IETF94におけるセキュリティオートメーション技術 (dots, i2nsf, mile, sacm)

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

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

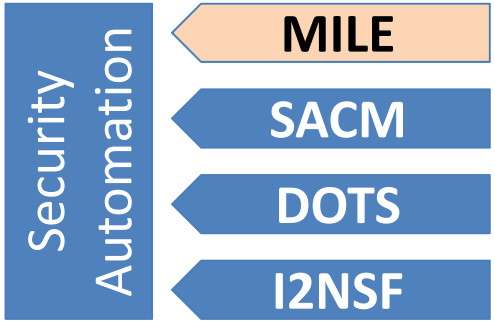
MILE : Managed Incident Lightweight Exchange — *IETF 82 ～*
インシデント情報の交換技術を検討

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

インシデント情報の交換技術を検討する
IETF MILE WG



MILE WGの概要

目的

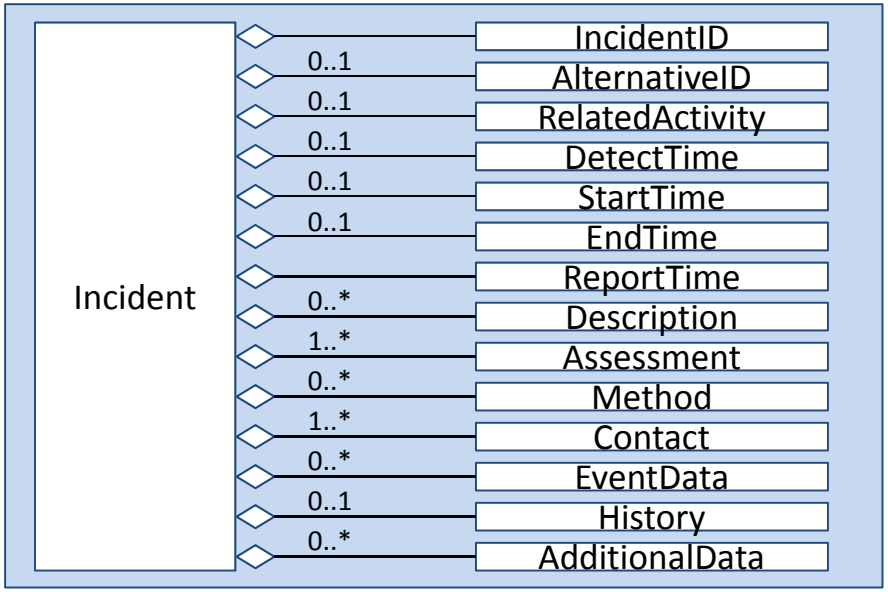
- MILEは、セキュリティインシデントに関する情報交換技術を検討
  - MILE (Managed Incident Lightweight Exchange)はINCH WGの後続
  - human-to-humanのみならず、machine-to-machineの情報交換も検討
  - インシデント情報のrepresentation、交換の際のPolicy、交換の際のTransport、実装に向けたガイドラインなどを検討

Chairs

- Alexey Melinkov and Takeshi Takahashi

Base spec

- IODEF: Incident Object Description and Exchange Format
- インシデント情報のデータモデルを規定
- 実質的にXMLベース
- US-Certで活用実績有



MILE WGの主なドラフト

審議終了

- RFC 6545 – RID / RFC 6546 – RID over HTTP/TLS
- RFC 6684 – Extension Guidelines and Template
- RFC 6685 – Expert Review for IODEF Extensions
- RFC 7203 – IODEF-SCI (extension for structured information)
- RFC-7495 – IODEF Enumeration Reference Format

現在審議中

- IODEF-bis — 1
- JSON-representation of IODEF — **Data representation** — 2
- Resource-Oriented Lightweight Indicator Exchange — 3
- XMPP-based IODEF exchange — **Transport** — 4
- IODEF implementation draft — 5
- IODEF guidance — **Guidelines** — 6

