



INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2004 情財第 1094 号

# 広域インシデント情報共有および分析技術の開発

---

## ソフトウェア仕様書

2005 年 10 月

独立行政法人 情報処理推進機構

<b><u>1. プロジェクト概要</u></b> .....	<b>1</b>
1.1. 背景.....	1
1.2. 目的.....	1
1.3. はじめに.....	2
1.4. 本開発の課題と期待される効果.....	2
1.5. 開発の概要.....	3
1.6. まとめ.....	7
<b><u>2. 基本定義</u></b> .....	<b>8</b>
2.1. イベント.....	8
2.2. インシデント.....	8
2.3. 広域インシデント DB.....	8
2.4. 広域インシデント.....	9
<b><u>3. 全体システム構成</u></b> .....	<b>10</b>
3.1. 広域インシデント分析・警戒システム.....	10
3.2. 広域不正アクセス追跡システム.....	11
<b><u>4. IODEF AUTHORIZING AP</u></b> .....	<b>14</b>
4.1. イベント情報の抽出.....	14
4.2. SIDA RECEIVER/ARCHIVER.....	17
4.3. SIDA IODEF GENERATOR.....	20
4.4. PACKET IODEF GENERATOR.....	23
4.5. IODEF SENDER.....	24
4.6. IODEF メッセージ生成.....	26
4.7. MANUAL AUTHORIZING.....	30
<b><u>5. IODEF DB MANAGER AP</u></b> .....	<b>33</b>

5.1. IODEF メッセージの受信と広域インシデント DB への格納 .....	33
5.2. 格納されたインシデント情報の閲覧 .....	36
5.3. 格納されたインシデント情報の検索 .....	36
5.4. 格納されたインシデント情報の選択と、新たな IODEF メッセージの生成 .....	37
<b>6. IODEF ANALYZER AP .....</b>	<b>38</b>
6.1. 世界規模の DoS インシデント分析 .....	38
6.2. 広く試みられている攻撃インシデント .....	41
<b>7. SNMP-IODEF GATEWAY .....</b>	<b>45</b>
7.1. 基本メッセージング仕様 .....	45
7.2. TRACEREQUEST .....	48
7.3. TRACEAUTHORIZATION .....	54
7.4. RESULT .....	55
7.5. 可視化 .....	58
<b>8. APPENDIX.....</b>	<b>59</b>
8.1. IODEF SCHEMA.....	59
8.2. RID SCHEMA.....	86

## 1. プロジェクト概要

### 1.1. 背景

社会基盤としてのインターネット上に次々と起こる新しいセキュリティインシデントに対応するため、世界的な連携を強化する動きが活発化しており、国や ISP を超えて連携(広域連携)できる新しいセキュリティシステムが必要とされている。

広域連携には、言語や特定のアプリケーションに依存しない標準化されたコミュニケーションの手段が不可欠である。そのため脆弱性情報の共有を目的として、世界各地の CERT が連携するための標準が提案され、IETF では、そのためのメッセージ交換の標準( IODEF: Incident Object Description Exchange Format ) を検討する INCH WG (Extended Incident Handling)が組織された。

IODEF 標準は 2001 年に議論が始まって以来、多くの検討がなされており、XML を基盤としたフォーマットとすることで基本合意している。しかし、一方で、非常に広範な期待が寄せられた結果、すべてを満たすメッセージの実現が難航している。

### 1.2. 目的

本技術開発では、広範囲なインシデント情報の共有および分析技術に関する技術開発を目的とし、現在 CERT 間の連携を目指して IETF 等で議論されているメッセージ交換の標準( IODEF: Incident Object Description Exchange Format ) を活用した以下のようなシステムを開発する。

- 広域不正アクセス追跡システム
- 広域インシデント分析・警戒システム

#### 1.2.1. 広域不正アクセス追跡システム

追跡技術は、セキュリティの観点から、他組織のセンサに問い合わせを出すことが難しいため、実際には世界的な連携ができずそのことが大きな課題となっていた。

そのようななか、2004 年 2 月、このような追跡を行うための連携手段 RID: Incident Handling:Real-Time Inter-Network Defense が INCH WG に提案され、今後 IODEF の一環として統合されることとなった。

そこで本技術開発では、課題となっていた追跡システムの広域連携に IODEF 標準を利用する技術を開発する。

### 1.2.2. 広域インシデント分析・警戒システム

本技術開発では、現在各所で個別に管理しているインシデント情報を IODEF 標準案に準拠した形で出力し、それらをネットワーク経由で収集することで、広域インシデントとして分析できる広域インシデント情報 DB を構築する技術の開発と、蓄積された広域インシデント情報 DB を分析して、広域インシデントとして警戒のために情報提供する技術を開発する。

### 1.3. はじめに

社会基盤としてのインターネット上に次々と起こる新しいセキュリティインシデントに対応するため、世界的な連携を強化する動きが活発化しており、国や ISP を超えて連携(広域連携)できる新しいセキュリティシステムが必要とされている。

広域連携には、言語や特定のアプリケーションに依存しない標準化されたコミュニケーションの手段が不可欠である。そのため脆弱性情報の共有を目的として、世界各地の CERT が連携するための標準が提案され、IETF では、そのためのメッセージ交換の標準( IODEF: Incident Object Description Exchange Format ) を検討する INCH WG (Extended Incident Handling) が組織された。

本技術開発では、広範囲なインシデント情報の共有および分析技術に関する技術開発を目的とし、IODEF を活用した以下のようなシステムを開発する。

- ・ 広域不正アクセス追跡システム
- ・ 広域インシデント分析・警戒システム

上記によって、組織を跨いだインシデント情報の共有と、各地で試みられている定点観測システム[1]の連携に IODEF を活用し、より柔軟な連携を可能とする技術の確立を目指す。

### 1.4. 本開発の課題と期待される効果

本標準の早期普及と実践的なアプリケーションの構築を目指す。IODEF 標準の活用と、その具体的な運用経験を示すことで以下のような効果が期待できる。

- ・ インシデント情報の自動で迅速な共有化
- ・ インシデントの広域追跡の実現
- ・ 広域インシデント情報のエンドユーザ活用

IODEF 標準を用いてインシデント情報を広く配布、活用することで、インターネット全体の安全に大きく寄与することが期待できる。

### 1.5. 開発の概要

本開発は、基盤技術として、IODEF 標準案をサポートする API を開発する。開発された API を活用して、上記 2 種類の具体的なアプリケーションを開発する。

図 1 に IODEF 標準が想定している基本モデルを示す<sup>[4]</sup>。

#### 1.5.1. IODEF-API

最新の IODEF 標準案（2005 年 8 月現在）に基づいた API を開発した。図 1 の Interface の部分が API として実装されており、CSIRT の部分で様々なアプリケーションを構築することができる。

