

インシデント情報の交換技術を検討する IETF MILE WG

平成27年3月11日

(独)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

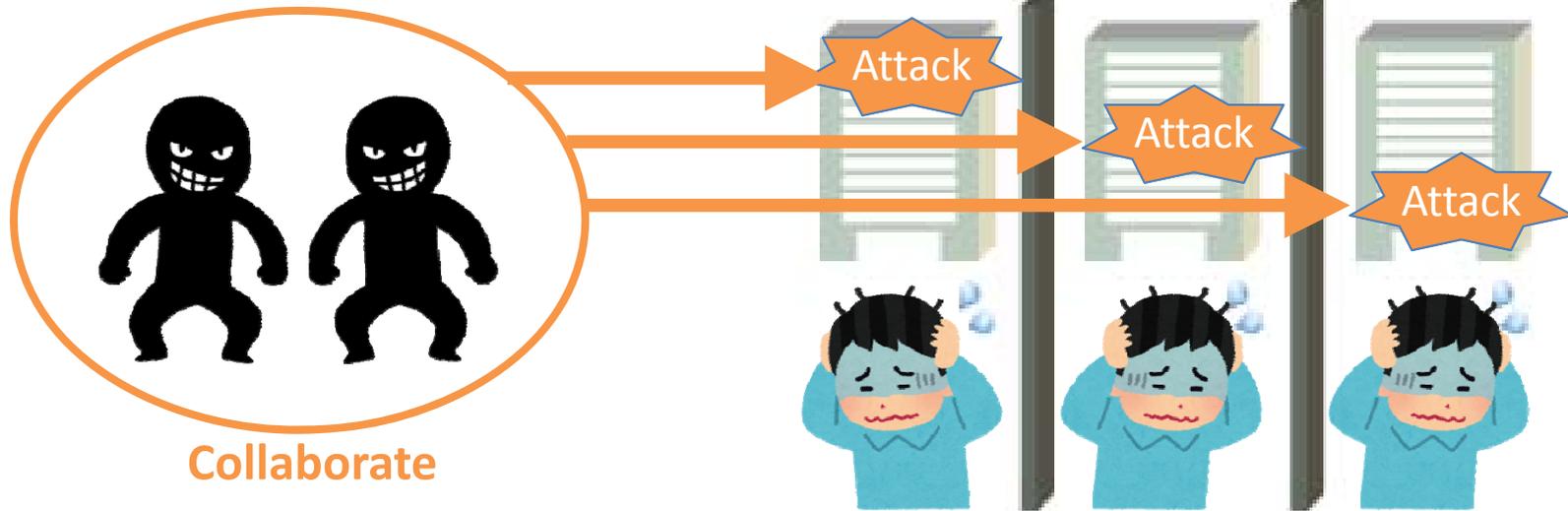


1. MILE WGの活動内容
2. ちょっとしたツール
3. 最近思うこと

問題認識

攻撃者

被害者(各組織)



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

2015/3/11

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
 - 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
 - INCH WGの後続であり、特にIODEFをベースとする

参加者

- 会場では20名程度と、小規模
 - US勢 + α
 - NIST, Mitre, USCert, McAfee, Cisco, EMC, ETH, etc. (Cert関係)
- Meetechoに10名程度

Chairs

Kathleen Moriarty
及びBrian Trammel

2014年
3月

- 元chair: それぞれSecurity ADとIABへ
- Chair: Alexey Melinkovと私
- Secretary: David Waltermire (NIST)

