MILE & SACM

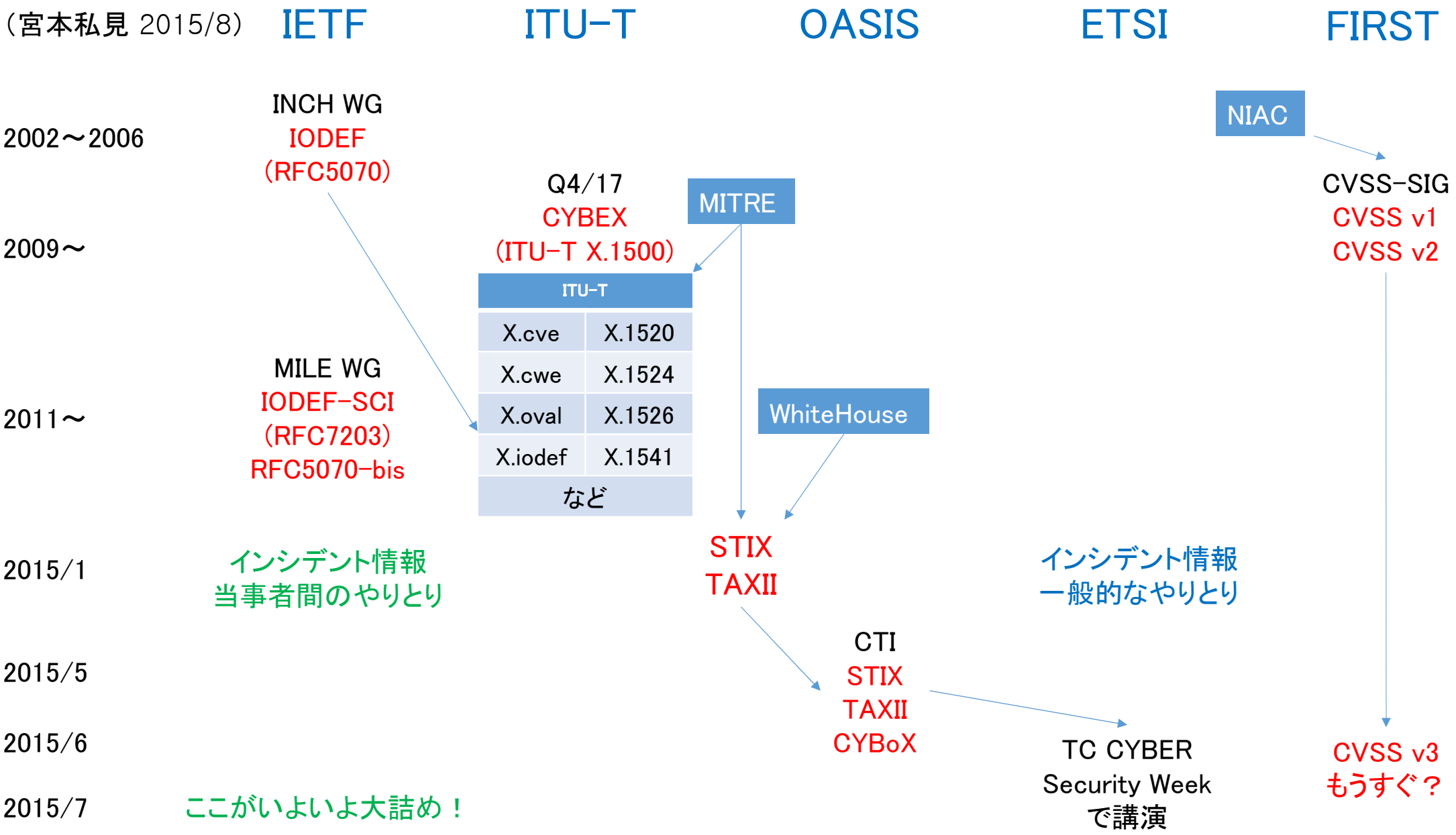
宮本 大輔
東京大学 / NICT
daisu-mi@nc.u-tokyo.ac.jp