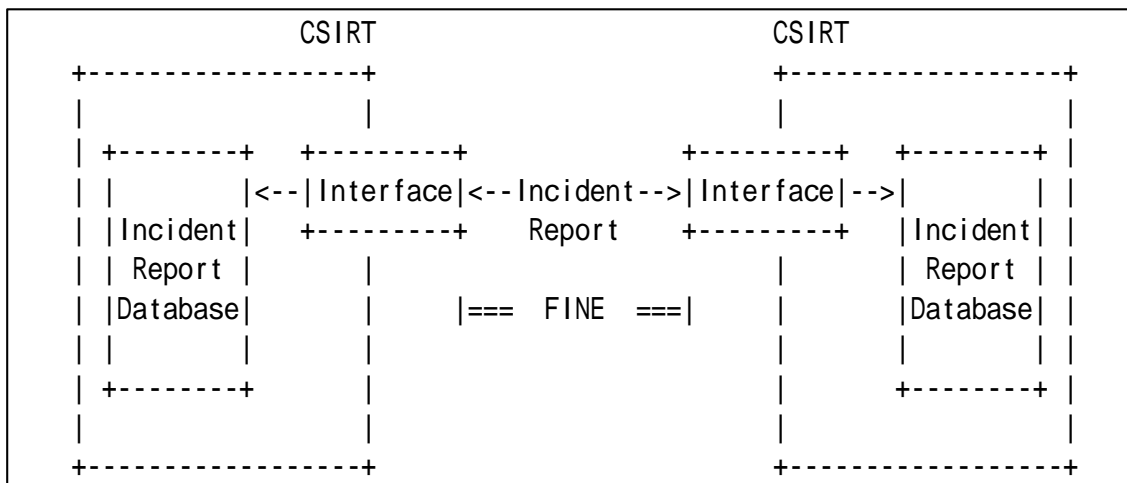


図 1 IODEF メッセージの概要

本実績は、IETF での議論にフィードバックするとともに、二つのシステムの基盤となっている。また、インシデントの届出フォームなどにも活用することができ、本開発で簡単な届出フォームも試作した（図 2）。

The screenshot shows a 'Manual Authoring' application window with the following fields and values:

- IncidentID:** Incident001
- Issuer:** IncidentIssuer
- Description:** IncidentDescription
- Observation point:** EventData-Description
- Contact:**
  - contactrole:** tech
  - contacttype:** organization
  - Name:** Tomohiro Tandai
  - Email:** tandai@cysols.com
  - Phone:** 022-000-0000
- Time:**
  - ReportTime:** 2005/09/27 19:03:40
  - StartTime:** 2005/09/27 19:03:00
  - EndTime:** 2005/09/27 19:03:00
  - DetectTime:** 2005/09/27 19:03:00
- Assessment:**
  - Impact:**
    - severity:** medium
    - completion:** succeeded
    - impacttype:** dos
  - MonetaryImpact:**
    - severity:** medium
    - currency:** mcurrency
    - value:** mvalue

Buttons: Publish, Send

図 2 IODEF-API を活用したインシデント届出アプリケーション

本アプリケーションでは、エンドユーザからの一般的な届出を IODEF 標準に準拠した形で出力、送信することが可能であり、届出およびその処理プロセスの自動化に大きく貢献することが期待できる。

結果として、大規模なインシデント情報を早期に知ることが可能となり、早期の警戒、対応を実現できる。

### 1.5.2. 広域不正アクセス追跡システム

送信元が詐称された不正アクセスの出所を特定するために、様々な技術が提案されており、そのうちのいくつかは実用的なレベルに達している。しかし全 Internet 規模で追跡を実行するためには、相互に運用できる標準化された技術が鍵となる。

本開発では、追跡システムの相互運用を目指して IETF で議論されている IODEF を拡張した IODEF-RID<sup>[14]</sup>を活用して、複数の独立した追跡システムを相互運用することを実現した。

本システムを基に標準化を推進することで、真の意味での広域追跡の第一歩とすることができる。

### 1.5.3. 広域インシデント分析・警戒システム

Internet で日々発生する不正アクセスは、DoS や Worm を初めとして多様化、広域化し、かつ非常に早く広まる傾向が強まっている。

一方で、企業や個人のセキュリティ管理者は、自サイトに訪れる様々なアクセスが妥当なものなのかどうかの判断をする必要があるが、Internet トラフィックは、多くの不正アクセスで汚染されており、それらの妥当性の評価は非常に困難である。

本分析システムは、インシデント情報を広域で共有するために議論されている標準化されたフォーマット IODEF で記述し、自動的に収集するとともに、その動向を分析するシステムである。応用として、現在、広く試みられている広域観測網を連携させることが可能となり世界的な不正アクセスの動向を効率よく知ることができる。それらを広く共有することで、個々のサイト管理者がそれを参照して、判断の指標とすることも可能となる。

図 3 に、開発した広域インシデント分析システムの運用例を示す。様々な観測点で観測された情報は、標準化されたフォーマット (IODEF) で記述され転送される。本アプリケーションは収集された多地点の情報を統合することにより、ネットワーク全体で、広く観測されるインシデント (広域インシデント) を抽出することができる。

また、分析された結果を新たなインシデント情報として IODEF フォーマットで「Publish」することも可能であり、エンドユーザに分析された情報を提供することができる。

DB Manager					
Search Condition					
Period		Observation Point	Incident Type		
from :	2005/06/01 18:53:18	Select point	Select type		
to :	2005/09/27 13:15:36	ALL	ALL		
					Search    Display All
Detected Time	Reported Time	Incident Type	Source Address	Incident Name	Observation Point
2005/06/01 19:37:18...	2005/09/27 13:15:36...	Alert	60.191.2.211	MS-SQL Worm propa...	csrit.cysols.com-20
2005/06/14 18:47:03...	2005/09/27 13:15:36...	Alert	202.101.42.176	MS-SQL Worm propa...	csrit.cysols.com-20
2005/06/01 18:53:18...	2005/09/27 13:15:36...	Alert	217.205.64.130	MS-SQL Worm propa...	csrit.cysols.com-20
2005/06/03 15:11:32...	2005/09/27 13:15:36...	Alert	222.179.216.66	MS-SQL Worm propa...	csrit.cysols.com-20
2005/06/09 03:01:44...	2005/09/27 13:15:36...	Alert	61.153.0.102	MS-SQL Worm propa...	csrit.cysols.com-20
2005/06/13 16:30:29...	2005/09/27 13:15:36...	Alert	222.136.87.240	ICMP PING NMAP	csrit.cysols.com-20
2005/06/22 00:41:50...	2005/09/27 13:15:36...	Alert	83.237.115.24	MS-SQL Worm propa...	csrit.cysols.com-20
2005/06/21 02:08:14...	2005/09/27 13:15:36...	Alert	222.174.115.18	MS-SQL Worm propa...	csrit.cysols.com-20
2005/06/11 12:36:07...	2005/09/27 13:15:36...	Alert	203.121.68.9	MS-SQL Worm propa...	csrit.cysols.com-20
2005/06/13 14:25:39...	2005/09/27 13:15:36...	Alert	222.178.152.96	MS-SQL Worm propa...	csrit.cysols.com-20
2005/06/19 00:52:51...	2005/09/27 13:15:36...	Alert	221.236.9.54	MS-SQL Worm propa...	csrit.cysols.com-20
2005/06/01 21:47:24...	2005/09/27 13:15:36...	Alert	220.176.14.200	MS-SQL Worm propa...	csrit.cysols.com-20
2005/06/07 08:01:31...	2005/09/27 13:15:36...	Alert	202.99.177.209	MS-SQL Worm propa...	csrit.cysols.com-20
2005/06/05 19:58:05...	2005/09/27 13:15:36...	Alert	202.100.140.8	MS-SQL Worm propa...	csrit.cysols.com-20
2005/06/07 13:36:09...	2005/09/27 13:15:36...	Alert	221.236.9.54	MS-SQL Worm propa...	csrit.cysols.com-20