- 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

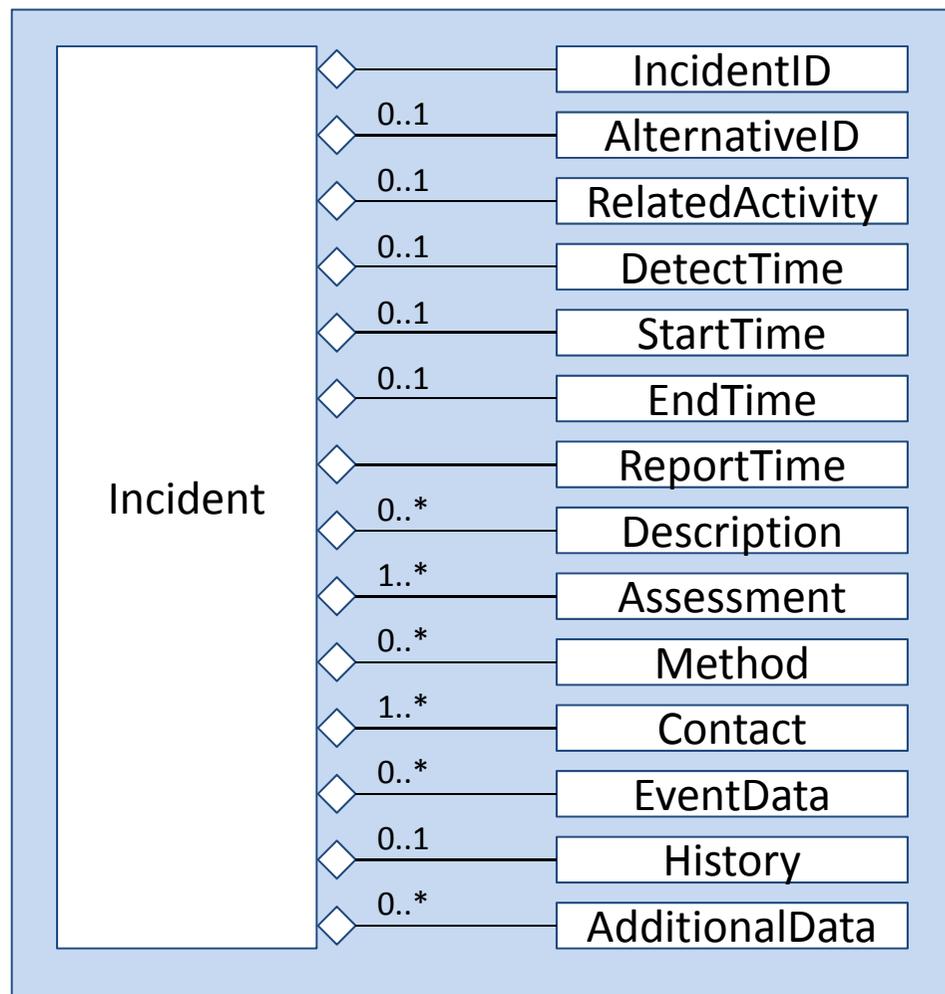


Fig. IODEFのデータモデル

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 – Guidelines and Template **2**
- RFC 6685 – Expert Review for IODEF Extensions **3**
- RFC 7203 – IODEF-SCI **4**
- RFC-tobe – IODEF Enumeration Reference Format **5**

現在
審議中

- Resource-Oriented Lightweight Indicator Exchange **6**
- IODEF-bis **7**
- IODEF implementation draft **8**
- IODEF cyber-physical extension **9**
- IODEF guidance **10**

