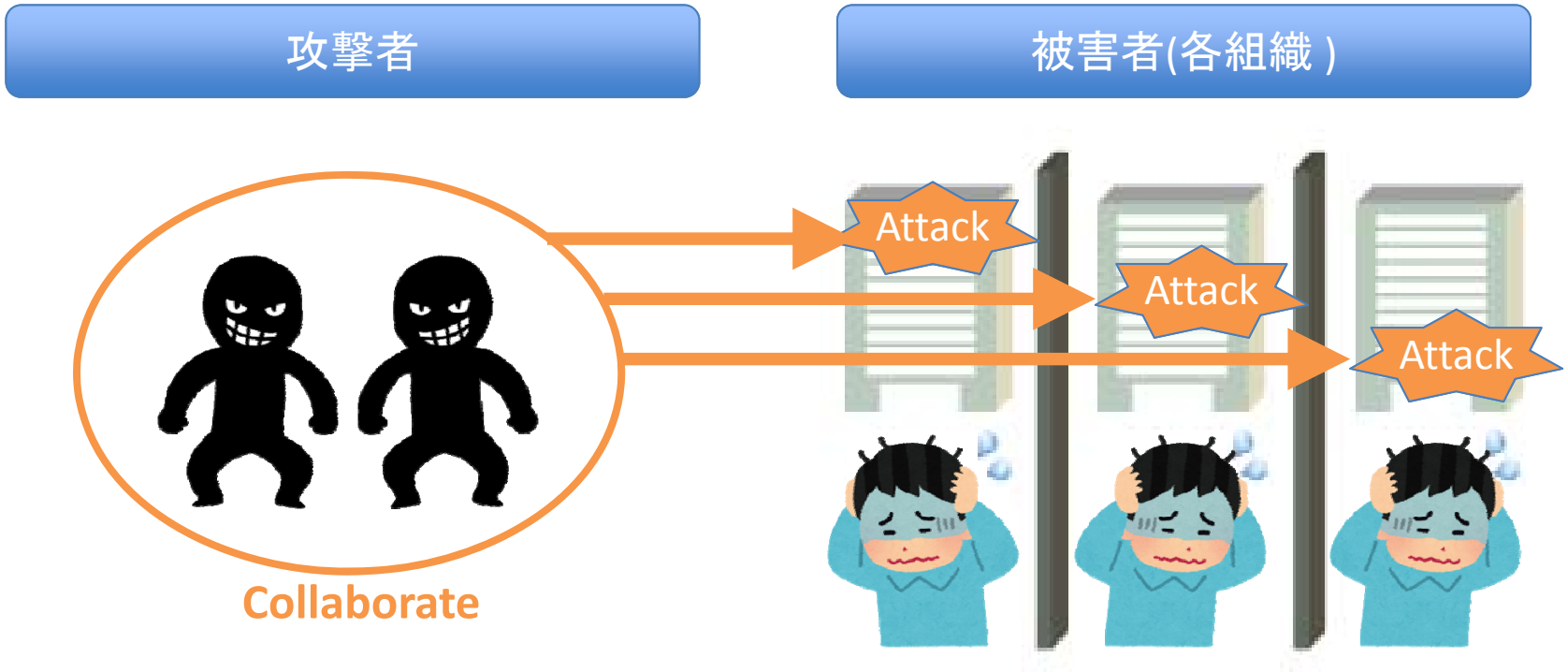
IETFにおけるセキュリティオートメーション技術 (DOTS, I2NSF, MILE, SACM WG)

国立研究開発法人 情報通信研究機構
ネットワークセキュリティ研究所
セキュリティアーキテクチャ研究室
高橋健志

発表者について

- IETFでの活動
  - IETF 79から参加 (Liaisonとして参加)
  - Security automation系のworking groupの動向をwatch
  - RFC 7203 (IODEF-SCI)をpublish
  - IETF 89からIETF MILE WG co-chair
  - IETF 89からIETF Security Directorate
- その他の活動
  - ITU-T SG17にも協力: X.1500, X.1570などをpublish
  - 所属機関では、主にSecurity automation周りでの研究開発業務に従事

問題認識



増加するセキュリティ脅威に対応するためには、各組織はお互いに
情報連携・協調する必要がある

Source: http://www.atmarkit.co.jp/fsecurity/rensai/cybex01/cybex01.html

IETFにて扱っているSecurity Automationのtopic

セキュリティオートメーションに関し、IETFでは以下の技術領域を検討

1. セキュリティ情報の交換 (ヒトとヒト、ヒトと機器、機器間のすべて)

2. エンドポイントのセキュリティ監視・評価

3. ネットワーク機器のセキュリティ設定・制御のためのシグナリング
   a. DDoS対策
   b. Firewallなどのセキュリティポリシの設定

4つのWGのトピック概要

セキュリティオートメーションに関し、IETFでは4つのWGにて検討

Security Automation

MILE : Managed Incident Lightweight Exchange — *IETF 82 ～*
インシデント情報の交換技術を検討

SACM : Security Automation and Continuous Monitoring — *IETF 85 ～*
Endpointのセキュリティ状態の監視・評価技術を検討

DOTS : DDoS Open Threat Signaling — *IETF 93 ～*
DDoS対策のための機器へのSignaling技術を検討

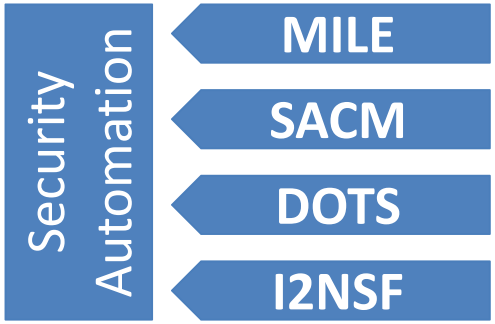
I2NSF : Interface to Network Security Functions — *IETF 94 ～*
機器のセキュリティ設定・制御のためのSignaling技術を検討

Short summary and comments

IETFでの現在の活動領域

セキュリティオートメーションに関し、IETFでは以下の技術領域を検討

1. セキュリティ情報の交換 (ヒトとヒト、ヒトと機器、機器間のすべて)
2. エンドポイントのセキュリティ監視・評価
3. ネットワーク機器のセキュリティ設定・制御のためのシグナリング
   a. DDoS対策
   b. Firewallなどのセキュリティポリシの設定



これらの活動に対する個人的な想い

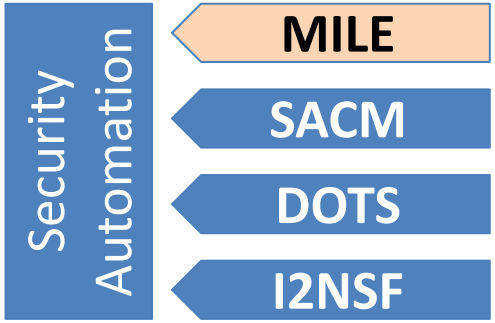
- IETFの中では未だ新興の分野。より多くの人に活動を知っていただき、賛同者を増やしたい
- どの技術が生き残るか否かという議論ではなく、Security Automationの重要性を共有し、今後同様のアクティビティをどんどん盛り上げて、潮流を作り上げていくことが重要と考えている