図 3 広域インシデント分析

#### 1.5.4. 広域インシデント情報の可視化

図 4 に本システムで実現した可視化例を示す。本開発ではインターネット規模の広域に影響を及ぼすインシデントを対象としている。本可視化システムでは、インシデントの発生地点をネットワーク地図上に示すことで、その広がり、影響範囲、拡散傾向を分析することができる。

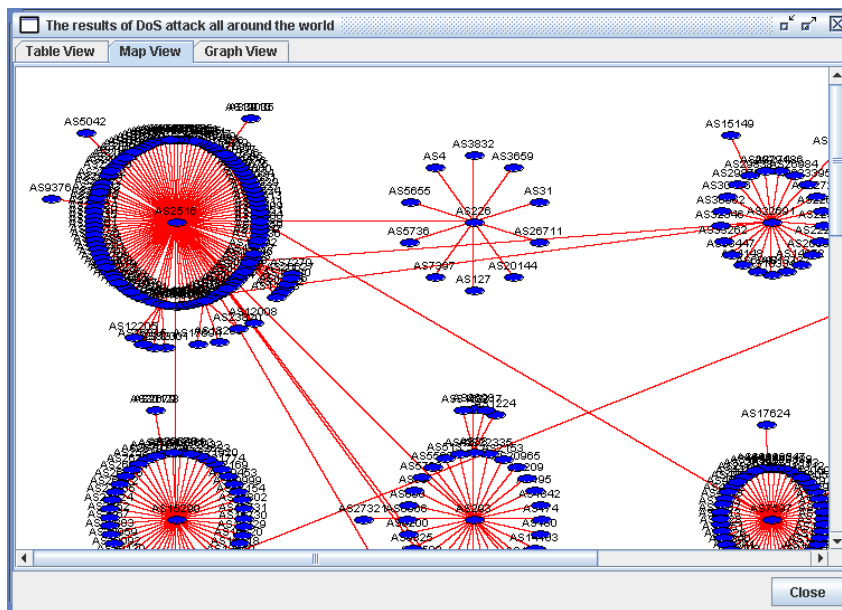


図 4 広域シンシデントの地図による可視化

#### 1.6. まとめ

本開発によって、IODEF 標準を活用するための基盤技術を確立することができた。また、具体的な応用例となるアプリケーションを開発し、その有用性を示すことができた。

今後は、本標準に基づく情報収集を推進するとともに、本技術および、分析結果のエンドユーザによる活用の可能性を検討していくことで、インターネット全体の安全と安心に寄与することが期待される。

## 2. 基本定義

本システムでインシデントを構成する各要素を以下のように定義する。

### 2.1. イベント

イベントはセンサで観測される基本情報である。本システムでは以下の 2 種類のイベントを定義する。本システムでは、ネットワークトラフィックを観測するシステムをセンサとして定義する。

1. Packet
2. Alert

すべてのイベントは、以下の情報をその属性として保持する。

- Source address
- Time stamp
- Type of event
- Event name

### 2.2. インシデント

インシデントは、複数のイベントで構成され、各観測点で生成される。インシデント生成時には必ず観測点に関する情報を付加するものとする。本システムでは、基本的に複数のイベントを一組にした集約された情報をインシデントとして定義する。

インシデントは以下の情報をその属性として保持する。

- Observation point
- Source address
- Incident name
- Type of incident
- Records

### 2.3. 広域インシデント DB

各観測点で観測され、インシデントとして集約されたイベントは、IODEF メッセージとして XML フォーマットで記述され、転送される。広域インシデント DB は、様々な観測点から転送されたインシデントを統合して保存するデータベースである。

#### 2.4. 広域インシデント

広域インシデントは、広域インシデント DB に集められたインシデントを分析し、複数の観測点にわたって観測されているインシデントである。

### 3. 全体システム構成

本開発で、開発する二つのシステムの全体構成を示す。

#### 3.1. 広域インシデント分析・警戒システム

図 5 に広域インシデント分析・警戒システムの概要を示す。本システムは、センサ、およびマネージャの二つのサブシステムからなり、センサ上で IODEF authoring AP、マネージャ上で IODEF DB manager AP および Analyzer AP が動作する。Analyzer AP によって広域インシデントの分析および警戒のための可視化を実行する。

センサからマネージャに、IODEF メッセージによって記述されたインシデント情報が転送され、マネージャ側に配備される広域インシデント DB に保存される。SNORT からのアラートは SNMP による SNORT アラート (sidaMIB) に対応した DB、sidaDB を経由する。本 DB への格納は Alert Receiver によって行われ、SNMP trap/inform にて通知されるアラートを DB へ格納する。