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

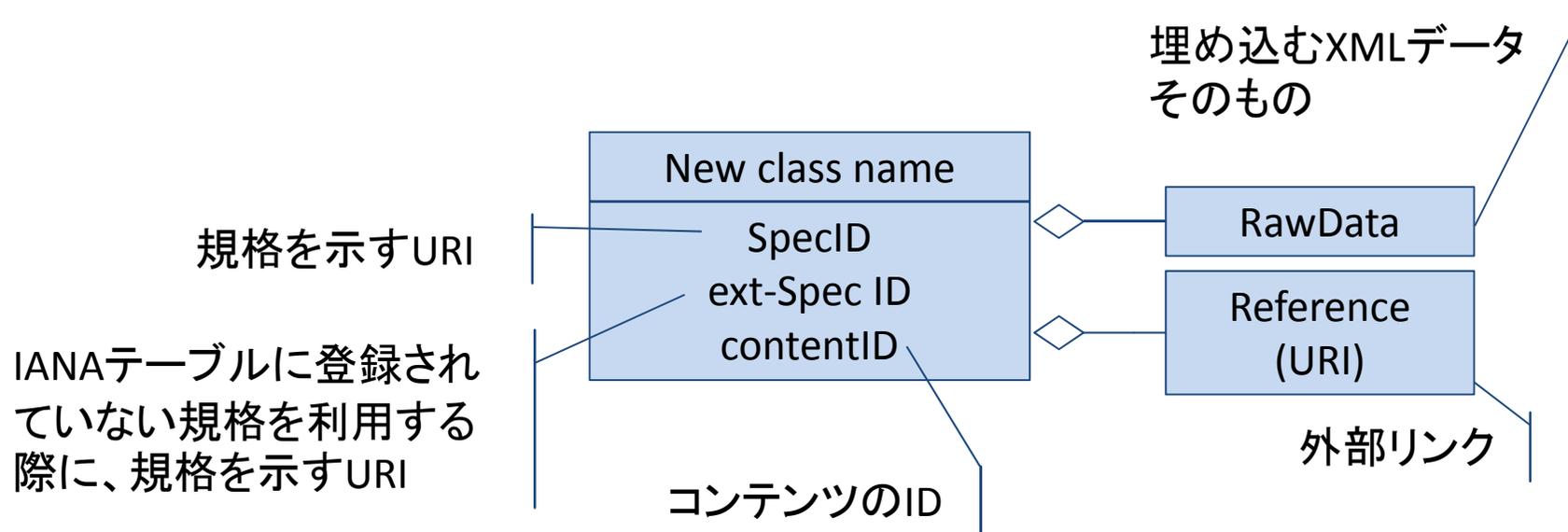
- IODEFを拡張する際のガイドラインと、そのテンプレートを規定したもの
- 本WGにて、IODEFの各種拡張が強く意識されていることを表している

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

4 RFC 7203 – IODEF-SCI

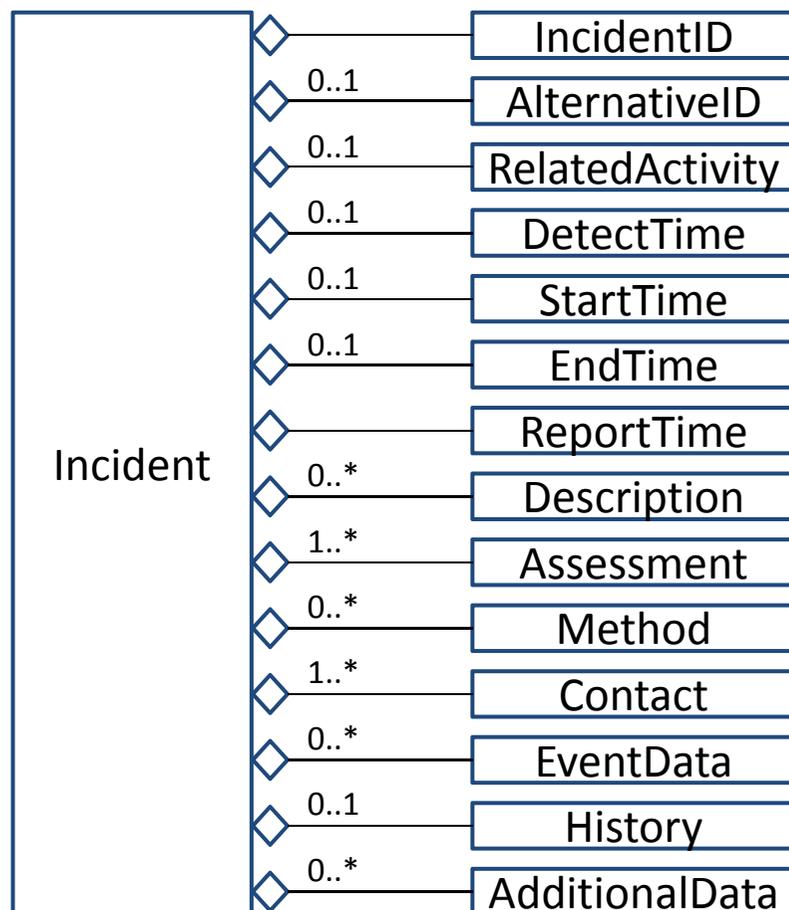
- IODEF-SCI: IODEF-extension for structured cybersecurity information
- IODEFの中の、機械可読でない部分をなるべく排除すべく、機械可読なSchemaをIODEFに組み込む技術
- IODEFを拡張して各種XML情報をIODEFに埋め込むインターフェースを定義