Agenda

16:30 - 16:40	MILEの紹介・議論
16:40 - 16:50	SACMの紹介・議論
16:50 - 17:00	I2NSFの紹介・議論
17:00 - 17:10	DOTSの紹介・議論
17:10 - 17:20	Security automation技術の進むべき検討の方向性について議論

※ SACMの紹介、およびMILE中のimplement draftの現状については東京大学の宮本大輔先生に、MILE中のguidance draftの現状についてはNICTの鈴木未央氏に、それぞれプレゼンをお願いさせて頂いております

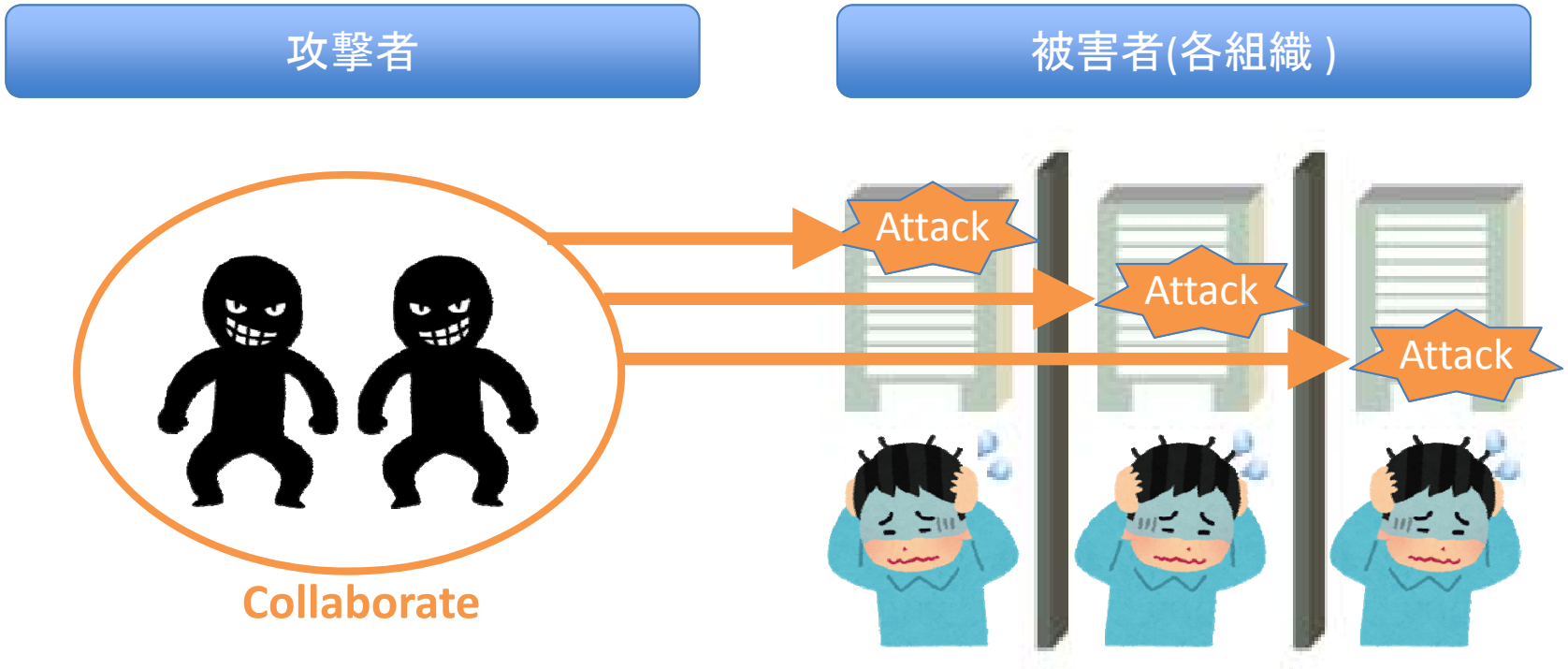
インシデント情報の交換技術を検討する
IETF MILE WG



Agenda

1. MILE WGの活動内容
2. 各種Draftの紹介
    a. 既にRFC化されたもの
    b. 現在検討中のもの

問題認識



増加するセキュリティ脅威に対応するためには、各組織はお互いに情報連携する必要がある

Source: http://www.atmarkit.co.jp/fsecurity/rensai/cybex01/cybex01.html

MILE WGの概要

目的

- **Incident Response関連の技術をIETF内で規格化する場所として、MILE WGは発足**
  - MILE: Managed Incident Lightweight Exchange
  - INCH WGの後続であり、特にIODEFをベースとする
- MILEは、セキュリティインシデント発生時の情報交換を少しでも前進させるための技術を検討する場所
  - 従来のhuman-to-humanのみならず、machine-to-machineの情報交換も目指す
  - インシデント情報のrepresentation、交換の際のPolicy、交換の際のTransport、実装に向けたガイドラインなどを検討

Chairs

Kathleen Moriarty,
Brian Trammel

2014年3月

- Alexey Melinkov, Takeshi Takahashi
- Secretary: David Waltermire (NIST)

Incident Object Description and Exchange Format

- IODEFは、インシデント情報を組織間で交換するフォーマットを規定
- 正確にはフォーマットではなく、データモデルを規定しているが、XMLでの利用が想定されており、XML schemaも規格内にて定義
- JSON等、その他の形式にも適用可能
- US-CertではIODEFを長らく活用
- 時代の先駆けとして作られたこともあり、改修・発展が必要