現在検討中のドラフト(1/3): Data representation

1 IODEF-bis

内容

- IODEFのdata modelを現状に合わせてreviseし、version 2とする

進捗

- WGLCを終了、現在editorのdraft update待ち
- 年明けあたりにIETF WGLCを実施する予定

2 JSON-representation of IODEF

内容

- 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

進捗

- IETF 94会合では、IODEFのJSON representationはすぐには難しい、という発表があったものの、IODEFの一つのprofileとしてJSON representationを検討することが重要との議論有
- IDEAという、CESNET (Czech)が独自に構築してきたJSON representationをベースに、IODEFのprofileを今後検討していく可能性が議論された

現在検討中のドラフト(2/3): Transport

3 Resource-Oriented Lightweight Indicator Exchange

内容

- インシデント情報をネットワーク上で交換する技術
- 情報フィードを作り、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”

進捗

- 現在WGLC中

4 XMPP-based IODEF exchange

内容

- SACMにて提案されていたXMPP grid draftについて、MILE向けprofileを作成したもの
- IODEF文書をXMPPを用いて交換する方法を記述

進捗

- IETF 94においては、MILEにて検討すべき技術であるとの議論を実施
- WG draftにするにはrecharterが必要

現在検討中のドラフト(3/3): Guideline

5 IODEF Implementation draft

内容

- 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
- 毎回の会合において大きな変化が生じるdraftではない

進捗

- 次回会合にて、WGLC実施をeditorは希望

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

内容

- IODEFの利用を促すため、IODEFの機能の中から実装が望まれる機能を説明
- 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

進捗

- Editorは早めの最終化を希望
- 現時点ではうまっていないsectionも存在するため、WGLCまであと数会期かかる模様

まとめと所感

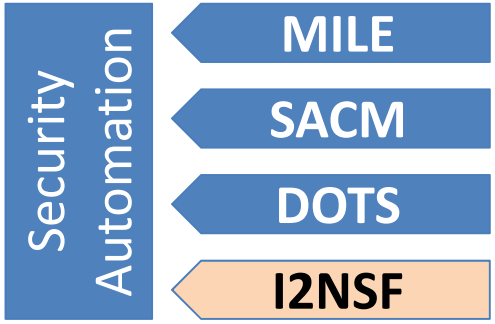
1. MILEでは、Data representation, Transport, guidelineの3つの領域にて、技術検討が進められている

2. 近年の最大の検討issueはdata representationを扱うRFC5070-bis (IODEF v2)であったが、これについては既にWGLCを終了しており、収束しつつある

3. 今後は、特にtransportに関するdraft 2件の検討の最終化が最大のissueとなる

4. さらにはrecharteringも検討が必要
   a. XMPP for IODEFやJSON-representation of IODEFは微妙にscopeに収まりにくい
   b. このタイミングで、何か仕掛けたい内容があれば、仕込みは簡単
   c. しかしながら、IETFにおいて本テーマについて十分なmomentumを維持するための施策を検討する必要有

I2NSFの概要



I2NSF WGの概要

目的	• 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
Chairs	• Linda Dunbar (Huawei) • Adrian Farrel(a consultant funded by Juniper Networks)
活動履歴	• 3回前 (IETF 91)にBoF • 2回前 (IETF 92)は、official meetingなし • 前回 (IETF 93)、working group forming BoF • 2015年9月18日に、正式にWG設立が決定 • 今回 (IETF 94)にて、第一回のWG meetingを開催

