IETF93 報告会 on 2015/8/27

I2NSF@IETF 93の概要

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

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

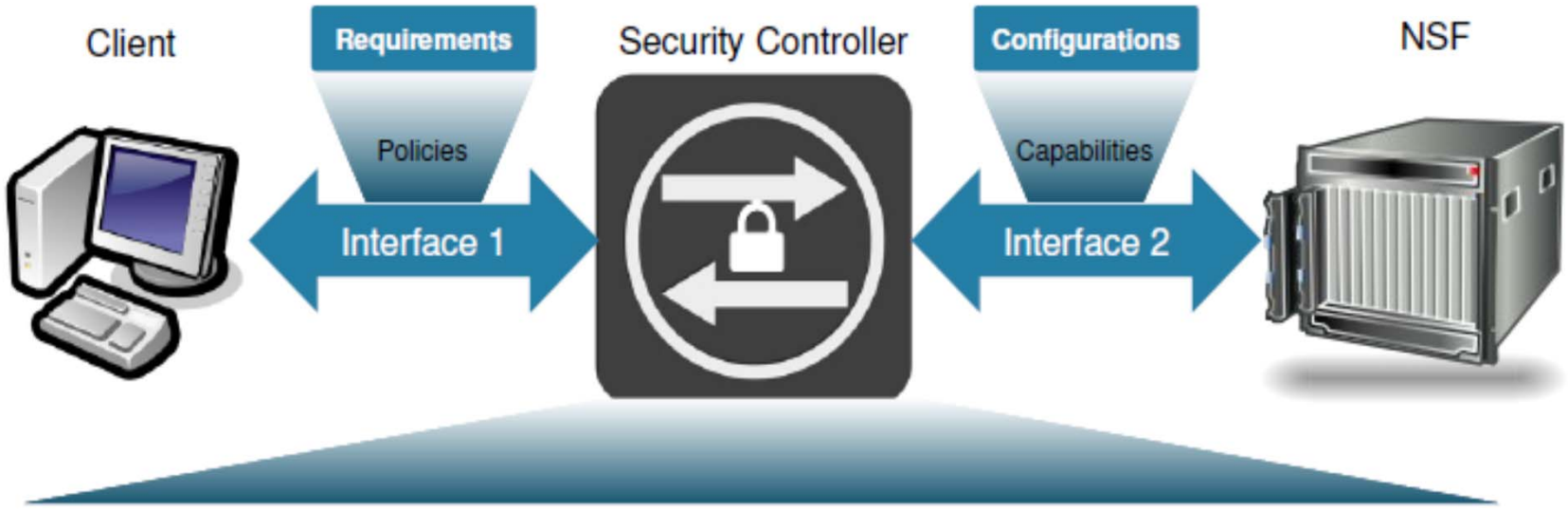
NSFの制御と監視を実施するための
情報・データモデルとソフトウェアインターフェースを定義する

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

- 8/27現在、charter textの最終化作業中

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

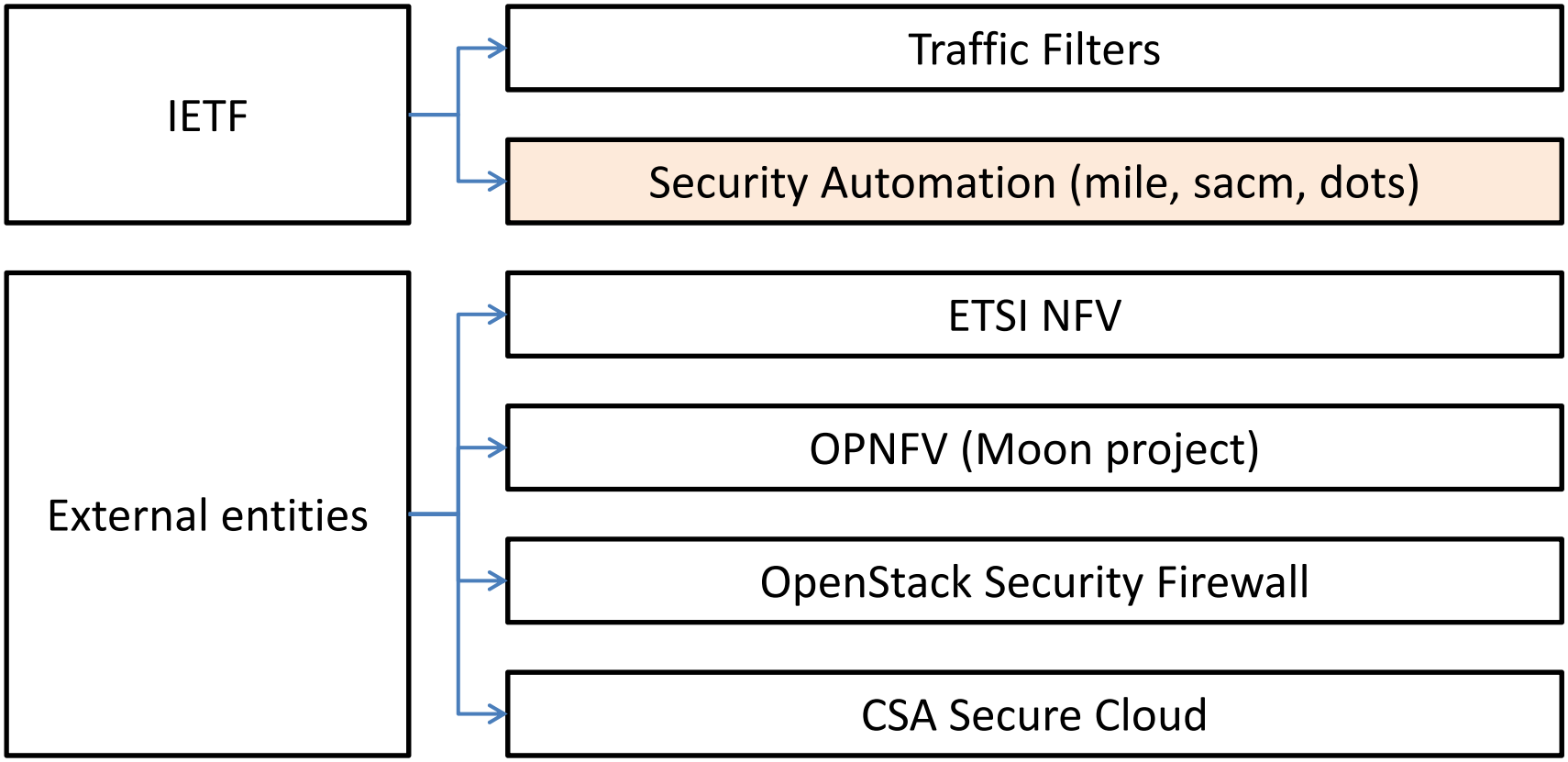
- I2NSFには2つのレイヤの概念が存在
  - I2NSF Capabilityレイヤ: NSFの機能レベルで、NSFをどのように制御・監視すべきかを定義。すなわち、I2NSFでは、NSFの制御と管理が起動され、実施され、監視されるインターフェース群を標準化する。
  - I2NSF Servicerレイヤ: クライアントのセキュリティポリシーをいかに表現し、監視するかを定義