概要

- MILE: Managed Incident Lightweight Exchange
  - インシデント情報交換の仕組みを考える
- SACM: Security Automation and Continuous Monitoring
  - エンドポイントの監視と自動的な対応

インシデント情報交換における重要な項目

- ポイント1：誰が誰に伝える？
  - 当事者間のやりとり
    - 「インシデントレスポンスに必要な情報の交換」
    - 例：サイバー攻撃の加害者と被害者
  - 一般的なやりとり（第三者間のやりとり含む）
    - 「サイバー攻撃の情報に関する一般的な情報の交換」
    - 例：国と，サイバー攻撃を受ける可能性のある企業
- ポイント2：誰にどうやって伝える？
- ポイント3：誰が何を伝える？


（宮本私見 2015/8）
IETF
ITU-T
OASIS
ETSI
FIRST
2002～2006
2009～
2011～
2015/1
2015/5
2015/6
2015/7
INCH WG
IODEF
(RFC5070)
Q4/17
CYBEX
(ITU-T X.1500)
MITRE
NIAC
CVSS-SIG
CVSS v1
CVSS v2
ITU-T
X.cve
X.1520
X.cwe
X.1524
X.oval
X.1526
X.iodef
X.1541
など
MILE WG
IODEF-SCI
(RFC7203)
RFC5070-bis
WhiteHouse
STIX
TAXII
インシデント情報
当事者間のやりとり
インシデント情報
一般的なやりとり
CTI
STIX
TAXII
CYBoX
TC CYBER
Security Week
で講演
CVSS v3
もうすぐ？
ここがいよいよ大詰め！

MILE / Managed Incident Lightweight Exchange

MILE

- 日時
  - 2015/7/22 15:50-17:20

- 議長
  - A. Melnikov, T. Takahashi

- 議事録
  - https://www.ietf.org/proceedings/93/minutes/minutes-93-mile

MILE の流れ

- 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の現在のタスク

- 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
- Flow-based event exchange Format
  - メッセージのフォーマット＆トランスポートに関する考察

RFC5070-bis

- WGLC に向けて微調整が進む
  - Service に Description を記述できるように (port80 -> port80, http)
  - Counter の単位が指摘できるように(packet -> packet, mbit, …)
  - Observableを1件ずつではなく Bulk で記述可能に
  - サンプルに例示されているホワイトスペースの削除(と統一)

- 議論されたテーマ
  - サンプルの拡充
  - RelatedDNS

```
<iodef:DateDomainWasChecked>2013-01-04T09:10:24+00:00</iodef:DateDomainWasChecked>
<iodef:RelatedDNS RecordType="MX">evildave.com MX prefernce = 10, mail exchanger = mail1.evildave.com</iodef:RelatedDNS>
<iodef:RelatedDNS RecordType="A">mail1.evildave.com internet address = 176.157.32.17</iodef:RelatedDNS>
<iodef:RelatedDNS RecordType="SPF">zuesevil.com. IN TXT ¥"v=spf1 a mx -all¥"</iodef:RelatedDNS>
```