現在の検討内容

I2NSFの位置づけの明確化

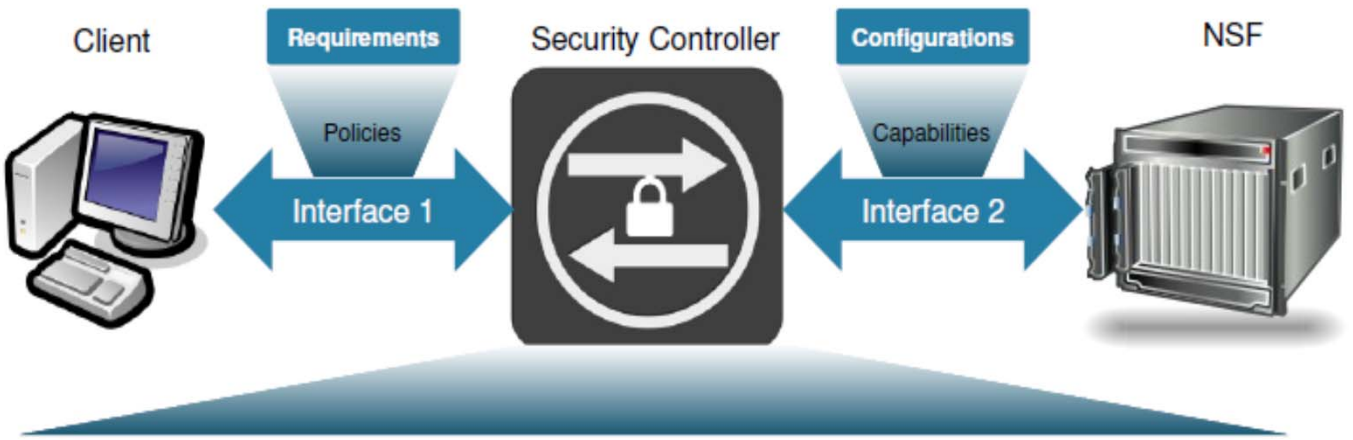
ユースケース	• Use Cases and Requirements for an Interface to Network Security Functions (NSF)
課題認識	• Interface to Network Security Functions (I2NSF) Problem Statement
フレームワーク	• Framework for I2NSF
ギャップ分析	• Analysis of Existing work for I2NSF

I2NSF内のsolution技術検討

情報モデル	• Information Model of I2NSF Capability Interface
SDN活用	• Software-Defined Networking Based Security Services using I2NSF
I2NSFデモ	• Interface to Network Security Functions Demo Outline Design
新規ドラフト	• User-group-based Security Policy for Service Layer • Inter-Cloud DDoS Mitigation API • Remote Attestation Procedures for vNSFs through the I2NSF Security Controller • The Capability Interface for Monitoring NSF in I2NSF

I2NSFでのユースケース検討

抽象化モデル



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

具体例

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
- 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
- その際の作業を簡略化。また、ミスを低減

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。ユーザの契約・契約解除に合わせてFirewallを設置・解消
- ユーザ側は、従来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

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

I2NSFのフレームワーク

- 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リファレンスモデル、およびフレームワークレベルで定義
  - 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