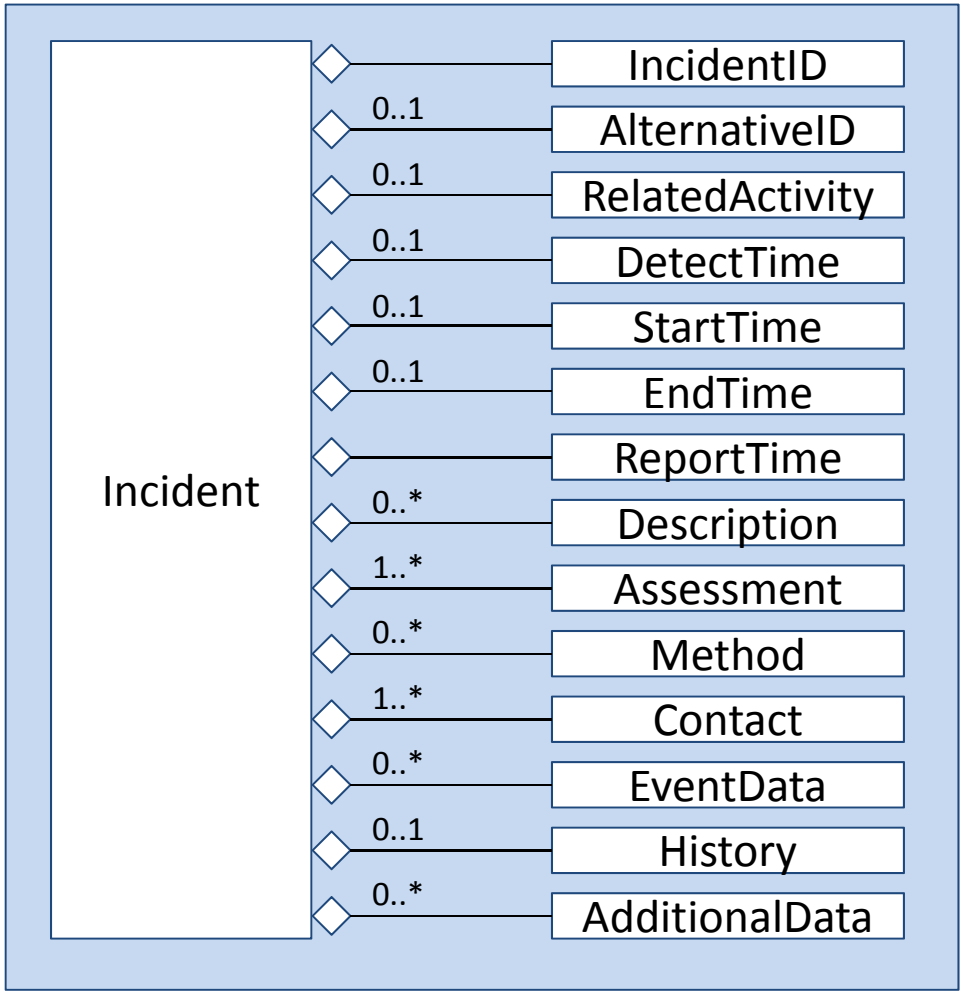


Fig. IODEFのデータモデル

MILE WGの主なドラフト

審議終了	• RFC 6545 – RID / RFC 6546 – RID over HTTP/TLS	1
	• RFC 6684 – Extension Guidelines and Template	2
	• RFC 6685 – Expert Review for IODEF Extensions	3
	• RFC 7203 – IODEF-SCI	4
	• RFC-7495 – IODEF Enumeration Reference Format	5
現在審議中	• Resource-Oriented Lightweight Indicator Exchange	6
	• IODEF-bis	7
	• IODEF implementation draft	8
	• IODEF guidance	9
Topic of interests	• IODEF in JSON	10
	• IODEF cyber-physical extension	11

Agenda

1. MILE WGの活動内容
2. 各種Draftの紹介
    a. 既にRFC化されたもの
    b. 現在検討中のもの

検討が終了したドラフト 1/3

1 RFC 6545 – RID / RFC 6546 – RID over HTTP/TLS

- IODEF documentを送信する際のコンテナ
- データ取扱いポリシー記述や署名などを埋め込める
- RIDはIODEFの安全性を担保。但し、IODEFはRIDを無視してもOK
- INCH WG時代には、informational RFCだったが、MILEにて、standard-track RFCへ

2 RFC 6684 – Guidelines and Template

- IODEFを拡張する際のガイドラインと、そのテンプレートを規定したもの
- 本WGにて、IODEFの各種拡張が強く意識されていることを表している

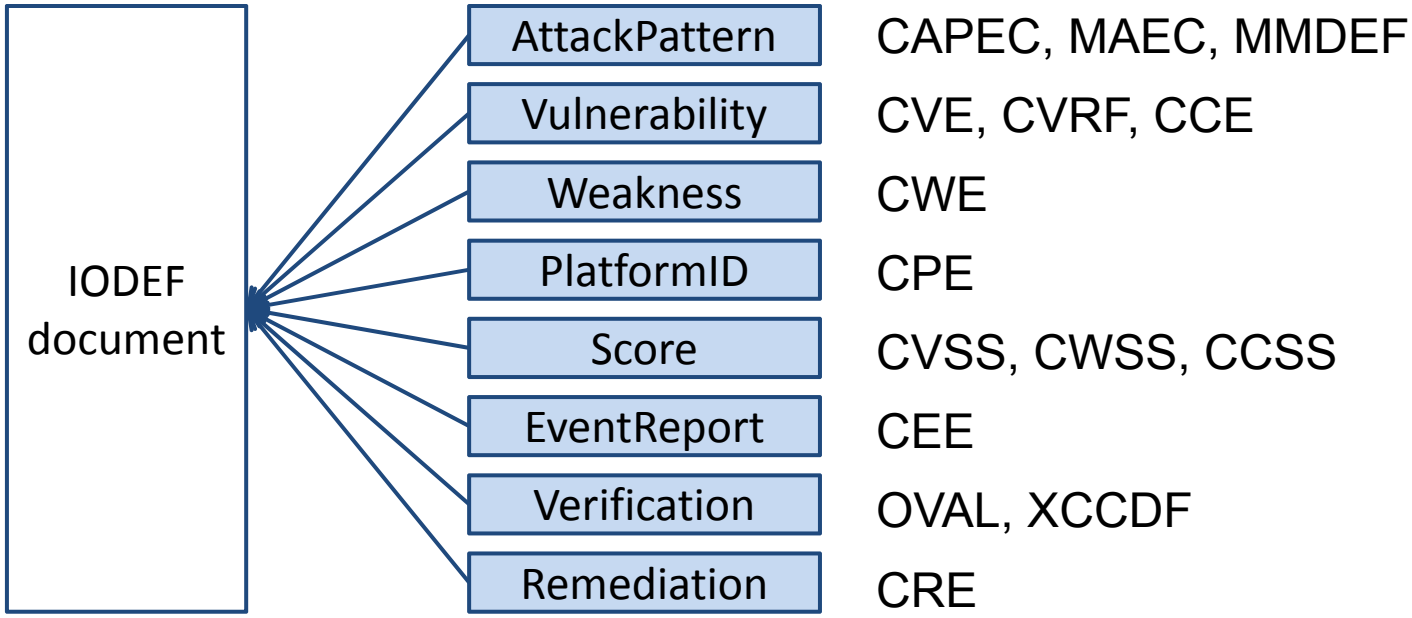
3 RFC 6685 – Expert Review for IODEF Extensions

- IODEFの拡張を定義したRFCにおいて、Expert Reviewを義務付ける際のガイドライン

検討が終了したドラフト 2/3

4 RFC 7203 – IODEF-SCI

- IODEF-SCI: IODEF-extension for structured cybersecurity information
- IODEFの中の、機械可読でない部分をなるべく排除すべく、機械可読なSchemaをIODEFに組み込む技術
- IODEFを拡張して各種XML情報をIODEFに埋め込むインターフェースを定義



検討が終了したドラフト 3/3

5 RFC 7495: IODEF Enumeration Reference Format

- IODEFの中の、機械可読でない部分をなるべく排除すべく、機械可読な各種情報のIDをIODEFに組み込む技術
- IODEFのReferenceクラスを利用し、CVEなどのidentifierを記述
  - IODEFのReferenceクラスを再定義
  - クラス内で、CVE IDなどの、セキュリティIDを引用できるようにしている
- IODEFから直接参照できるように、独立したschemaを持つ