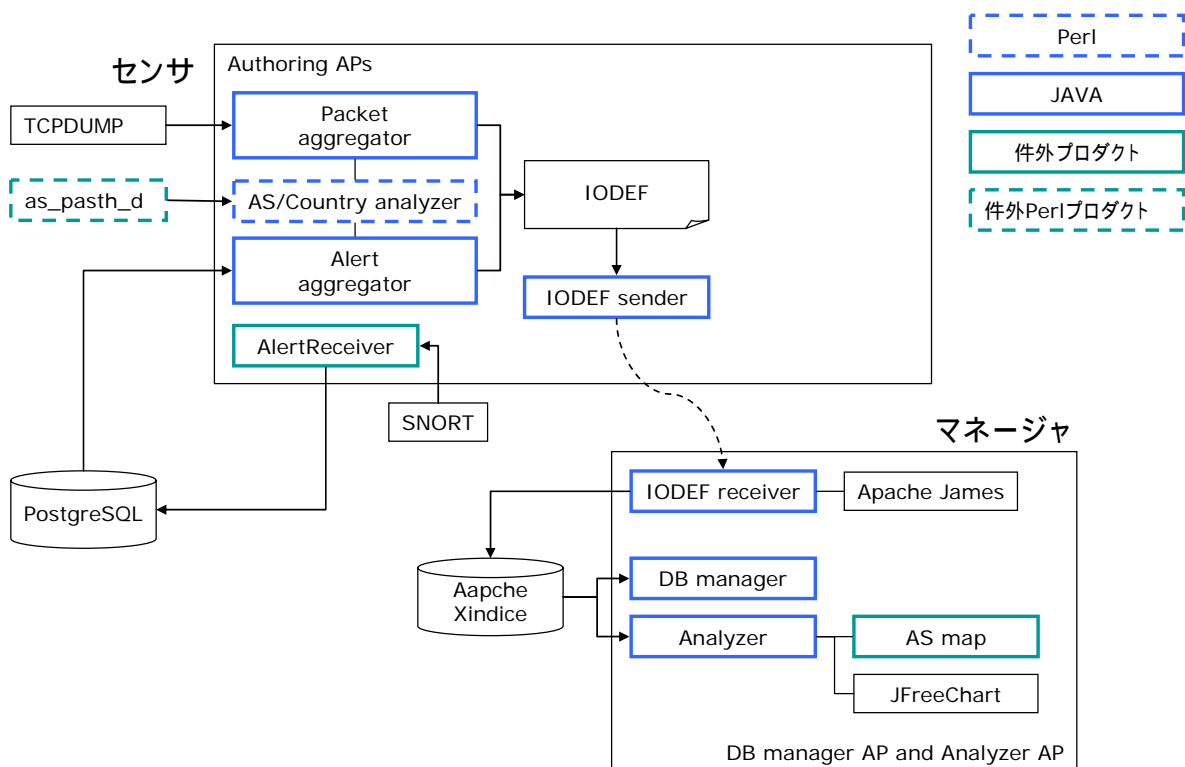


図 5 広域インシデント分析・警戒システムの概要

図 6 に上記概要の実装システム構成を示す。

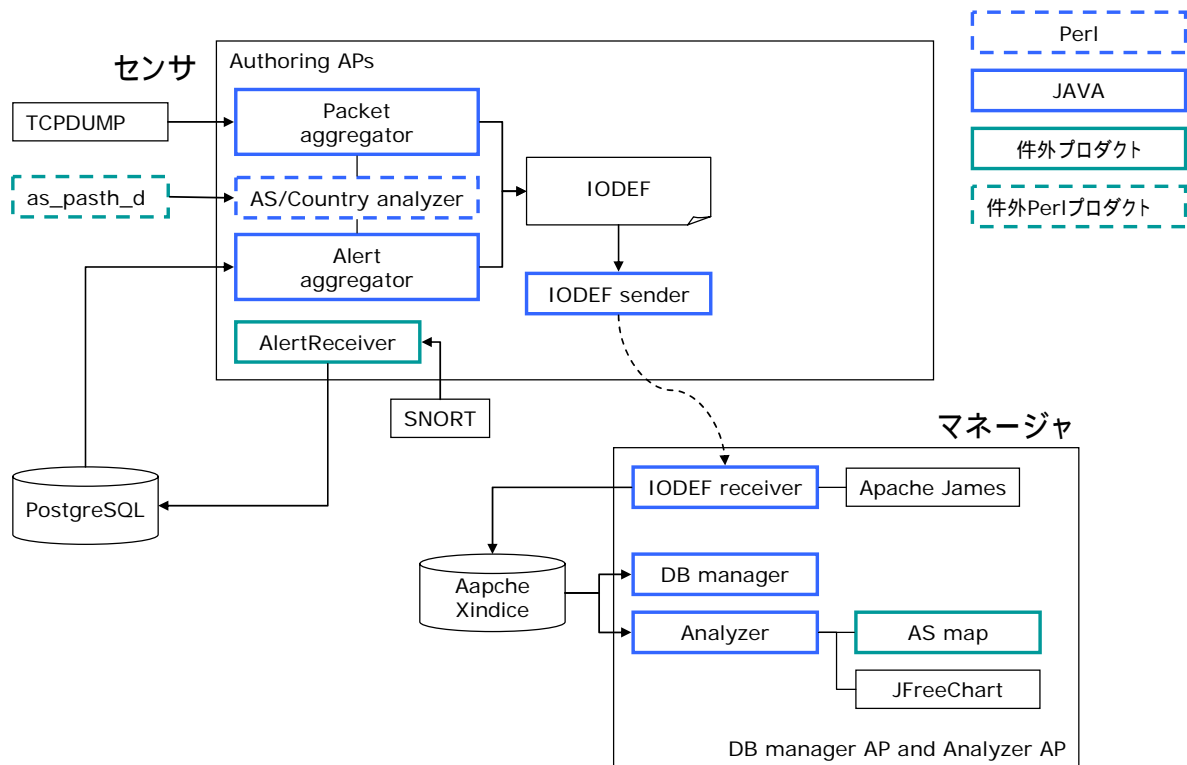


図 6 広域インシデント分析・警戒システムの構成

### 3.2. 広域不正アクセス追跡システム

図 7 に広域不正アクセス追跡システムの概要を示す。本システムは、センサ、およびマネージャの二つのサブシステムからなり、センサ上でローカル追跡システム（本システムでは PacketChaser）と RID 通信機能を備える SNMP-IODEF gateway AP、マネージャ上で同じく RID 通信機能を備える Wide area tracker が動作する。

Wide area tracker から SNMP-IODEF gateway AP に、IODEF メッセージによって記述されたインシデント情報に RID で記述された Query を SOAP によって送信し、センサ側ではローカルな追跡を実施、結果を RID で記述し、SOAP で返信する。