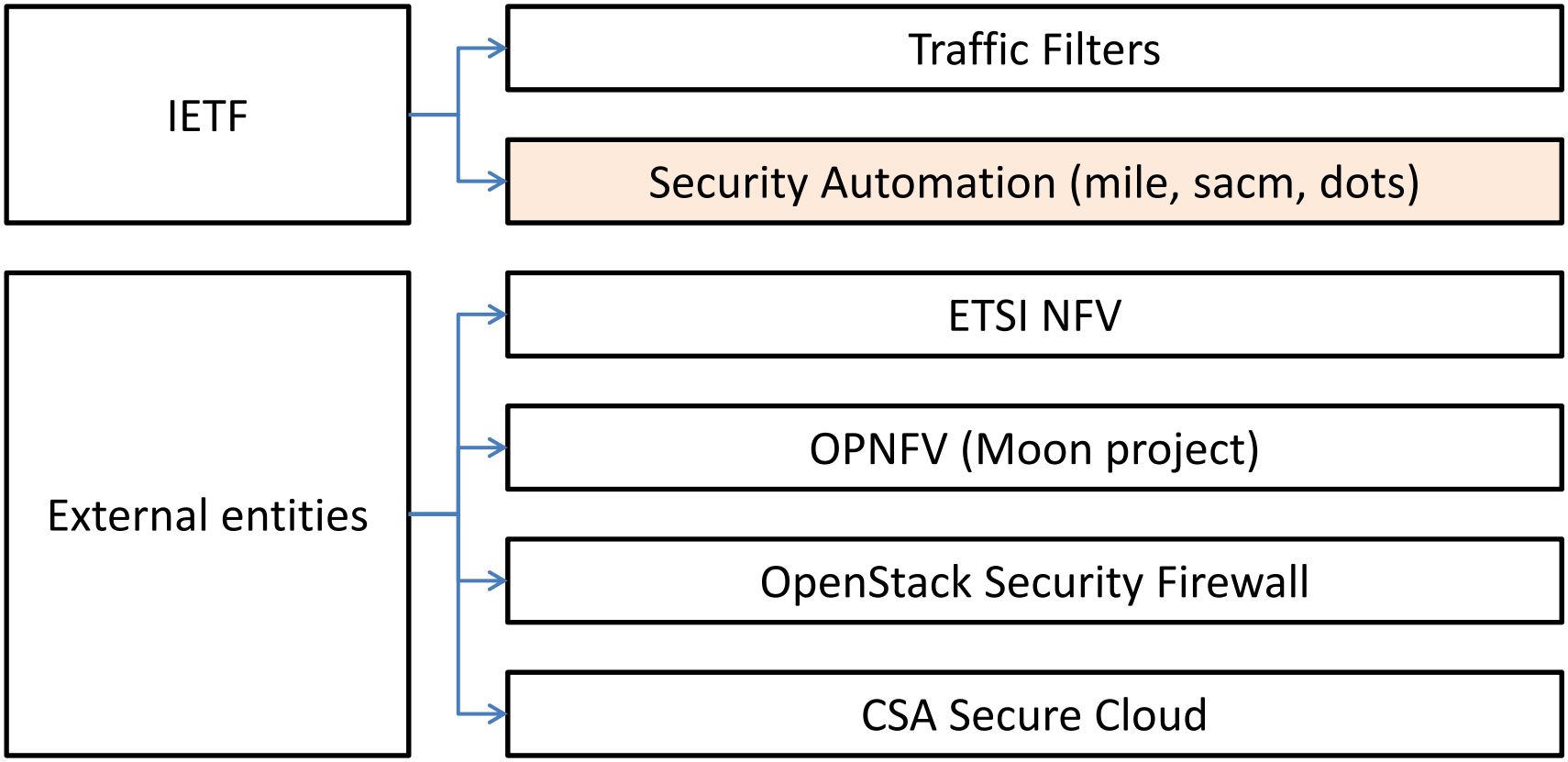
- I2NSFには2つのレイヤの概念が存在
  - I2NSF Capabilityレイヤ: NSFの機能レベルで、NSFをどのように制御・監視すべきかを定義。すなわち、I2NSFでは、NSFの制御と管理が起動され、実施され、監視されるインターフェース群を標準化する。
  - I2NSF Servicerレイヤ: クライアントのセキュリティポリシーをいかに表現し、監視するかを定義