Agenda

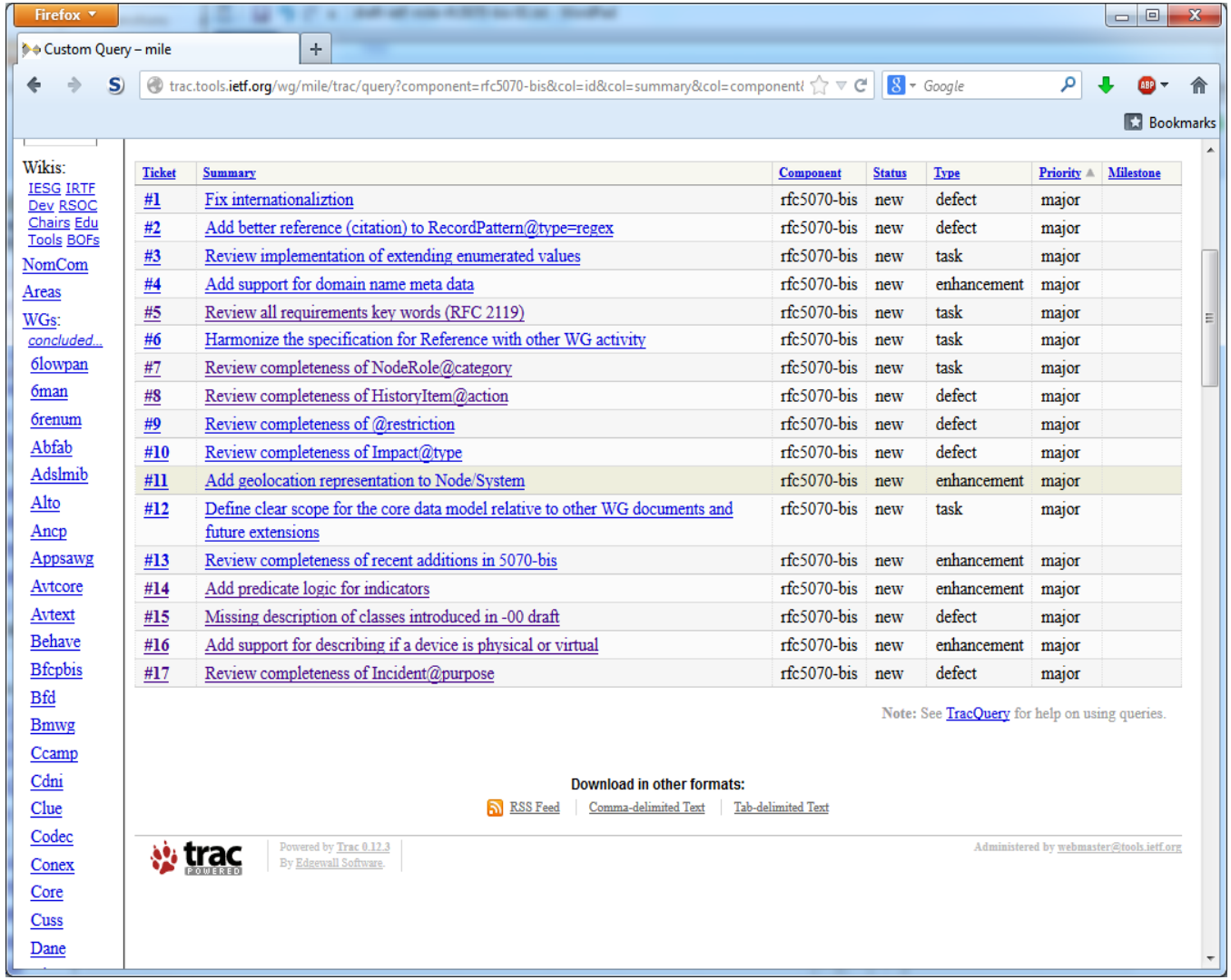
1. MILE WGの活動内容
2. 各種Draftの紹介
    a. 既にRFC化されたもの
    b. 現在検討中のもの

現在検討中のドラフト 1/2

6 IODEF-bis

- IODEFを現状に合わせてreviseし、version 2とする
- revisionの議論を1年以上継続
  - Enum valueの見直し、拡充
  - 埋め込み情報のリンケージをつけるためのID (Indicator-UID)を追加
  - 伝搬される情報のconfidence levelを付加
  - メール内容の添付にはARFを検討
  - Purpose of attackフィールドの拡充
  - Referenceクラスについては外部draft参照
  - Schema修正
  - “ext-*” attributeとIANA tableを用いた拡張性の見直し、など
- 残課題はDNSレコードの記載・交換、など
- 年内にWGLC

【FYI】IODEF-bisの課題管理



現在検討中のドラフト 2/2

7 Resource-Oriented Lightweight Indicator Exchange

- 情報フィードを作り、インシデント情報をネットワーク上で交換する技術
- Atom +XML形式でHTTP通信するRESTアーキテクチャ
- “コンテンツを何度も送るのではなく、そのリンクだけ送る方法を考えると、本ドラフトは有効なはず”

8 IODEF Implementation draft

- 東京大学の宮本先生のdraft
- IODEF関連のツールを紹介し、また、IODEF関連のツールを作る際、利用する際に考慮すべき点をまとめたもの
- 毎会合ごとに新たなツールが追加されるドラフト

9 IODEF guidance (draft-ietf-mile-iodef-guidance-01)

- NICTの鈴木未央さんのdraft
- IODEFの利用を促すため、実装者が実装するとよいと思われる機能を説明する
- 時代や用途による必要機能・不必要機能を明確化する
- 以前登場した、darknet draftの内容は、本draftに吸収される

今後に向けた活動

10 IODEF in JSON

- IODEFはデータモデルであり、representation formatを限定していないが、現時点ではXMLを想定した実装のみが存在
- XMLの向かない実装環境も存在するため、JSONに基づくIODEFを検討
- XML versionとJSON versionの対応を担保するのか否か、またどのように担保するのかが、最大の焦点
- 現時点ではversion 0自体投稿されておらず、水面下にて検討が進められている
- Czech RepublicのCESNETが、独自のIODEFをベースとしたJSONに基づきオペレーションを実施しており、その経験を元にdraft作成を検討中

11 Cyber-Physical extension

- IODEFをcyber-physicalの分野で活用する際に必要なフィールドを定義
- 現時点では検討を継続するのに適した人材がおらず、保留中

MILE: IODEF guidance draft

(NICT 鈴木未央さんによるご紹介)

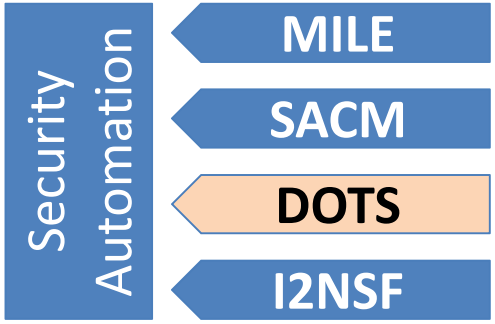
MILE: IODEF implementation draft

及び

SACM WGの概要

(東京大学 宮本大輔先生によるご紹介)

DDoS対策を考える
IETF DOTS WG



Agenda

1. MILE WGの活動内容
2. 各種Draftの紹介

DOTS WGの概要

目的

- DDoS Open Threat Signaling WG
- Inter-domainでDDoS対策を効率的に実現するための
  シグナリング技術を規格化することを目指す

経緯

- IETF92 : BoF
  - http://www.isoc.jp/wiki.cgi?page=IETF92Update
- 2015.06.27 WG化
- 会合としてはIETF 93から開始

Chairs

- Roman Danyliw (CERT)
- Tobias Gondrom (Cisco)

現在のDDoS対策

Technology pioneered by Robert Hooke in 1667, only slightly improved!

