

MILE, SACM, DOTS (BOF)

宮本 大輔

東京大学 / NICT

daisu-mi@nc.u-tokyo.ac.jp

概要

- MILE: Managed Incident Lightweight Exchange
 - インシデント情報の構造化を行うRFC5070の再設計
- SACM: Security Automation and Continuous Monitoring
 - エンドポイントの監視と自動的な対応
- DOTS: DDoS Open Threat Signaling
 - DDoS対策に関連する情報のシグナリング

DOTS / DDoS Open Threat Signaling

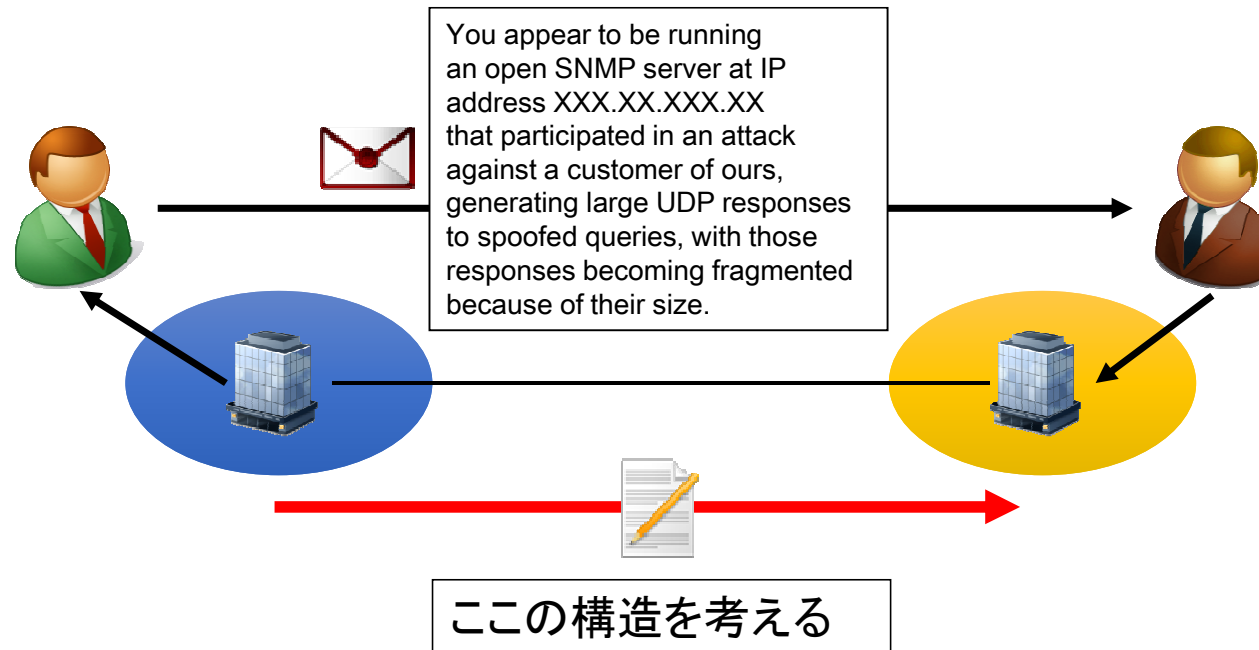
DOTS / DDoS Open Threat Signaling

- 日時
 - 2015/3/24 15:20–17:20
- 議長
 - R. Housley, R. Danyliw
- 議事録
 - <https://www.ietf.org/proceedings/92/minutes/minutes-92-dots>
- 参加者
 - 約150人
 - <https://www.ietf.org/proceedings/92/bluesheets/bluesheets-92-dots-01.pdf>

DOTS の目的

- 各社が別々に動かしているDDoS対策装置同士が通信し、現在の状況やデータを伝えられるような標準を考えましょう

(※宮本の理解)



DOTS の内容

- Open Threat Signaling using RPC API over HTTPS and IPFIX
- IPFIX Information Elements for inspecting network security issues
- Panel Discussion

Open Threat Signaling using RPC API over HTTPS and IPFIX (1)

趣旨

- CPE deviceやService Provider間でSOS をどう出せば良いですか？
- 内容は、Bandwidth 等の項目
- トランスポートはRPC API over HTTPSやIPFIX over UDP