- 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

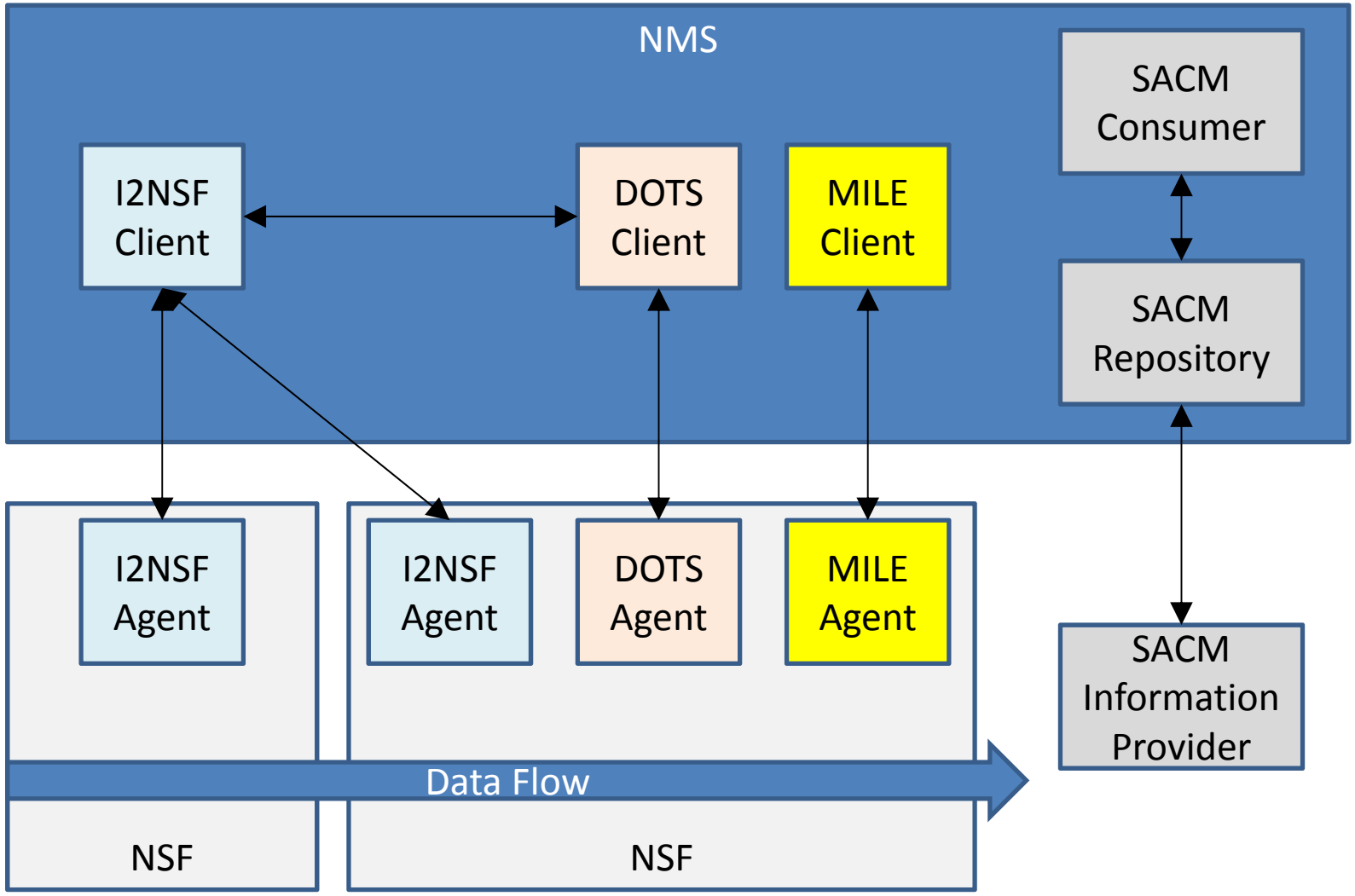
Gap分析

- 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



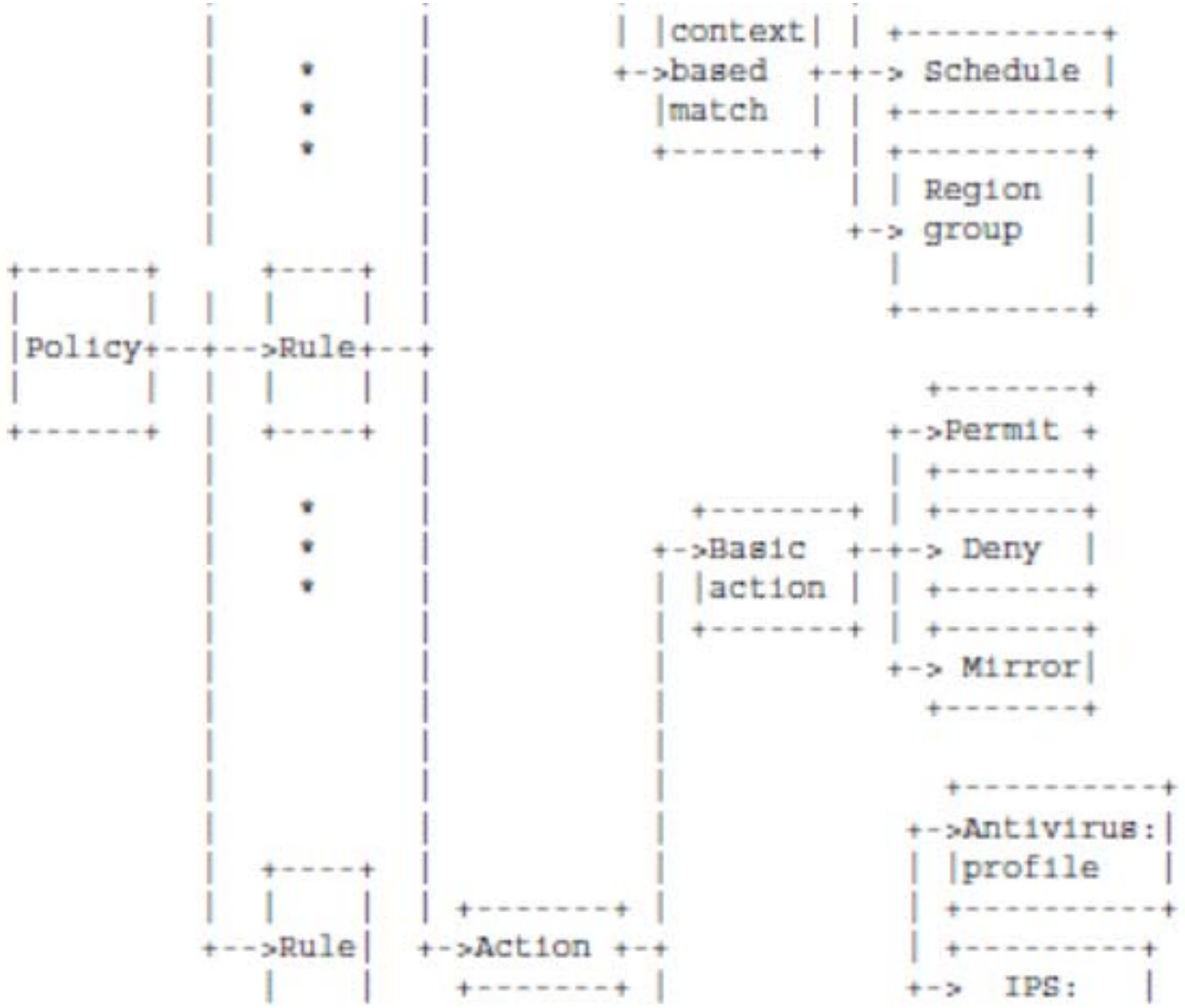
Source: draft-hares-i2nsf-gap-analysis-00.txt

Security automation works



Source: slides-93-i2nsf-0.pdf

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

新規ドラフト紹介@IETF94

User-group-based Security Policy for Service Layer

- ユーザグループごとにセキュリティ設定を実施するフレームワークをI2NSFのコンテクストの中で提案
- 現時点では、本テーマをI2NSF WGの中で扱うかどうかを探るためのdraftの書き方となっており、問題提起が主眼
- 特に反対はないが、相変わらずTerminologyを気を付けろ、との議論のみ

Iner-Cloud DDoS Mitigation API

- タイトルの通り、DDoS対策向けのAPIをI2NSFで定義しようとするもの
- 議論では、DOTSとの接点となり、scope分けに注意しつつ進めていきたいなどのコメントが出された

Remote Attestation Procedures for vNSFs through the I2NSF Security Controller

- vNSFとそこで設定されているPolicyがSecurity Controllerにより正しくenforceされていることの証明をユーザに提供する技術を提案
- ありがとう、とのコメントで終了

The Capability Interface for Monitoring NSF in I2NSF

- I2NSFのcapability Interfaceでどのように情報を収集し、そしてその収集した情報をどのように報告するかについて、その議論の必要性を提案
- 議論では、現在はこれを議論するインフラがI2NSFにはない。MILEなどを検討するのも一つの方法かもしれないとのコメント有

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
- I2NSFは、その活動にいくつかの企業(JuniperやHuawei)が投資しているため、具体的な成果が期待できる
- 質疑応答の中でよく議論されるservice layer関係のTerminologyおよびscope認識の統一が喫緊の課題
  - Terminologyの合意形成がまだできていない
  - Policy federationなどのお話なども議論されている
  - OpenStackのGroup-based Policyを活用しようとの議論有
  - PICMの利用も議論されたが、SUPAの成果を利用すべきとの議論有