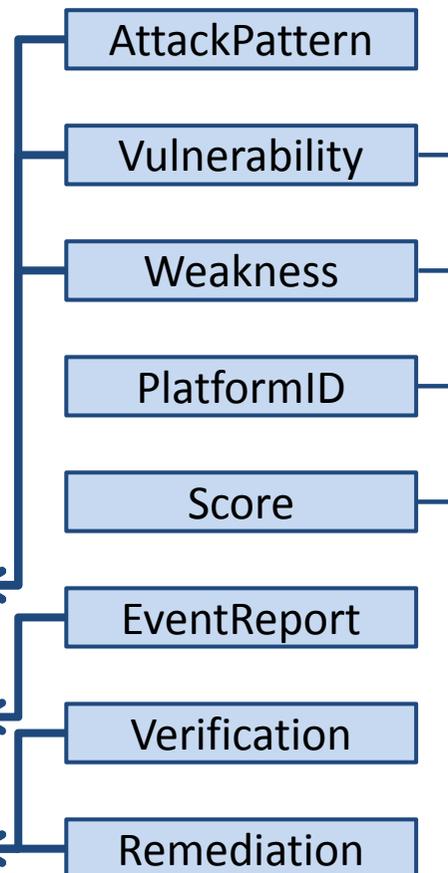
IODEF-SCI文書の構造



Original IODEF classes



Extended classes



Embedded info. (ex.)

CAPEC, MAEC, MMDEF

CVE, CVRF, CCE

CWE

CPE

CVSS, CWSS, CCSS

CEE

OVAL, XCCDF

CRE

Example: a sensor sends incident info with logs



```
<Method>
  <Description>An identifier of the exploited vulnerability is embedded</Description>
  <AdditionalData dtype="xml">
    <iodef-sci:Vulnerability SpecID="http://cve.mitre.org/cve/downloads/1.0"
      VulnerabilityID="CVE-2010-0483"/>
  </AdditionalData>
</Method>

<EventData><Record><RecordData>
  <Description>a Web-server event record</Description>
  <RecordItem dtype="xml">
    <iodef-sci:EventReport SpecID="http://cee.mitre.org">
      <iodef-sci:RawData dtype="xml">
        <cee:cee xmlns="http://cee.mitre.org/1.0/profile/" xmlns:cee="http://cee.mitre.org/1.0/"> ...
      </cee:cee>
    </iodef-sci:RawData>
  </iodef-sci:EventReport>
</RecordItem>
</RecordData></Record></EventData>
```

5 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
- 既にIESGからapprove済み。Standard-track RFC化目前

6 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”

7 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、などなど
- 残課題は下記の通り
 - 無効な証明書に対する対応
 - DNSレコードの記載・交換
 - “ext-*” attribute versus IANA table registration
- もうすぐWGLC: 本来はIETF91にてWGLCの予定であり、遅延気味

IODEF-bisの課題管理



Wikis:
[IESG IRTF](#)
[Dev RSOE](#)
[Chairs Edu](#)
[Tools BOFs](#)

NomCom

Areas

WGs:
[concluded...](#)
[flowpan](#)
[oman](#)
[orenun](#)
[Abfab](#)
[Adslmib](#)
[Alto](#)
[Ancp](#)
[Appsawg](#)
[Avtcore](#)
[Avttext](#)
[Behave](#)
[Bfcpbis](#)
[Bfd](#)
[Bmwg](#)
[Ccamp](#)
[Cdni](#)
[Clue](#)
[Codec](#)
[Conex](#)
[Core](#)
[Cuss](#)
[Dane](#)