ラベル	内容
Access Token	Pre-shared nonce
Key	イベント識別子
Time	イベント開始時刻
Type	攻撃の種類
Description	概要(テキスト)
Counter	pps, bps 等
Scope	進行状況
SOS	SOSビット
Thresholds	% of max

```
METHOD:POST
URL:{scheme}://{host}:{port}/ocs/api/cloudinfo
Request Body: {
  "device_ip":"<device ip>",
  "load_factor1": "<alias>",
}
Response Body: {
  "access_token":"<Access-Token>",
  "export_host":"<ip>"
  ...
}
```

Set ID = 2	Length
Template ID n	Field Count = 8
[1] Access Token	Field Length = n
[1] Key	Field Length = n
[1] Time	Field Length = n
[1] Type	Field Length = n
[1] Description	Field Length = n
[1] Scope	Field Length = n

Open Threat Signaling using RPC API over HTTPS and IPFIX (2)

- 議論

- CPE device がトラフィック異常を検知することが前提
 - Threshold はオペレータによって決める
- IPFIXは拡張性が高いし、使われかたの議論をするのは良い
 - が、そもそも攻撃受けている時にIPFIX over UDPでメッセージを受け取れるのか？
 - ただし SOS が概念にあることは良い
- 関連するアクティビティ
 - RFC5013: The Dublin Core Metadata Element Set
 - RFC6046: Transport of Real-time Inter-network Defense (RID) Messages
 - RFC7011: Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information

IPFIX Information Elements for inspecting network security issues

- 趣旨

- IPFIX で送れる統計情報を増やしましょう
 - HTTPのF5攻撃 (CC, Challenge Collapsar)
 - 通常の packets に見えるが、HTTP 2xx系の status コードが増える
 - Fragment
 - Fragment Overlap など、どのようなフラグメントをしているのか
 - ICMP echo/echo replyの速度
 - 普通の ping なら 1 pps だが、どのようなインターバルでやってきているのか
- 統計情報を書けるような拡張をすれば DDoS 脅威情報

Panel による課題抽出

- パネラーにとっての DOTS
 - (1) 標準があればベンダーのみならずカスタマーにとってもbeneficial
 - (2) DDoS 対策ソリューションはあるが、その機能拡張には関心がある
 - (3) 協調したインシデント対応が必要
 - (4) 軽量で、“deployable” な標準が求められる
 - (5) サイバー脅威への対応を進化させ、高速化を目指す
- 一番の問題は(WGとしての)SCOPE

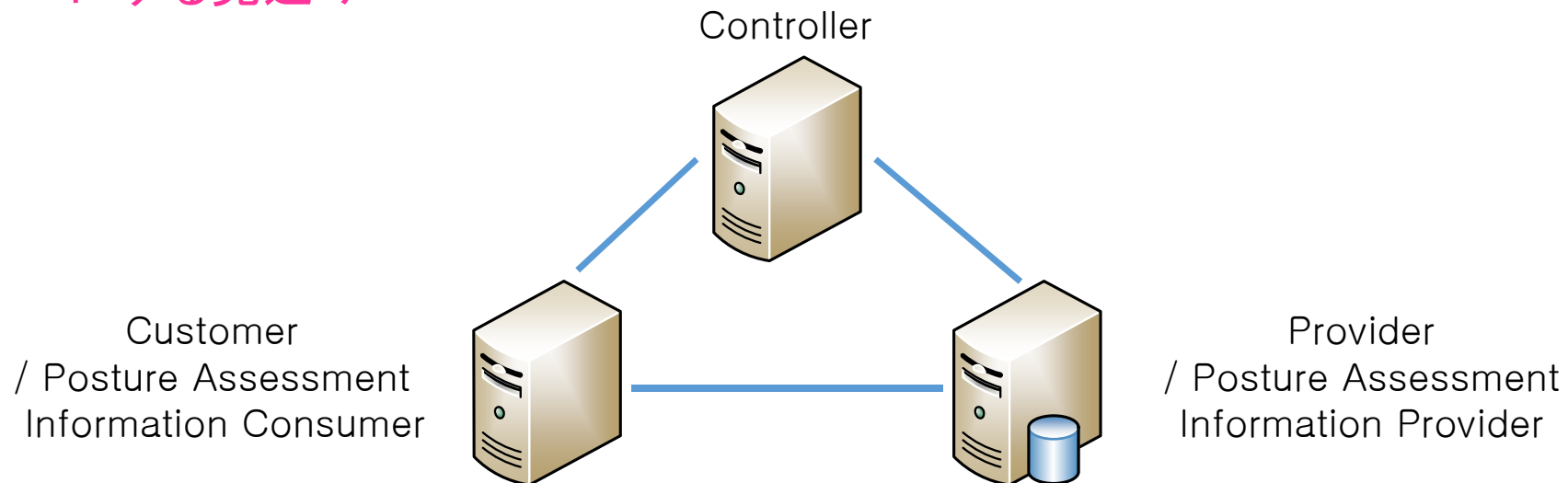
SACM / Security Automation and Continuous Monitoring