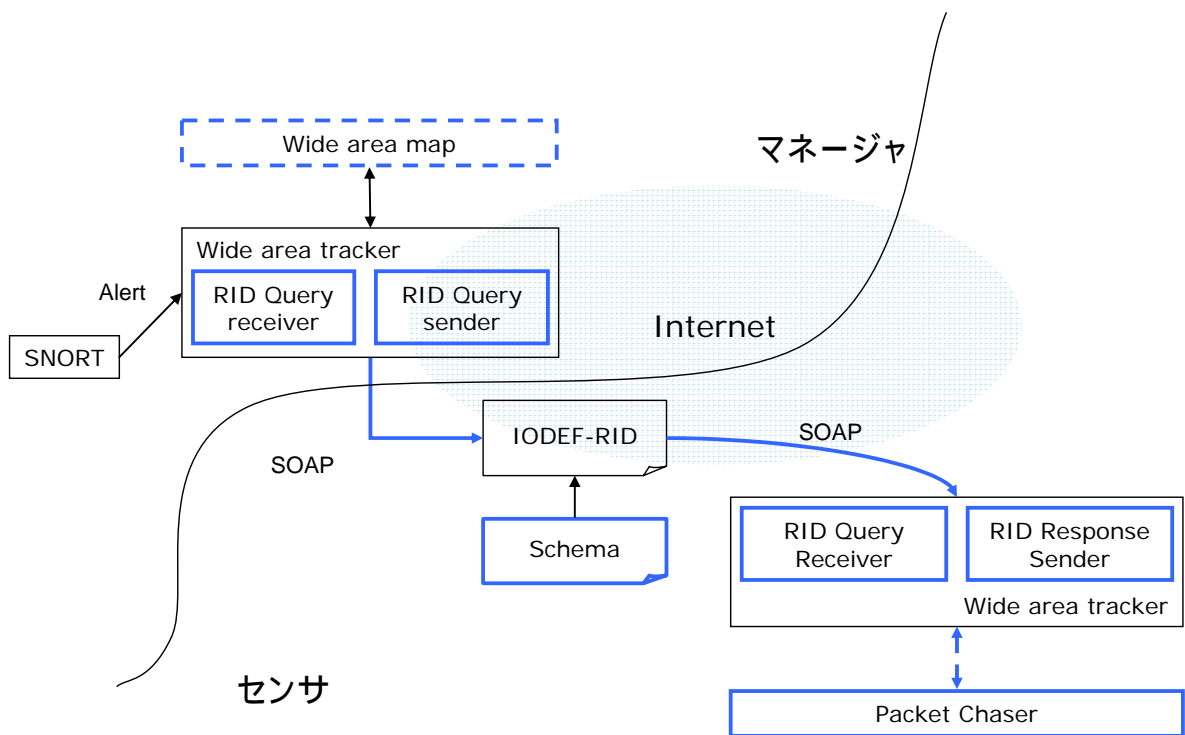


図 7 広域不正アクセス追跡システムの概要

図 8 に上記概要の実装システム構成を示す。図中の青の実線枠は JAVA によるプログラム、同じく青の点線は Perl によるプログラム、緑は件外プロダクトを示す。

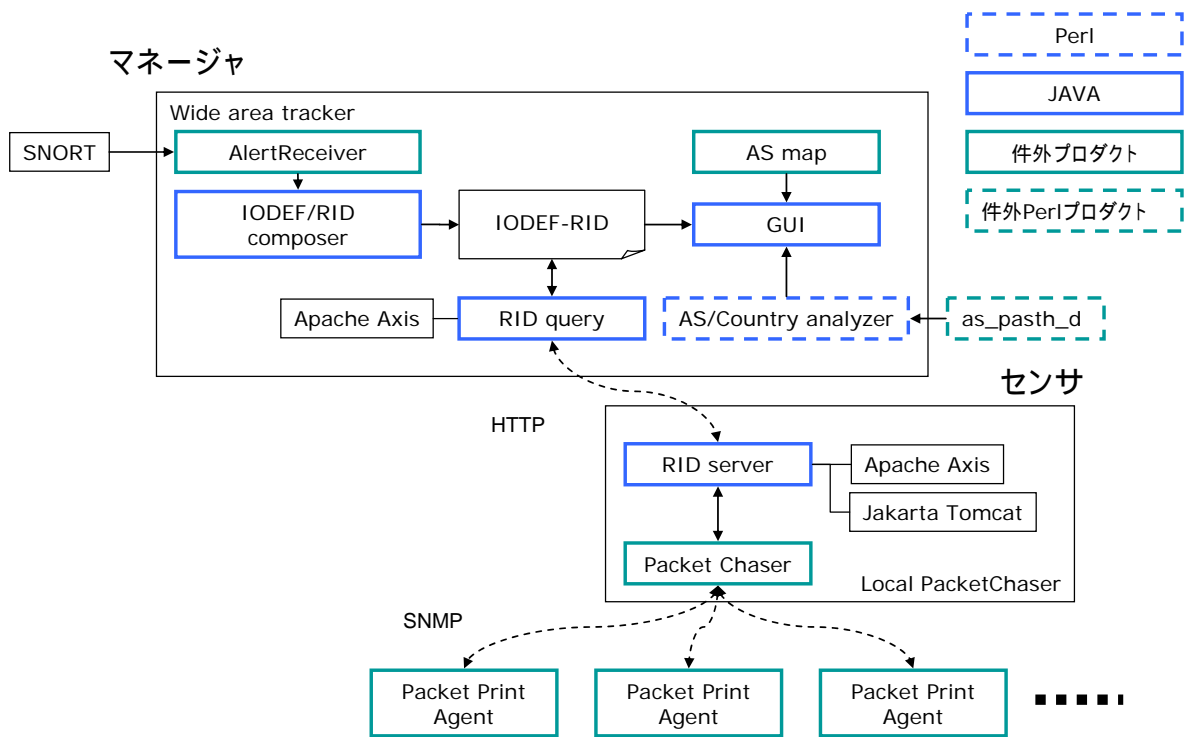


図 8 広域不正アクセス追跡システムの構成

#### 4. IODEF authoring AP

IODEF authoring AP は観測されたイベント情報からインシデント情報を生成し、IODEF メッセージとして XML 文書を生成する。

IODEF メッセージの生成の基本フローを図 9 に示す。

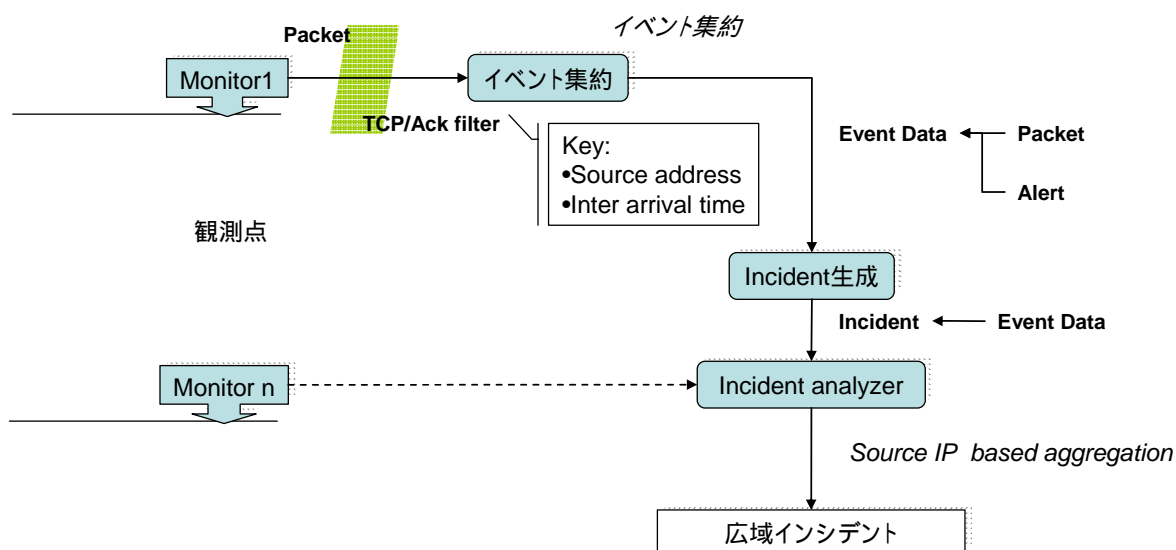


図 9 イベント集約およびインシデント生成の基本フロー

##### 4.1. イベント情報の抽出

本システムは、

A. Snort および SNMP アウトプットプラグインによって生成、通知される Snort アラート (略称: sida) を

1. 受信し、DB に保存、
2. DB から sida レコードを読み出し IODEF XML ファイルを作成、
3. 作成された IODEF XML ファイルを E メールにてマネージャに送信、