Source: “Operational Requirements,” slides-93-dots-3.pdf, DOTS@IETF93

Agenda

1. MILE WGの活動内容
2. 各種Draftの紹介

DOTSのドラフト一覧

- **ユースケースの検討**
  - DDoS Open Threat Signaling use cases (draft-mglt-dots-use-cases-00)
  - The Extended DDoS Open Threat Signaling Use Cases (draft-xia-dots-extended-use-cases-00)
- **要求条件の検討**
  - DDoS Open Threat Signaling Requirements (draft-mortensen-threat-signaling-requirements-00)
- **DOTSメカニズムの検討**
  - Information Model for DDoS Open Threat Signaling (DOTS) (draft-reddy-dots-info-model-00)
- **メッセージングの検討**
  - Co-operative DDoS Mitigation (draft-reddy-dots-transport-00)

ユースケースドラフト

draft-mglt-dots-use-cases-00 (Ericsson)

- dotsに期待する4つの要諦
  - より早く正確なDDoS検知の実現
  - 一貫性のある効率的なDDoS対策を実現
  - 複数組織間でモニタリング情報を共有
  - DDoSの監視と対策について第三者と協業もしくは委譲
- 現時点では、下記3種類のユースケースを掲載
  - On-premise use case (Symmetric, Asymmetric)
  - Cloud Use Case
  - Hybrid Cloud Use Case

draft-xia-dots-extended-use-case-00 (Huawei)

- 2つのユースケースを追加。具体的な対処法に焦点をあてて上記ユースケースを補完
  - セキュリティ関連のフロー情報を収集し、関連性を分析することでDDoSを検知するユースケース
  - VNFをエッジネットワークに展開することによりDDoS対策を実現するユースケース

Source: “DDoS Open Threat Signaling use cases,” draft-mglt-dots-use-cases-00

DOTS要求条件に関するドラフト

- DOTS技術の満たすべき要求条件を記載
- まずは、用語の定義からスタート
- やっと文書ができて、これから中身について議論する段階

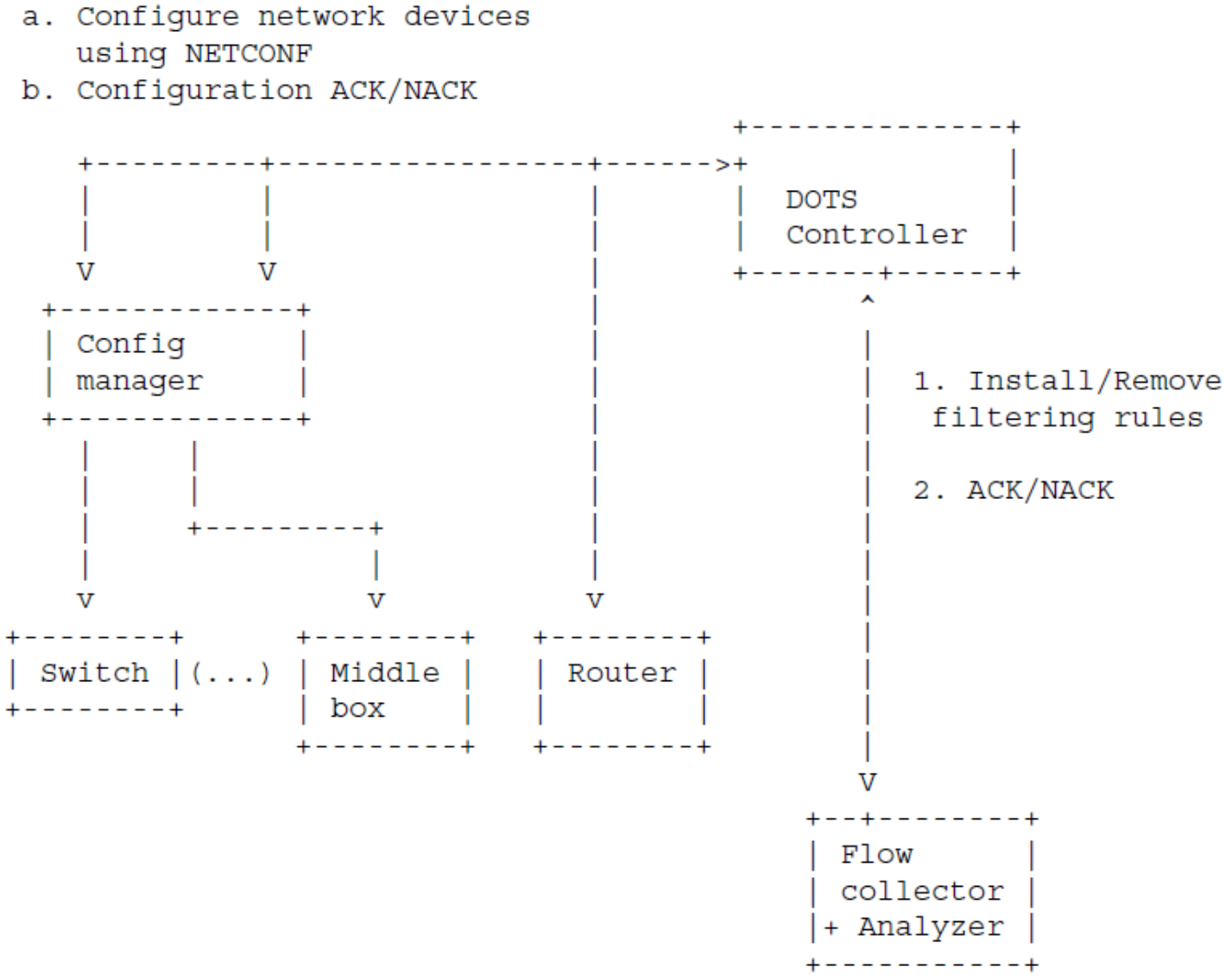
Source: “DDoS Open Threat Signaling Requirements”, draft-mortensen-threat-signaling-requirements-00

DOTSメカニズムのドラフト(1/2)

- Ciscoの提案
- ネットワーク監視デバイスの設定を動的に更新するためのシグナリングメカニズムとインターフェースを定義
- 具体的なシグナリングのデータ構造についいては、RFC6728 (“Configuration Data Model for the IP Flow Information Export (IPFIX) and Packet Sampling (PSAMP) Protocols”)を参照している程度で、本ドラフトの範囲外の模様
- 現時点では、IPFIXに基づくsolutionを想定

Source: “Information Model for DDoS Open Threat Signaling (DOTS)”, draft-reddy-dots-info-model-00.pdf

DOTSメカニズムのドラフト(2/2)



Source: “Information Model for DDoS Open Threat Signaling (DOTS)”, draft-reddy-dots-info-model-00.pdf

メッセージングに関するdraft

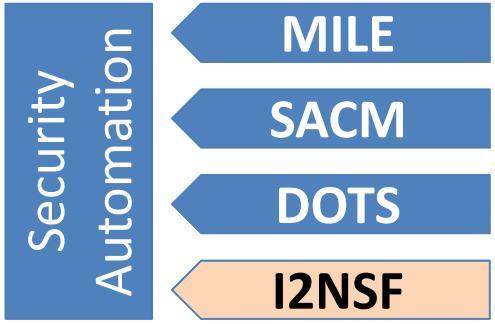
- AS間にてDDoS攻撃に協力して対応すべく、下流のASが上流のASに対してフィルタリングなどの処理をリクエストする手法を定義
- RESTとBGPが考察されている

