFの設定を行うIF
NSFのモニタリングを行うIF

I2NSFハッカソン

■Jeong教授(SKKU)により，既存のOSSを活用してPoCが実装された．今回のハッカソンではユーザの抽象的な要求からSFCを活用してfacebook向けトラヒックをフィルタする一連の動作が可能なことが示された.
■Consumer-Facing InterfaceはRESTCONF & YANGで実装
■Registration InterfaceはNETCONF & YANGで実装
■NSF-Facing Interfaceは不明(装置独自のIFを使用?)
■SFC技術としてはNSHを使用.





cf. slides-100-i2nsf-i2nsf-hackathon-report

もくじ

これから初参加される方に向けて

Innovative R&D by NTT

■ 当初の林の懸念と役に立ったこと

・そもそもIETFってどんな組織なんだ…

⇒IETFのタオ，Newcomer’s Orientation

・初心者っていうことで議論もさせてくれないのでは…

⇒IETF初心者リボン，Newcomers' Meet and Greet

サイドミーティング

これから初参加される方に向けて

◆IETFのタオ

・読めば初心者が解らない大抵のことが解決.

・実際解決したこと

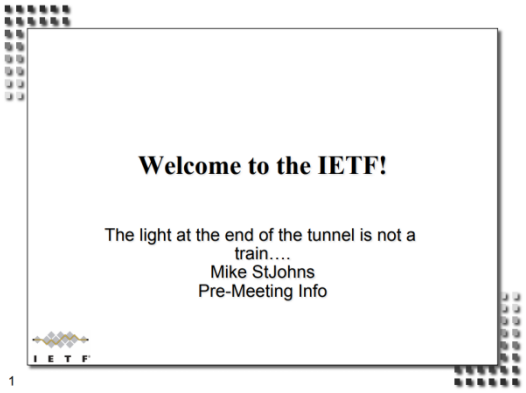
- 略語
- I-DがRFCになるまでの過程
- 誰がどのくらい偉いのか＆凄いのか
- 「ラフコンセンサス」「ランニングコード」文化

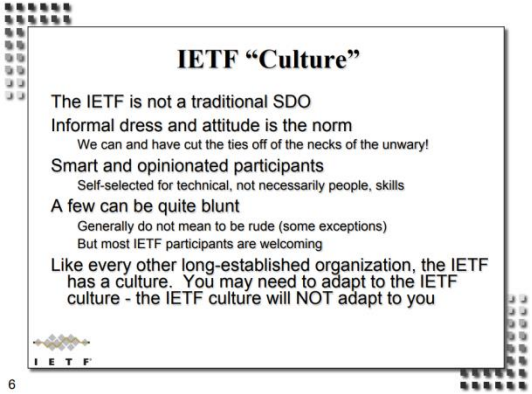
https://www.ietf.org/tao.html

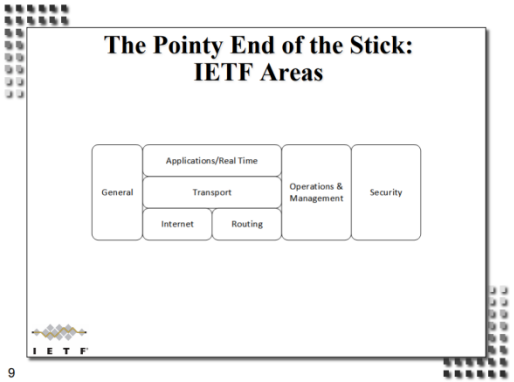
◆Newcomer's Orientation

・日曜の昼にスライドを用いたオリエンテーション形式で開催.

・ハミングの練習として「部屋の寒さ」についてラフコンセンサスが得られた.







https://www6.ietf.org/meeting/100/documents/Newcomers_Webinar_IETF100.pdf

これから初参加される方に向けて

◆IETF初心者リボン

・登録の際に初参加である欄にチェックを入れると，当日に貰える.
・これがあると皆が優しくなるとの噂を聞いていたが実際そうだった.

◆Newcomers' Meet and Greet

・日曜の夕方に開催される初心者向けの立食.
・各WGのチェア，エリアディレクタと初心者のみの参加.
・気になるトピックがあると，適切なWGの席にフォワードしてくれる.
・この場でアポを取り付けるのも問題なさそうな雰囲気.

◆サイドミーティング

・事前にアポを取れば，結構みなさん時間を作って議論してくれる.
・Registrationデスク前で集合して打ち合わせすることが多かった.
・論点を整理しておくと話が発散せずに済む.

所感

■DOTSの所感
-ステータス：主要なドラフトはWG-LCがかかる勢い.
-メッセージ交換能力：攻撃名や通信のソース情報のやり取りが出来ないのが難点
-実装の兆し：複数社による実装が登場，Arborが参加している，要件が軽いことからベンダによる実装は期待できそう.
⇒短期的な検討として実際使ってみることができそう.
⇒不足要件のインプットはリチャータ時を狙うのが良さそう.

■I2NSFの所感
-ステータス:IFに関するドラフトはまだWG-LCはかからなさそう.
-メッセージ交換能力：YANGモデルが充実しており多くのメッセージ交換ができそう
-実装の兆し：実装は大学のみ，有力セキュリティベンダが参加していない，要件が重いことからベンダによる実装はまだ先の様子.
⇒中長期的な検討向け．SFCとの連携とかは面白そう.
⇒不足要件のインプットはできそう.

■その他所感
-どこに所属しているかではなくどれだけIETFに貢献したかの世界.
-みんな技術が好き.