または

B. tcpdump などを使って収集したパケットダンプデータを元に、

1. データを読み出し IODEF XML ファイルを作成、

2．作成された IODEF XML ファイルを E メールにてマネージャに送信，  
を実施する 2 つのサブシステムで構成されるものである．その概要を図 10 に示す．

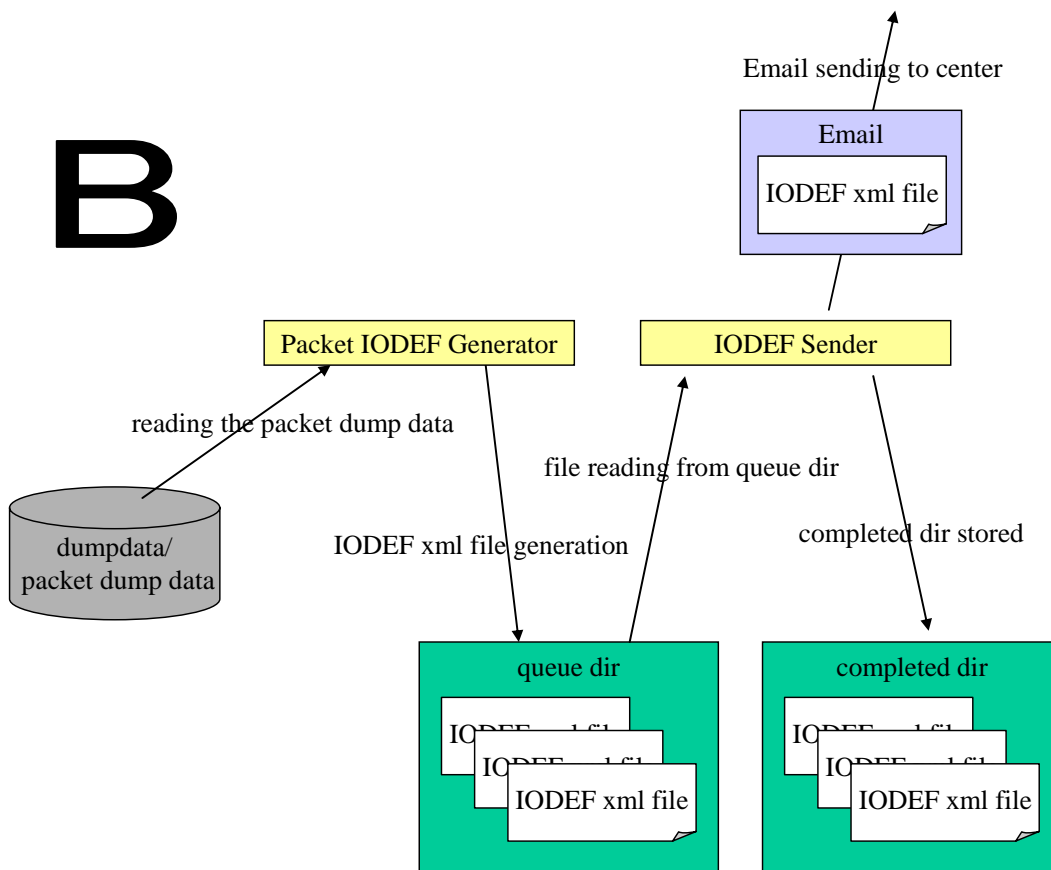
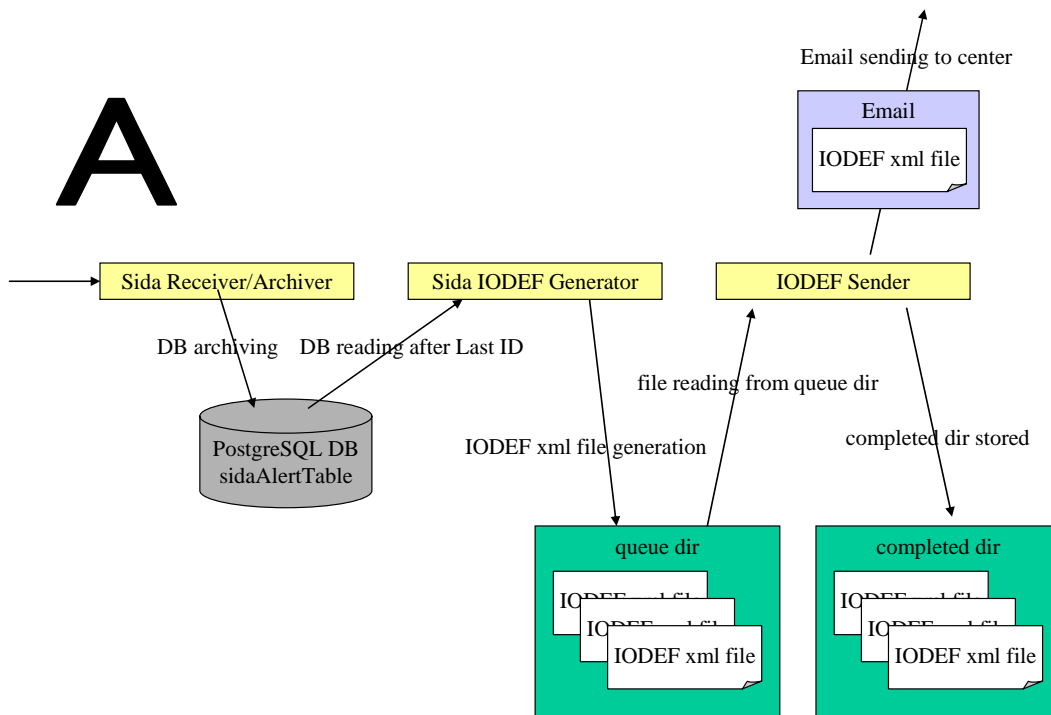


図 10 IODEF メッセージ生成の構成要素

これらは以下のコンポーネントより実行される。

1. Sida Receiver/Archiver  
弊社既存パッケージによって提供される Snort アラートの受信および DB 保存を実行するコンポーネント。
2. A . Sida IODEF Generator  
DB に保存された sida レコードを読み出しイベントを集約して IODEF XML ファイルを作成し保存するコンポーネント。  
B. . Packet IODEF Generato  
予め収集されたパケットダンプデータを読み出しイベントを集約して IODEF XML ファイルを作成し保存するコンポーネント。
3. IODEF Sender  
保存されている IODEF XML ファイルを読み込み E メールでセンターに送信するコンポーネント。