例示

```
POST https://www.example.com/.well-known/v1/acl
Accept: application/json
Content-type: application/json
{
        "policy-id": 123321333242,
        "traffic-protocol": "tcp",
        "source-protocol-port": "1-65535",
        "destination-protocol-port": "443",
        "destination-ip": "2001:db8:abcd:3f01::/64",
        "source-ip": "2002:db8:6401::1",
        "lifetime": 1800,
        "traffic-rate": 0,
}
```


Source: “Co-operative DDoS Mitigation,” draft-reddy-dots-transport-00

I2NSFの概要



Agenda

I2NSFの位置づけ

1. やりたいこと
2. i2nsfのWGに向けたあゆみ
3. Use Case
4. scope
5. Gap分析

I2NSFにおける技術検討

1. Draft一覧
2. 情報モデル

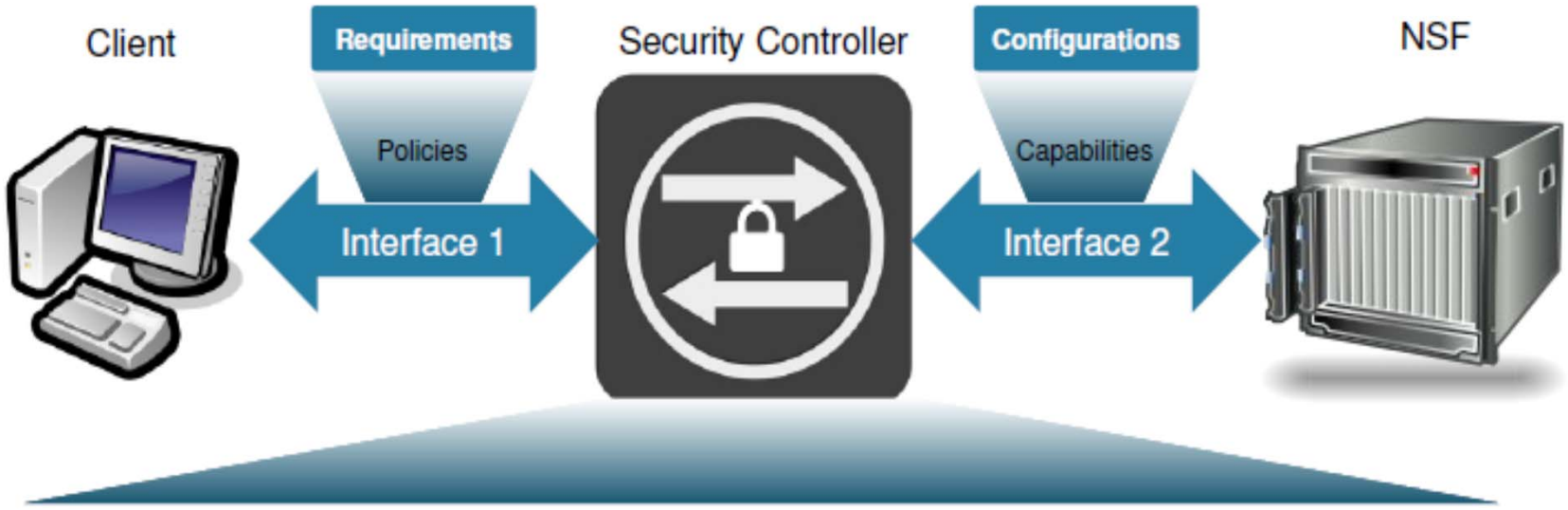
I2NSFで実現したいこと

NSFの制御と監視を実施するための
情報・データモデルとソフトウェアインターフェースを定義する

I2NSFのこれまで

- 2回前 (IETF 91)にBoF
- 前回 (IETF 92)は、official meetingなし
- 今回 (IETF 93)、working group forming BoF
- 本BoFの中では、working groupを作ることでほぼ合意
- そして2015年9月18日に、正式にWG設立が決定

I2NSFでのユースケース検討 (1/2)



インストールと設定　アップデート　ステータスの把握　動作検証

Source: draft-pastor-i2nsf-merged-use-cases-00.txt, slides-93-i2nsf-3.pdf

I2NSFでのユースケース検討 (2/2)

クラウドデータセンター

- データセンターでは、ネットワークセキュリティデバイスはソフトウェアもしくは仮想化により実現されている
- I2NSFにより、各クライアントのコンピュータグループ毎に、動的に仮想ファイアウォールを配置・設定することができる
- その際の複雑な作業を簡略化でき、またミスを減らすことも、自動化を促進することも可能となる

アクセスネットワーク

- NSP内にて提供されるセキュリティサービスに対し、
- NSP側は、ユーザ毎にFirewallを動的に設定し、ユーザの契約・契約解除に合わせてFirewallを設置・解消可能
- ユーザ側は、これまで画一的であった設定を自らのポリシーに合わせて設定し、また設定の現状を把握することが可能

Source: draft-pastor-i2nsf-merged-use-cases-00.txt, slides-93-i2nsf-3.pdf

I2NSFのscope

- NSFの制御と監視を実施するための情報・データモデルとソフトウェアインターフェースを定義することが最大の目的
  - NSFに関するデバイスやネットワークの構築や設定などは範囲外
  - 制御と監視には、NSFを特定・問い合わせ・監視・制御する能力が必要
  - I2NSFでは特に、IPS/IDSやウェブフィルタリング、フローフィルタリング、DPIやパターンマッチングなどの、フローベースのNSFに注力する