- 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

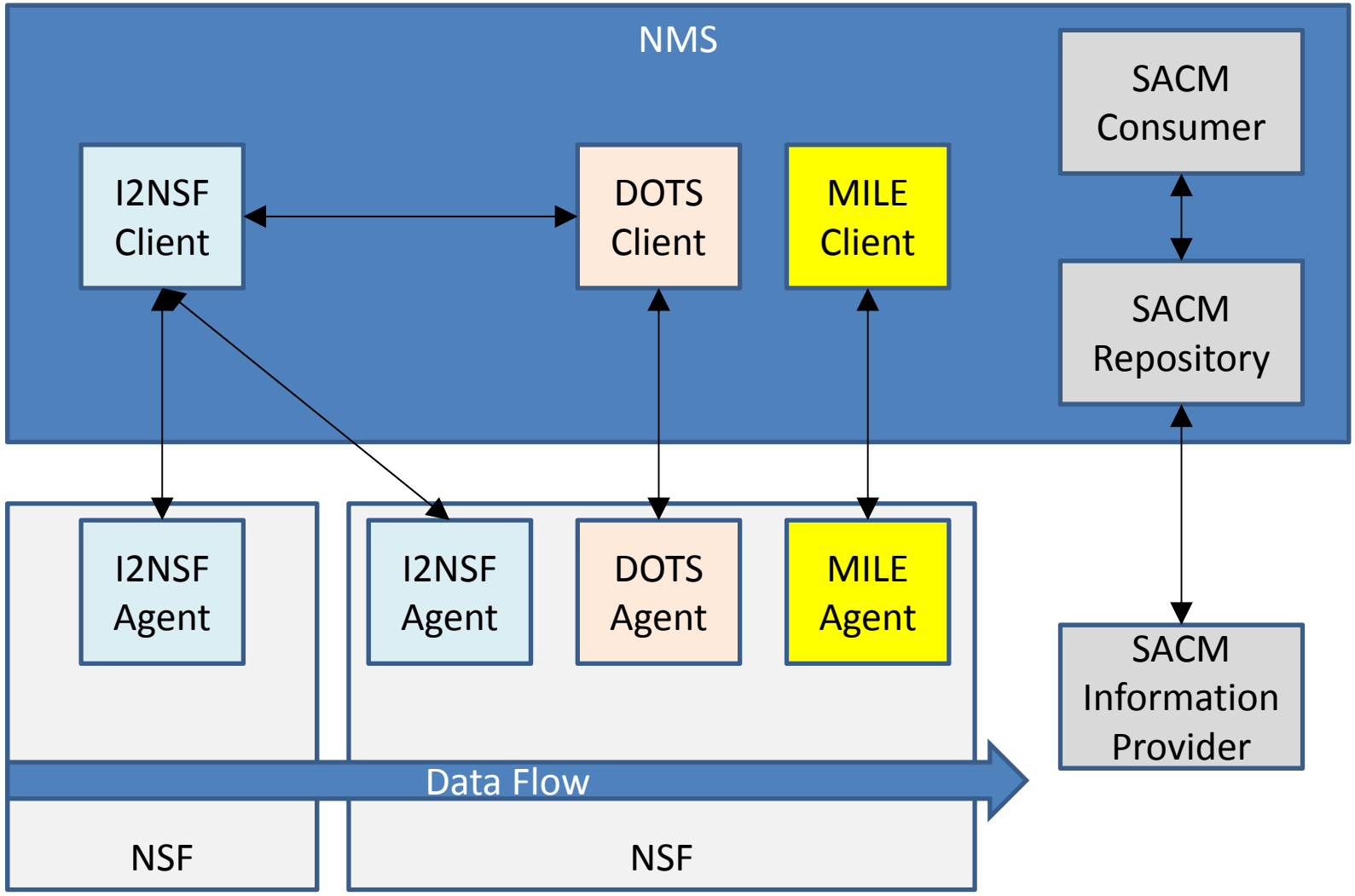
Gap分析

- 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

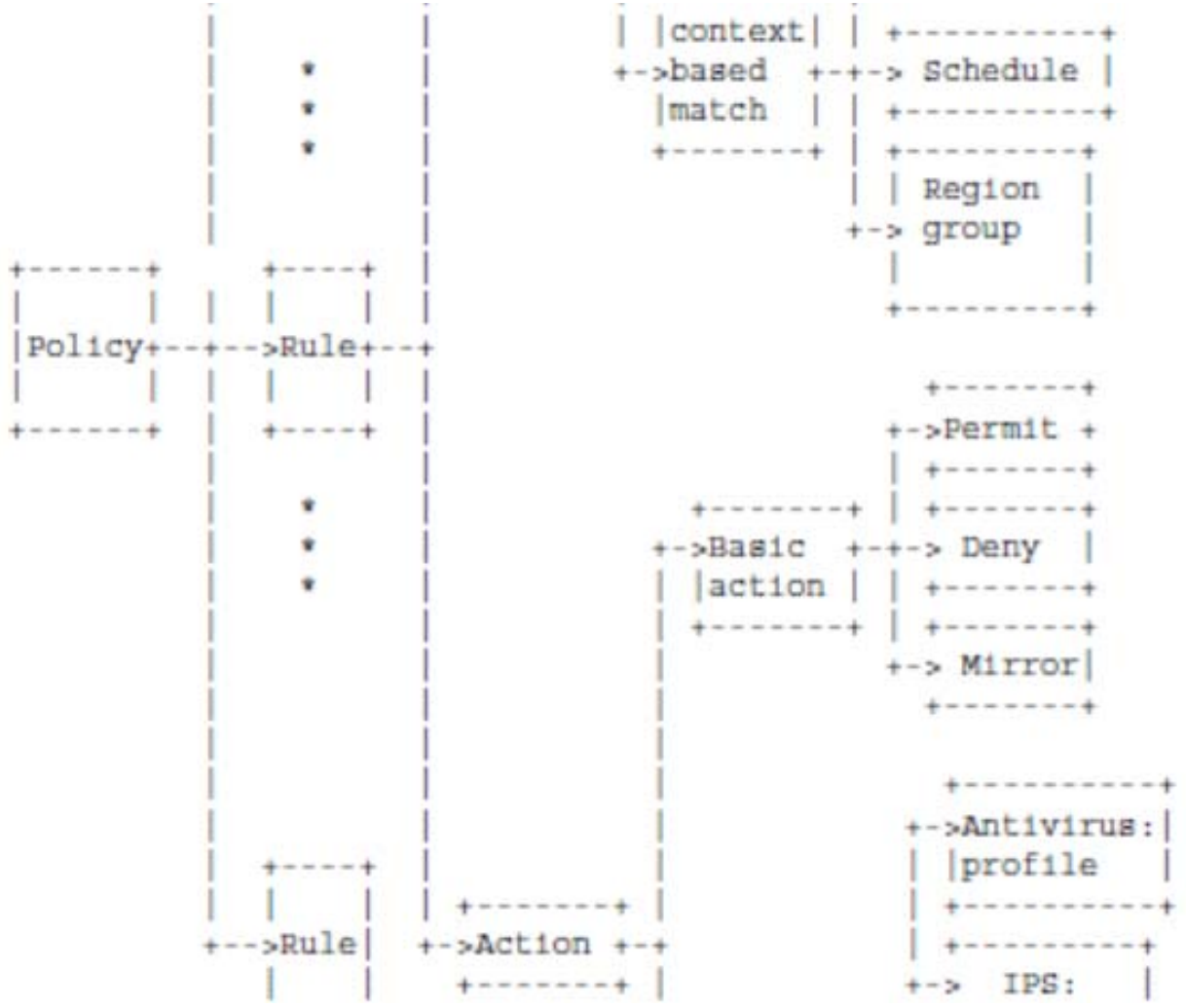
- Use Cases and Requirements for an Interface to Network Security Functions
- Interface to Network Security Functions (I2NSF) Problem Statement
- Framework for Interface to Network Security Functions
- Analysis of Existing work for I2NSF

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
- 今後の動向を注視したい