Ticket	Summary	Component	Status	Type	Priority	Milestone
#1	Fix internationalization	rfc5070-bis	new	defect	major	
#2	Add better reference (citation) to RecordPattern@type=regex	rfc5070-bis	new	defect	major	
#3	Review implementation of extending enumerated values	rfc5070-bis	new	task	major	
#4	Add support for domain name meta data	rfc5070-bis	new	enhancement	major	
#5	Review all requirements key words (RFC 2119)	rfc5070-bis	new	task	major	
#6	Harmonize the specification for Reference with other WG activity	rfc5070-bis	new	task	major	
#7	Review completeness of NodeRole@category	rfc5070-bis	new	task	major	
#8	Review completeness of HistoryItem@action	rfc5070-bis	new	defect	major	
#9	Review completeness of @restriction	rfc5070-bis	new	defect	major	
#10	Review completeness of Impact@type	rfc5070-bis	new	defect	major	
#11	Add geolocation representation to Node/System	rfc5070-bis	new	enhancement	major	
#12	Define clear scope for the core data model relative to other WG documents and future extensions	rfc5070-bis	new	task	major	
#13	Review completeness of recent additions in 5070-bis	rfc5070-bis	new	enhancement	major	
#14	Add predicate logic for indicators	rfc5070-bis	new	enhancement	major	
#15	Missing description of classes introduced in -00 draft	rfc5070-bis	new	defect	major	
#16	Add support for describing if a device is physical or virtual	rfc5070-bis	new	enhancement	major	
#17	Review completeness of Incident@purpose	rfc5070-bis	new	defect	major	

Note: See [TracQuery](#) for help on using queries.

Download in other formats:
[RSS Feed](#) | [Comma-delimited Text](#) | [Tab-delimited Text](#)

Powered by [Trac 0.12.3](#)
By Edgewall Software

Administered by webmaster@tools.ietf.org

8 IODEF Implementation 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 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