SACM

- 日時
 - 2015/3/23 9:00–11:30, 3/27 9:30–11:30
- 議長
 - D. Romascanu, A. Montville
- 議事録
 - <https://www.ietf.org/proceedings/92/minutes/minutes-92-sacm>

SACMの目的

- エンドポイントの状態(=設定)を観測し、レポジトリと照合して評価をするための標準を考えましょう
 - アーキテクチャ、情報モデル、要件定義と利用例、用語解説をまとめて RFC にする見込み



SACMの内容

Session 1: (2015/03/23)

- SACM Use Cases
- SACM Information Model
- SACM Architecture
- SACM Requirements
- SACM Terminology
- SACM Scope Considerations

Session 2: (2015/03/27)

- Requirements
- Architecture
- Information Model
- Liaisons and SACM

SACM の主要ドラフトの動向

- WGLCが終わっているドラフト
 - SACM Use Case
- WGLCを目指すドラフト
 - SACM Requirements 2015/5
 - DataModel については Operations のセクションを定義
 - SACM Architecture 2015/7
 - SACM Information Model 2015/11
 - SACM Terminology (未定?)
 - 用語解説。今回は簡潔化を行っている。

MILE / Managed Incident
Lightweight Exchange

MILE / Managed Incident Lightweight Exchange

- 日時
 - 2015/3/25 9:10–11:30
- 議長
 - A. Melniko, T. Takahashi
- 議事録
 - <https://www.ietf.org/proceedings/92/minutes/minutes-92-mile>
- 参加者
 - 約30人
 - <https://www.ietf.org/proceedings/92/bluesheets/bluesheets-92-mile-01.pdf>

MILE の目的

- IODEF (RFC5070) の機能拡張を整理しましょう
 - 機能拡張の経緯
 - RFC5070: IODEF の定義 (2007/12)
 - RFC5901: IODEF のフィッシング対策拡張 (2010/07)
 - RFC6685: IODEF の XML の名前空間の IANA による定義(2012/07)
 - RFC7203: IODEF の構造的な拡張 (2014/04)
- IODEFに関する実装や利用についての知見を広めましょう

MILEの内容

- The Incident Object Description Exchange Format v2
 - RFC5070-bisと呼ばれる IODEF の改訂
- MILE Implementation Report and its related activities
 - 宮本が担当している、IODEFの実装に関するサーベイ
- Resource-Oriented Lightweight Indicator Exchange
 - REST形式による IODEF の内容の交換についての検討
- IODEF Usage Guidance
 - IODEFの使い方に関するガイドライン

Mile Implementation Report に至る経緯 (IETF89)

- 実験報告

- IODEFを東京大学のインシデントレポートシステムに組み入れてみた

- 解決が難しい問題が発生した

- IODEFのフォーマットの難解さに伴う問題
- IODEFのこの項目に何を入れていいのかわからない問題

ライブラリの自動生成に関する問題

```
#!/usr/bin/perl
use XML::Pastor;
my $file = shift;
my $pastor = XML::Pastor->new();
$pastor->generate(
    mode => 'offline',
    style => 'single',
    schema => $file,
    class_prefix => 'IODEF::',
    destination => './', );
```

```
# perl xsd-generate.pl rfc5070.xsd
Pastor : Unexpected element 'any'
in schema!

<sequence >
  <any namespace="##any"
processContents="lax"
minOccurs="0"
maxOccurs="unbounded" />
</sequence>
```