#### 4.2. Sida Receiver/Archiver

弊社既存パッケージによって提供される Snort アラートの受信および DB 保存を実行するコンポーネントであり、Snort アラート受信設定、および DB 設定の 2 つの設定ファイルにより動作する。概要を以下の図 11 に示す。

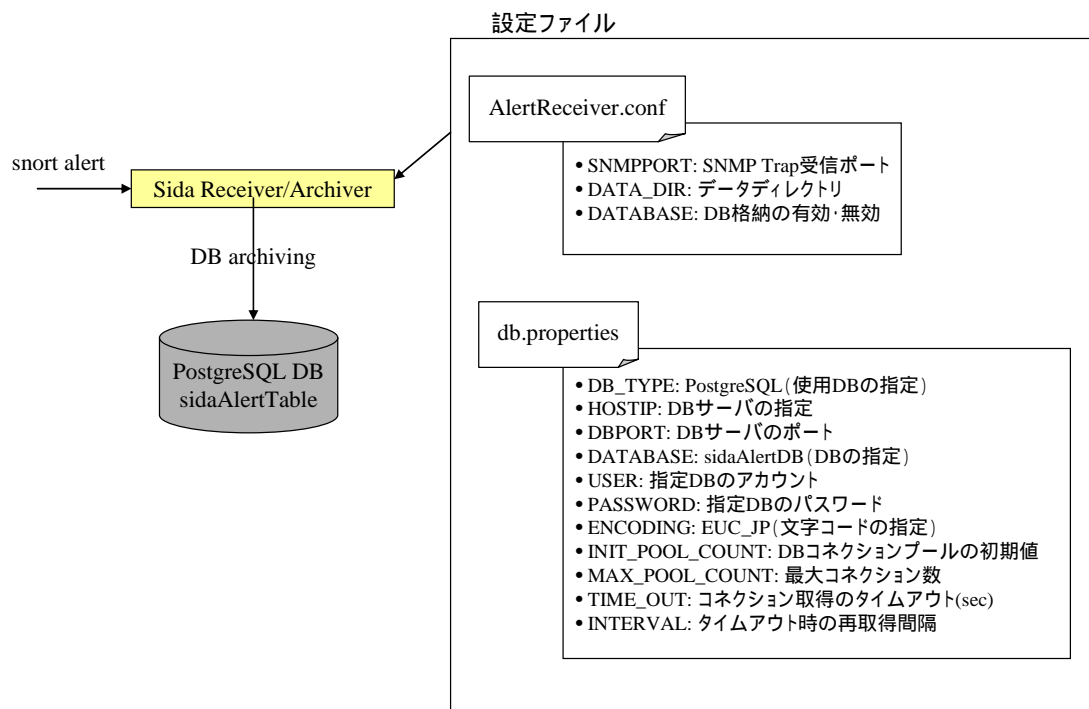


図 11 アラート情報の抽出

- Snort アラート受信設定 ( config/AlertReceiver.conf )
  - ✧ SNMPPORT : 162 - SNMP Trap/Notification のデフォルトポート , Snort アウトプットプラグインの設定に合わせて受信ポートを設定する .
  - ✧ DATA\_DIR : data/を指定 . DATABASE が無効の場合 , このディレクトリに受信した Snort アラートの情報がログされる .
  - ✧ DATABASE : true を指定 . これにより DB 保存が有効となる .
- DB 設定
 

DB サーバの設定に合わせて以下の DB 接続のパラメータを設定する .

  - ✧ HOSTIP
  - ✧ DBPORT
  - ✧ DATABASE
  - ✧ USER
  - ✧ PASSWORD

以下に Snort アラートが保存される PostgreSQL の sidaAlertTable テーブル定義を示す . 本定義の詳細は、SNORT の拡張として広く配布されている SNMP output plugin に付属の MIB 定義を参照のこと .

カラム名	データ型	制限
ID	SERIAL8	NOT NULL PRIMARY KEY
TrapID	INT	NOT NULL default 0
sidaSensorID	INT	NOT NULL default 0
sidaAlertSensorType	INT	NOT NULL default 1
sidaSensorAddress	VARCHAR(39)	NOT NULL
sidaAlertID	INT	default NULL
sidaAlertTimeStamp	TIMESTAMP	NOT NULL
sidaAlertMsg	VARCHAR(255)	default NULL
sidaAlertMoreInfo	VARCHAR(255)	default NULL
sidaAlertSrcAddressType	INT	NOT NULL default 1
sidaAlertSrcAddress	VARCHAR(39)	default NULL
sidaAlertSrcPort	INT	NOT NULL default 0
sidaAlertSrcMacAddress	VARCHAR(20)	default NULL
sidaAlertDstAddressType	INT	NOT NULL default 0
sidaAlertDstAddress	VARCHAR(39)	default NULL
sidaAlertDstPort	INT	NOT NULL default 0
sidaAlertDstMacAddress	VARCHAR(20)	default NULL
sidaAlertImpact	INT	NOT NULL default 0
sidaAlertEventPriority	INT	NOT NULL default 0
sidaAlertProto	VARCHAR(64)	NOT NULL default 0
sidaAlertRuleID	INT	NOT NULL default 0
sidaAlertRuleRevision	INT	NOT NULL default 0
sidaAlertPacketPrint	VARCHAR(255)	default NULL

また，上記テーブルを作成する SQL CREATE 文を以下に示す．

```
CREATE TABLE sidaAlertTable (
  ID SERIAL8 NOT NULL PRIMARY KEY,
  TrapID INT NOT NULL default 0,
  sidaSensorID INT NOT NULL default 0,
  sidaAlertSensorType INT NOT NULL default 1,
  sidaSensorAddress VARCHAR(39) NOT NULL,
  sidaSensorInterfaceIndex INT default NULL,
  sidaAlertID INT NOT NULL default 0,
```

sidaAlertTimeStamp	TIMESTAMP	NOT NULL,
sidaAlertMsg	VARCHAR(255)	default NULL,
sidaAlertMoreInfo	VARCHAR(255)	default NULL,
sidaAlertSrcAddressType	INT	NOT NULL default 1,
sidaAlertSrcAddress	VARCHAR(39)	default NULL,
sidaAlertSrcPort	INT	NOT NULL default 0,
sidaAlertSrcMacAddress	VARCHAR(20)	default NULL,
sidaAlertDstAddressType	INT	NOT NULL default 1,
sidaAlertDstAddress	VARCHAR(39)	default NULL,
sidaAlertDstPort	INT	NOT NULL default 0,
sidaAlertDstMacAddress	VARCHAR(20)	default NULL,
sidaAlertImpact	INT	NOT NULL default 0,
sidaAlertEventPriority	INT	NOT NULL default 0,
sidaAlertProto	VARCHAR(64)	NOT NULL default 0,
sidaAlertRuleID	INT	NOT NULL default 0,
sidaAlertRuleRevision	INT	NOT NULL default 0,
sidaAlertPacketPrint	VARCHAR(255)	default NULL

);