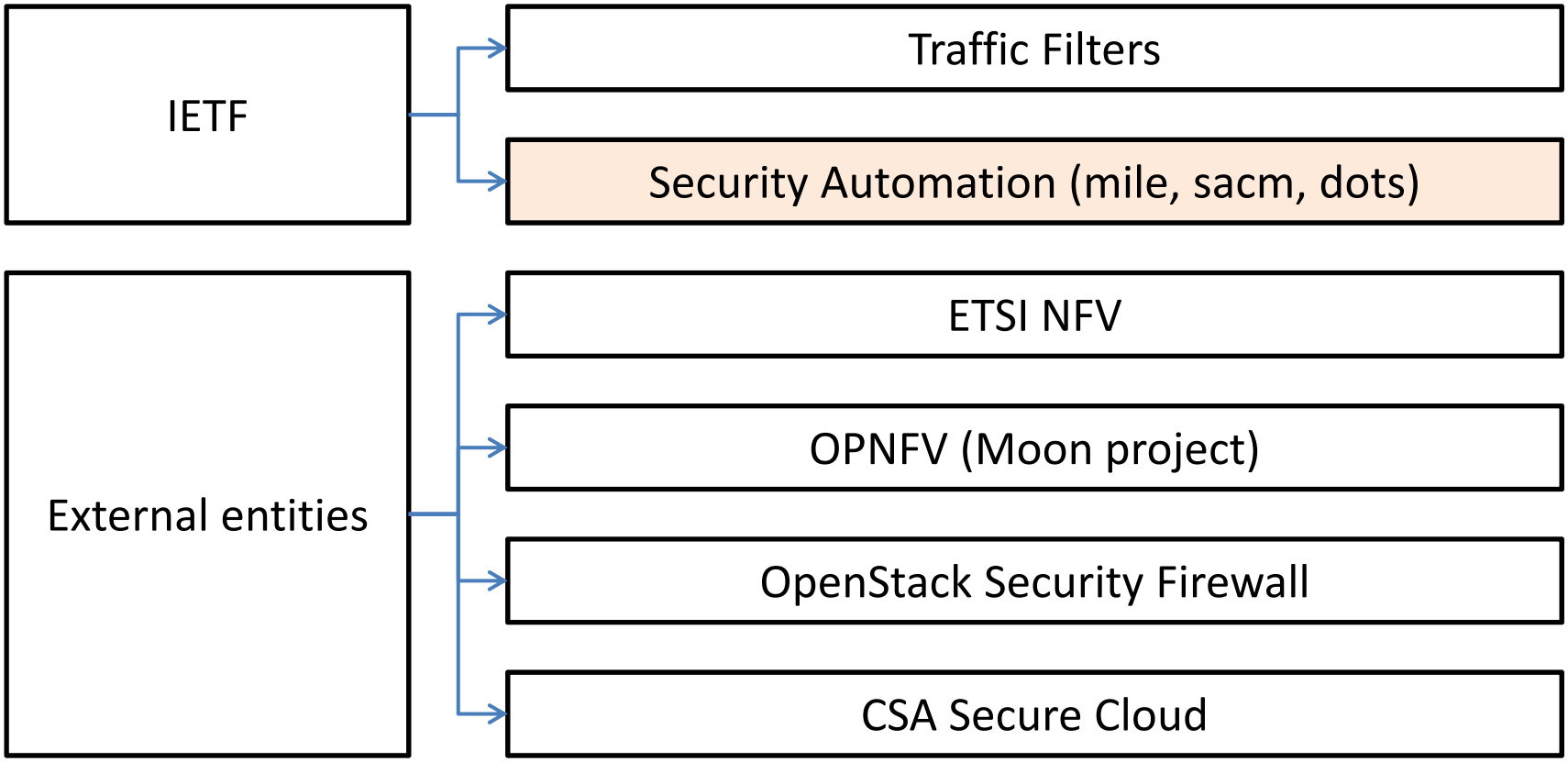
- I2NSFには2つのレイヤの概念が存在
  - I2NSF Capabilityレイヤ: NSFの機能レベルで、NSFをどのように制御・監視すべきかを定義。すなわち、I2NSFでは、NSFの制御と管理が起動され、実施され、監視されるインターフェース群を標準化する。
  - I2NSF Servicerレイヤ: クライアントのセキュリティポリシーをいかに表現し、監視するかを定義