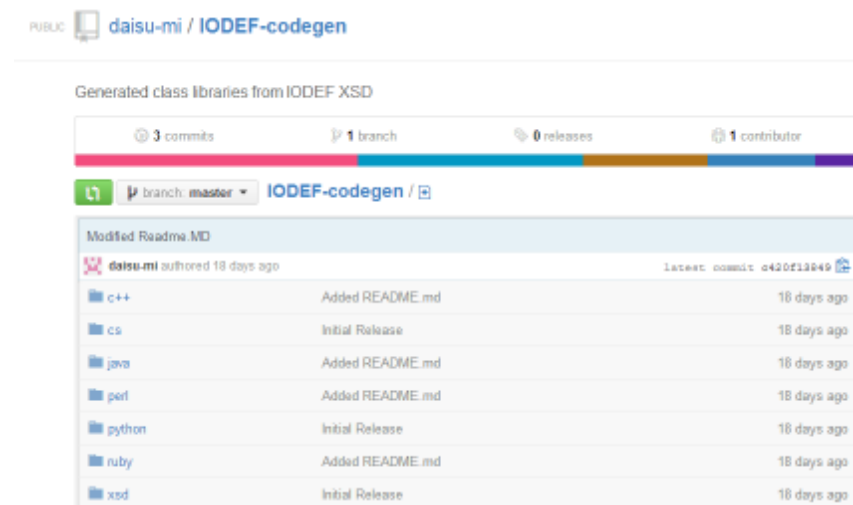
Code generator	Result for RFC5070.xsd
XML::Pastor (perl)	Error
RXSD (ruby)	Error
PyXB (python)	OK
JAXB (Java)	Error
Codesynthesis XSD (c++)	OK
XSD.exe (c#)	OK

ライブラリの自動生成問題

- ワークアラウンドの説明



- クラス名の命名規約との整合性



github.com/daisu-mi/IODEF-codegen

インシデントの分類問題

- JPCERT/CCとIODEFのインシデント分類の違い

Categories used in JPCERT	“type” attributes @ Impact Class
Phishing site	social-engineering
Web defacement	file ?
Malware propagation	file ? admin ?
Scan	recon
DoS/DDoS	dos
Control systems	ext- type?

ノードの役割の分類問題

- ノードの役割
 - メールサーバ、Webサーバ ...
- 複数の機能を持つ場合は？
 - Proxy Server : `<NodeRole category="www?"/>`
 - Web Mailer: `<NodeRole category="www?mail?"/>`
- 選択肢

```
client, server-internal, server-public, www, mail,  
messaging, streaming, voice, file, ftp, p2p, name,  
directory, credential, print, application, database,  
infra, log, ext-value
```


情報漏えいの可能性

- インシデント発生頻度の問題

```
<Incident ID="1">  
  <DetectTime>2013-09-11T04-57-00+09:00</DetectTime>  
  
<Incident ID="2">  
  <DetectTime>2013-09-11T05-02-34+09:00</DetectTime>  
  
<Incident ID="3">  
  <DetectTime>2013-09-11T05-09-12+09:00</DetectTime>
```

MILE Implementation Report (1)

- 実装の紹介
 - ベンダー実装
 - オープンソース実装
 - その他の実装
 - 知見の共有
- 経緯
 - Kathleen Moriarty 氏から宮本が引き継いだ
 - CMU の Chris Inacio氏が共同著者

MILE Implementation Report (2)

• ベンダーの実装

- Deep Secure
- IncMan Suite, DFLAbs
- Surevine Proof of Concept
- MANTIS Cyber-Intelligence Management Framework
- Threat Central, HP (予定)

• オープンソースの実装

- EMC/RSA RID Agent
- NICT IODEF-SCI implementation
- CERT Polska (NASK) n6

MILE Implementation Report (3)

- **その他の実装**

- NATO

- Collaborative Incident Management System
- Cyber Coalition 2013 用に製作
- Request Tracker のプラグインとして実装
- メッセージのメールにIODEF文書が添付され、情報交換が促進される仕組み

- **関連する実装**

- AirCERT
- JPCERT/CC ISDAS
- eCSIRT.net

MILE Implementation Report (4)

- 実装方法関連

- XSDからコンバートする知見の共有

- lodeflib (Python)

- <http://www.decalage.info/python/iodeflib>
 - NATO の Philippe Lagadec 氏が実装

- p5-XML-IODEF (Perl)

- <http://search.cpan.org/~saxjazman/XML-IODEF-0.11/>
 - REN-ISAC の Wes Young 氏が実装

RFC5070-bis

- IETF90での主な変更

- インシデントの分類の整理

- Impact@typeを廃止する
 - IncidentCategory (テキスト入力)に、組織ごとに異なるインシデントの種類を書いてもらう
 - SystemImpact (数値選択形式)に、システムへの影響を書いてもらう

- IETF91での主な変更

- Extending Attributes

(※現状維持されることになった)

```
<NodeRole category= "ext-value"  
ext-category= "extension value" >
```

```
<NodeRole category= "ext-value"  
ext-category= "extension value" >
```

```
IANA Registry "IODEFv2->NodeRole-category"
```