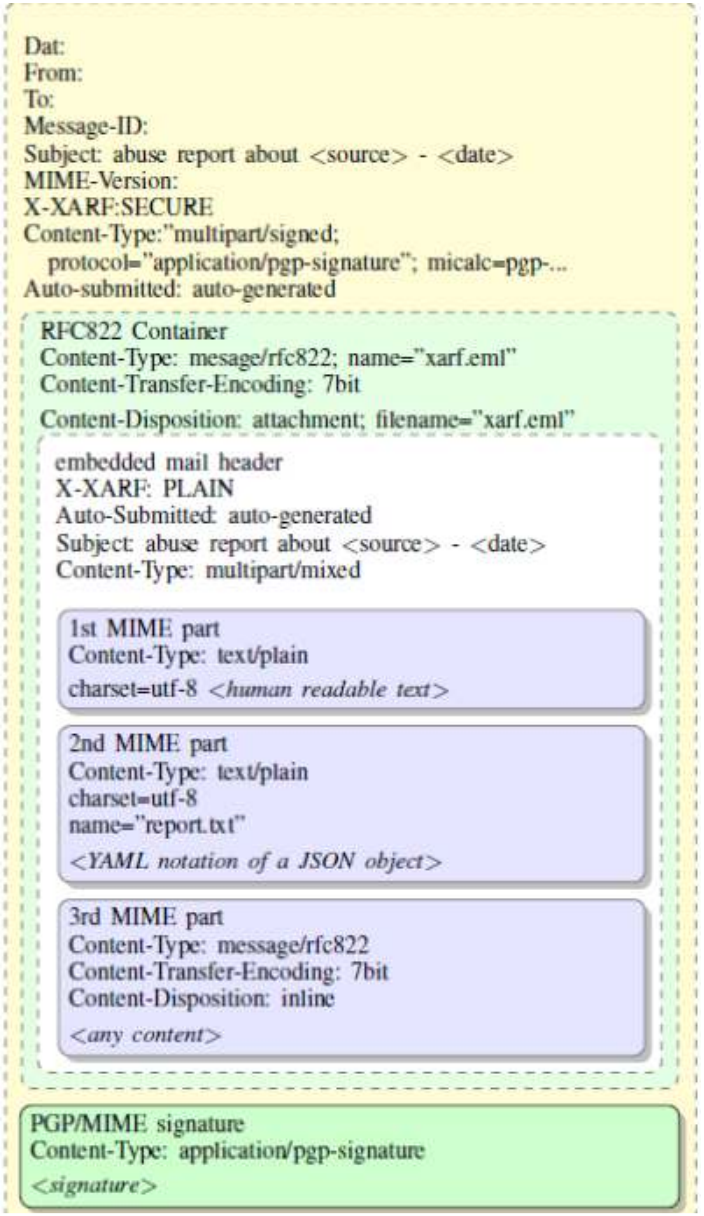
- WGLCは年内

MILE Implementation Report

- Missing Piece ほぼ埋まる
  - ISAC による使用例
    - APWG: フィッシングサイト情報のレポートツールがIODEFをサポート
    - ACDC: ボットネット報告ツールにおいて IODEF をサポート
    - REN-ISAC: インシデント情報に IODEF 形式の文書が添付される仕組み
  - Other Implementation
    - AirCERT, CyberFed における実装
- RFC5070-bis の後に WGLC となる可能性がある

FLEX

- トランスポートについての議論
  - SMTP
  - STOMP
  - XMPP
- フォーマットについての議論
  - FLEX, IODEF …
  - NetFlow …
  - XML / JSON



その他の話題（宮本私見）

- IODEF Usage Guidance
  - RFC5070-bis にともなって本格化する見込み，とりわけアラート情報（例：Darknet のモニタリング）などもRFC5070-bis を使ってシンプルに記載できるという知見が得られているので，Usageに記述されると思われる
- Resource-Oriented Lightweight Incident Exchange (RORIE)
  - RESTful / HTTP も有力なトランスポートであることから，IETF94, 95 からのキーとなるテーマとなる可能性が高い
- IODEF extensions for Reporting Cyber-Physical System Incidents (CPS)
  - その後大きな進展はない