- I2NSFでは、このうちCapability Layerにフォーカスして検討を進めていく

Source: draft-merged-i2nsf-framework-02.txt

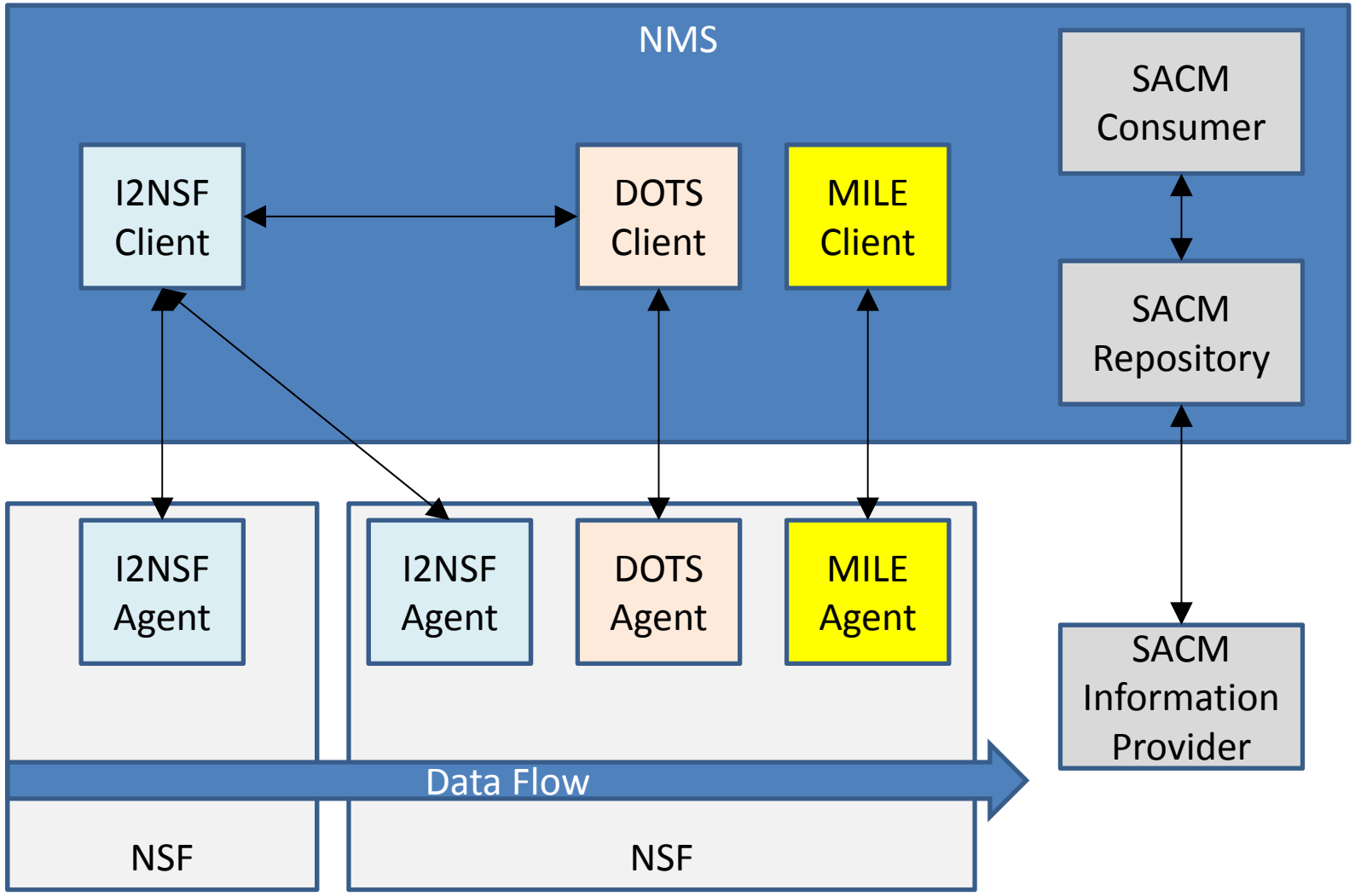
Gap分析

- 下記の領域が近接領域としてあげられており、そのgapが議論されている



Source: draft-hares-i2nsf-gap-analysis-00.txt

Security automation works



Source: slides-93-i2nsf-0.pdf

Agenda

I2NSFの位置づけ

1. やりたいこと
2. i2nsfのWGに向けたあゆみ
3. Use Case
4. scope
5. Gap分析

I2NSFにおける技術検討

1. Draft一覧
2. 情報モデル

Draft一覧

I2NSFの位置づけを明確にするドラフト群

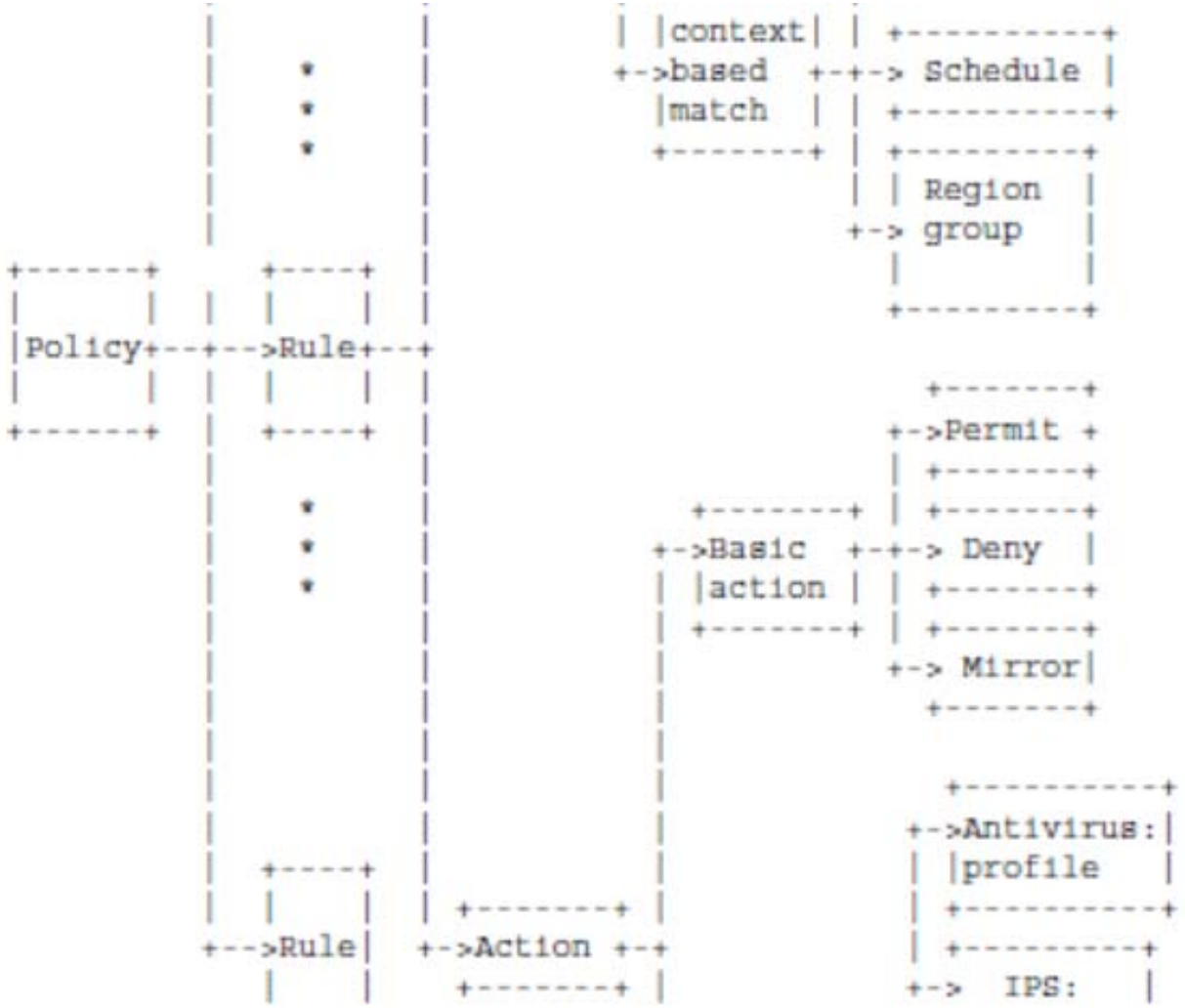
- Use Cases and Requirements for an Interface to Network Security Functions
- Interface to Network Security Functions (I2NSF) Problem Statement
- Framework for Interface to Network Security Functions
- Analysis of Existing work for I2NSF

I2NSF内のsolutionに関するドラフト群

- Information Model of Interface to Network Security Functions Capability Interface
- Software-Defined Networking Based Security Services using Interface to Network Security Functions
- Interface to Network Security Functions Demo Outline Design

Source: draft-xia-i2nsf-capability-interface-im-03.txt

Information model draft (1/2)



Source: draft-xia-i2nsf-capability-interface-im-03.txt

Information model draft (2/2)

Routing Backus-Naur Form [RFC5511]にて書くと…

<Policy> ::= <policy-name> <policy-id> (<**Rule**> ...)
<Rule> ::= <rule-name> <rule-id> <**Match**> <**Action**>

<Match> ::= [<packet-based-match>]
[<context-based-match>]
<packet-based-match>
::= [<packet-header-payload> ...]
[<service> ...]
[<application> ...]

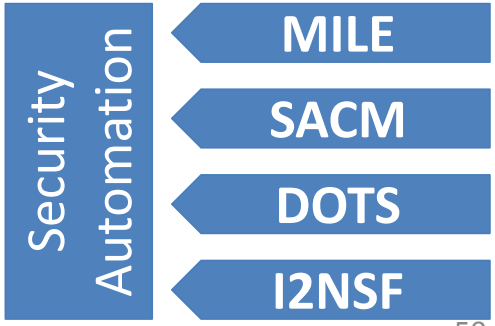
<action> ::= <basic-action>
[<advanced-action>]
<basic-action> ::= <pass> | <deny>
| <mirror>
| <call-function>
| <encapsulation>

Source: draft-xia-i2nsf-capability-interface-im-03.txt

まとめ

- I2NSFでは、NSFの制御と監視を実施するための情報・データモデルとソフトウェアインターフェースを定義する
- solution技術はこれから作っていくところであるものの、I2NSFの課題認識への賛同者は多く、また、実装したいという声もそれなりに多い
- Security automationに関するworking groupが、i2nsfを加えて4つとなり、だいぶ増えてきている (DOTS, I2NSF, MILE, SACM)
- I2NSFはtargetも絞られてきているので、具体的な動きが期待できるのではないか
- Service Layerについては、OpenStackのGroup-based Policyを活用しようとの方向性で議論中
- 今後の動向を注視したい

Discussion



Discussion Topics

情報交換技術 (MILE)	• ヒトとヒトだけでなく、機器間でのインシデント情報共有を如何にして促進していくべきか? • 日本国内で広く使われるためには何が必要か？ – 別のレイヤで、情報共有のmotivationなどが議論されているが、技術面での課題はもうないのか？ – 代替する技術が存在するのか？また、如何にして共栄していけるのか？
エンドポイント評価技術 (SACM)	• セキュリティの脆弱性評価技術(OVAL)、エンドポイントの資産情報(AI)の共有など、発展してくれることで、オペレーションは本当によくなるのか？
シグナリング技術 (DOTS, I2NSF)	• DDoS対策において、フィルタリングルールをシグナリングするのみで十分か？ • NSFのセキュリティ設定で、具体的に設定したいルールはどのようなものか？(I2NSFの現状のものにinputしなくて大丈夫か?)