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

- 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

11 Darknet system using IODEF

- Daedalusで利用する情報交換のフォーマットを共有
- 次回会合に向け、Daedalusの出力をIODEF対応にしていく

Agenda

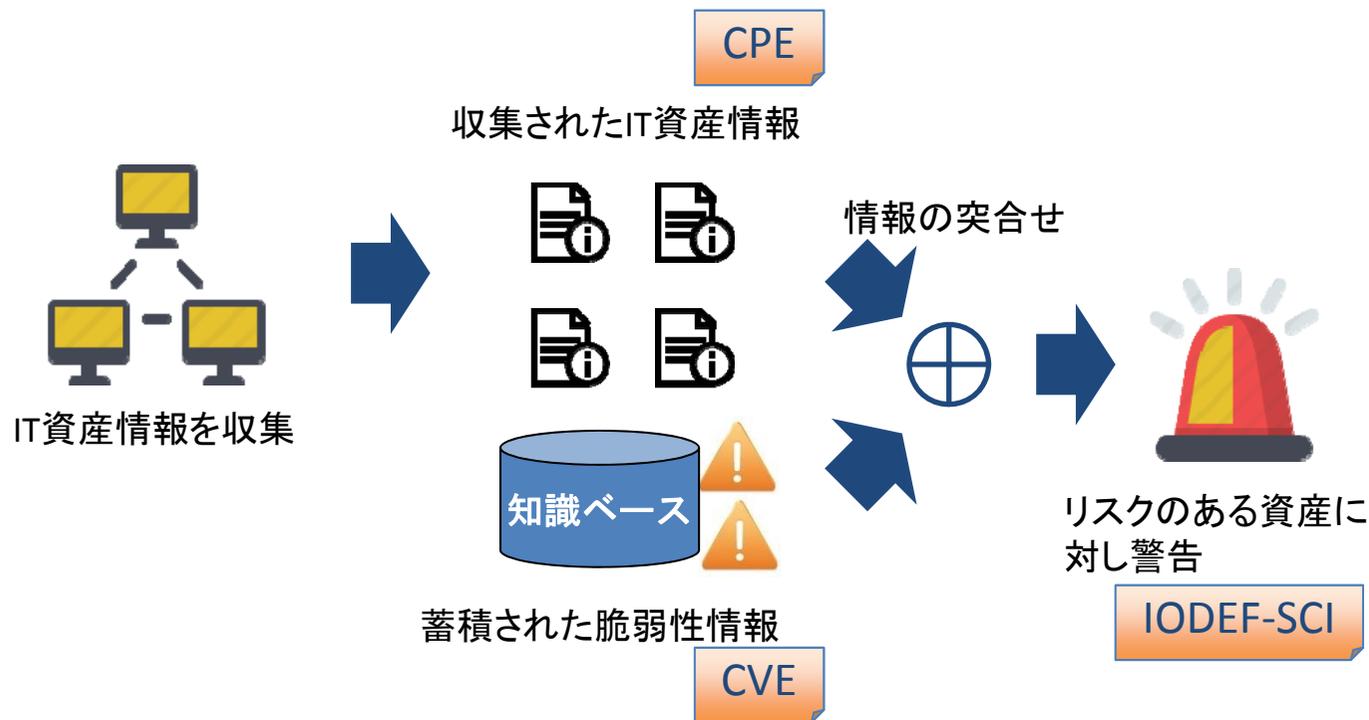


1. MILE WGの活動内容
2. ちょっとしたツール
3. 最近思うこと

規格を利用したセキュリティ自動化に向けて



- 昨今のセキュリティ関連schemaの発展は、様々な技術発展の可能性有
- アセット情報と脆弱性情報に関し、規格が存在しているので、それらをうまく使って、脆弱性管理を楽にするツールを作りたい



- 規格だけではうまくいかず、それをうまく使う工夫と、使ってくれる人間を増やしていく必要がある

Agenda



1. MILE WGの活動内容
2. ちょっとしたツール
3. 最近思うこと

- 国際標準化活動は、一つ一つの小さな技術をつなげて社会が求める技術を作る、もしくは技術の潮流を作る
 - 多くの人が使っこそ意味のある技術に対し、国際標準化活動は必須
 - 国際標準化活動をリードすれば、皆が使う技術の発展の方向性に対し自らの意思を反映可能
- 規格は、多くの人にその価値を認めてもらい、意味のあるものになる
 - 使われなければ無意味。皆で使っこそ意味がある
 - 一人で活動してもあまり意味はない
 - その点、経験豊かなIETFerは、小さなお話でも時間をかけて多くの人を巻き込み、コミュニティを大きくするのが上手
 - 完璧なものを作ることはすべてではない
- 日本においても、多くの人を巻き込む活動を、もっとセキュリティ分野で展開していきたい

- 国際標準化活動で技術を先導していくためには、ある程度の人数でモメンタムをつくって議論に参加するのが有効
 - US勢は、国内での打ち合わせを経てから会合に臨んでいる模様
 - どうやら、国関係の機関が資金面で後押ししている模様
 - 最近では、多くのWGにてUse CaseやRequirementの議論で、十分なaudienceを引きつけるのに時間を費やしているWGも多い
- 日本からのSec Areaへの参加者を増やし、お互いに連携を強めていければ幸い
 - 日本に閉じる必要はないが、地理的に近い参加者から連携するほうがコストは低い
 - そのためにはISOC-JPをはじめとした、各種コミュニティ活動の場所を活用していけるのではないかと
 - 実はco-authorを求めているdraftは結構あるので、こういったところから入るのも一つの手
- 既に参加している側として、標準化活動の場に対する魅力を育むと同時に、伝えていく努力をしたい

- 国際標準化活動で技術を先導していくためには、ある程度の人数でモメンタムをつくって議論に参加するのが有効
 - US勢は、国内での打ち合わせを経てから会合に臨んでいる模様
 - どうやら、国関係の機関が資金面で後押ししている模様
 - 最近では、多くのWGにてUse CaseやRequirementの議論で、十分なaudienceを引きつけるのに時間を費やしているWGも多い

**強力なモメンタムを
如何に作るか？**

- 日本からのSec Areaへの参加者を増やし、お互いに連携を強めていければ幸い
 - 日本に閉じる必要はないが、地理的に近い参加者から連携するほうがコストは低い
 - そのためにはISOC-JPをはじめとした、各種コミュニティ活動の場所を活用していけるのではないかと
 - 実はco-authorを求めているdraftは結構あるので、こういったところから入るのも一つの手

**如何にして日本からの
参加者を増やし、連携するか？**

- 既に参加している側として、標準化活動の場に対する魅力を育むと同時に、伝えていく努力をしたい

**如何にしてわかりやすい
魅力を作っていくべきか？**