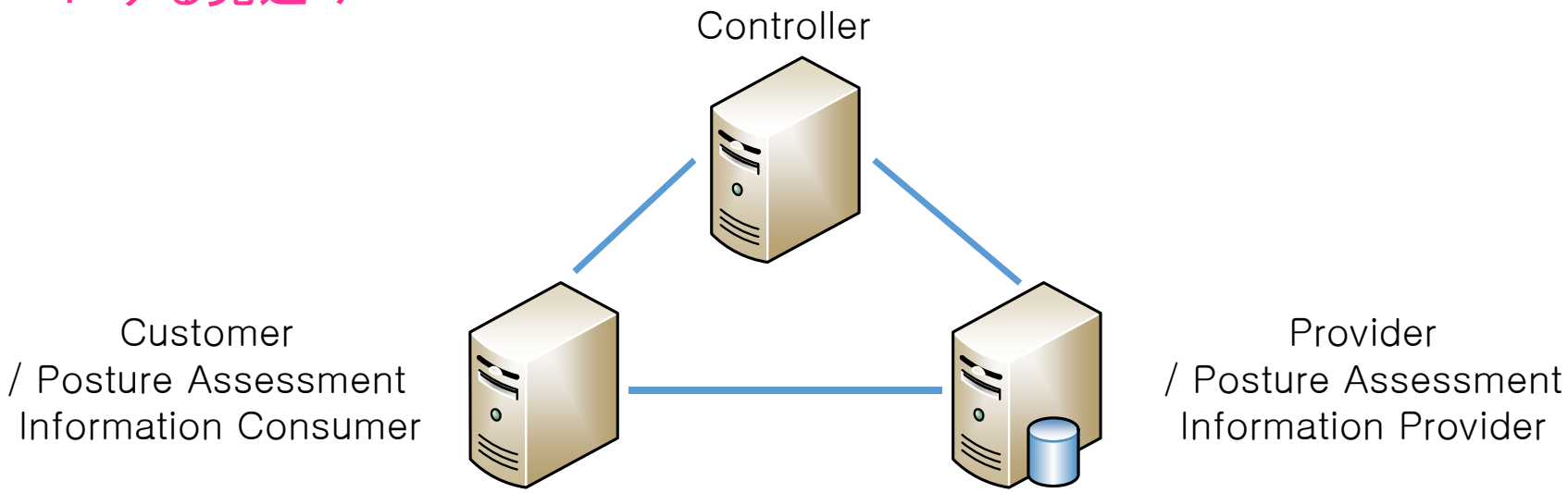
SACM / Security Automation and Continuous Monitoring

SACM

- 日時
  - 2015/7/20 13:00-15:30, 7/24 11:50-13:20
- 議長
  - D. Romascanu, A. Montville
- 議事録
  - https://www.ietf.org/proceedings/93/minutes/minutes-93-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: (2015/07/20)

- SACM Requirements
- SACM Terminology
- SACM Architecture
- SACM Information Model
- OVAL Assessment
- NEA Assessment
- ECP Mapping

Session 2: (2015/07/24)

- Requirements
- Architecture
- Information Model
- Terminology
- Way Forward

オープニングの議論

- トランスポートをどうするか？
  - RID (RFC6545: Real-time Inter-network Defense)
    - Does not scale
  - TAXII
    - Less Interoperability, does not scale
  - XMPP/Grid
    - Scale する
    - Vendor のサポートも可能

SACM の主要ドラフトの動向

- 作業自体は githubで協調編集されています
  - https://github.com/sacmwg

- 動向
  - Requirements : Open Issue あと4つ
  - Terminology : 18 (規模の大小はある: 用語の定義をどこでするか問題)
  - Architecture : 14 (provider/consumer間のinteroperabilityとdata model)
    - 一週間議論して整理 (capability, function, role)
    - 今後は I2NSF の terminology との整合性についても確認していく方針
  - Information Model: 22 (Endpoint ID design組と連携して実施)

SACM その他の動き

- 他の標準との兼ね合い
  - NEA Assessment
    - Network Endpoint Assessment (RFC5209)
    - Access Control の検証が主眼，SACM からするとスコープが小さい向きがある
  - ECP Mapping
    - Endpoint Compliance Protocol (Trusted Computing Group)
    - Trusted Network Connect (TNC) であれば産業界は注目してくれるか？
  - OVAL Assessment
    - Open Vulnerability Assessment Language (ITU-T X.1526)
    - VERY complex な点との兼ね合いが問題

まとめ

- MILE
  - いよいよ主要 WG Draft が大詰めである
  - 次の課題(「どのようにインシデント情報を送るか」)に
    シフトしていく可能性は現時点では高そう

- SACM
  - Open Issue は順調に減らしている
  - 他のWG / 他の Standard と兼ね合いを調べ, RFCにする予定の文書の社
    会的なインパクトにも着目している印象