#### 4.3. Sida IODEF Generator

DB に保存された sida レコードを読み出し IODEF XML ファイルを作成，保存するコンポーネントであり，DB 設定，および IODEF 作成設定の 2 つの設定ファイルとインシデントを作成するための 3 つの参照ファイルにより動作する．概要を以下の図 12 に示す．

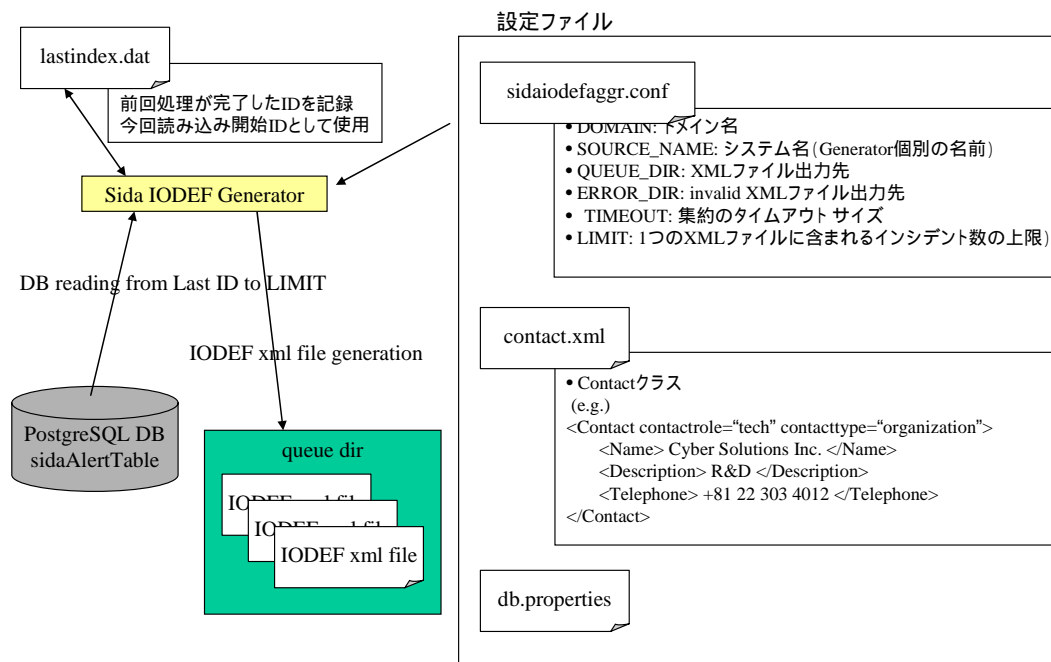


図 12 アラートからの IODEF メッセージ生成

入力：LastIndex，Snort アラートのレコード（DB から）

出力：IODEF XML ファイル（QUEUE\_DIR へ），LastIndex

- DB 設定（config/db.properties）  
Sida Receiver/Archiver の設定と同様 .保存した Snort アラートを DB から読み出す .
- IODEF 作成設定（config/sidaiodefaggr.conf）
  - ◇ DOMAIN：IODEF 作成元（組織など）のドメイン名
  - ◇ SOURCE\_NAME：監視場所などを基に IODEF 作成元名称（ユニークな名称で複数の IODEF Generator が存在する場合にそれらを識別する）
  - ◇ QUEUE\_DIR：作成した IODEF XML ファイルの保存先ディレクトリ
  - ◇ ERROR\_DIR：作成時に規約違反した IODEF XML ファイルの保存先ディレクトリ
  - ◇ TIMEOUT: 集約のタイムアウト
  - ◇ LIMIT：1つの IODEF XML ファイルに含まれるインシデント数の上限

IODEF メッセージのインシデント ID は上記設定情報を元に作成される .

name 属性：ドメイン名

インシデント ID：ドメイン名#システム名 + Snort アラートのセンサ ID +

## DB の ID

参照ファイルとして以下の情報を用いて IODEF XML ファイルは作成される。

- config/contact.xml  
インシデントに含まれる Contact クラスを定義する。<contact>タグおよびその子要素を予め指定しておくことで、IODEF XML ファイル作成時に指定された Contact クラスをインシデントに含める。
- sid-msg.map , reference.config  
Snort アラートのルール ID ( sidaAlertRuleID ) よりそのルールに関連するリファレンスを取得して、インシデント内の Assessment-Classification クラスとして含める。

IODEF XML ファイル作成のフローチャートを以下の図 13 に示す。

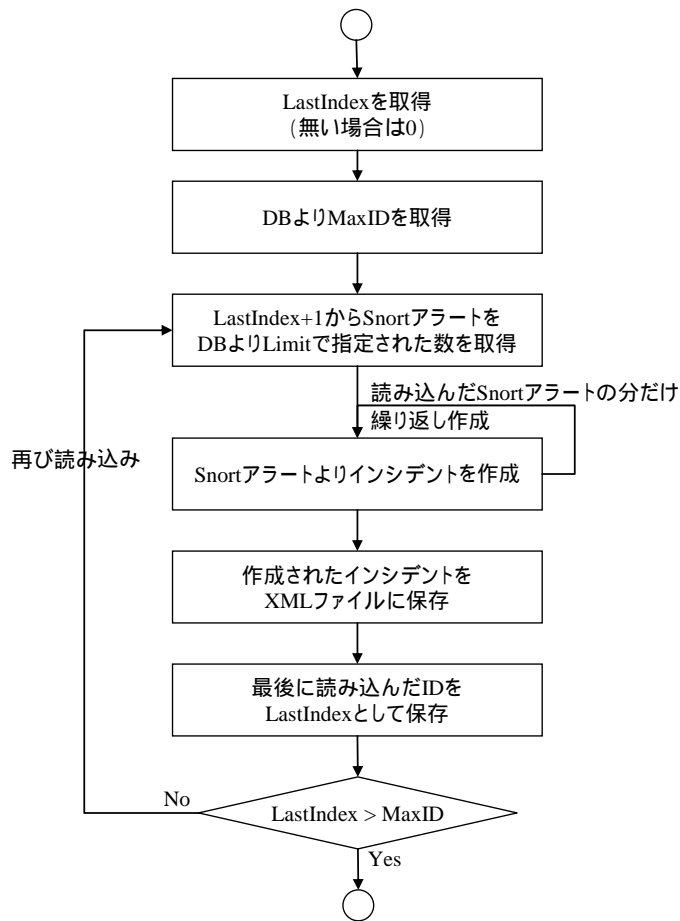


図 13 IODEF XML 生成フロー

IODEF XML ファイルは QUEUE\_DIR で指定されたディレクトリに保存される。

ファイル名は

incident-ドメイン名-システム名-時刻.xml

となる。

#### 4.4. Packet IODEF Generator

予め収集されたパケットダンプデータを読み出しイベントを集約して IODEF XML ファイルを作成し保存するコンポーネントであり、IODEF 作成設定ファイルより動作する。概要を以下の図 14 パケットからの IODEF メッセージ生成に示す。

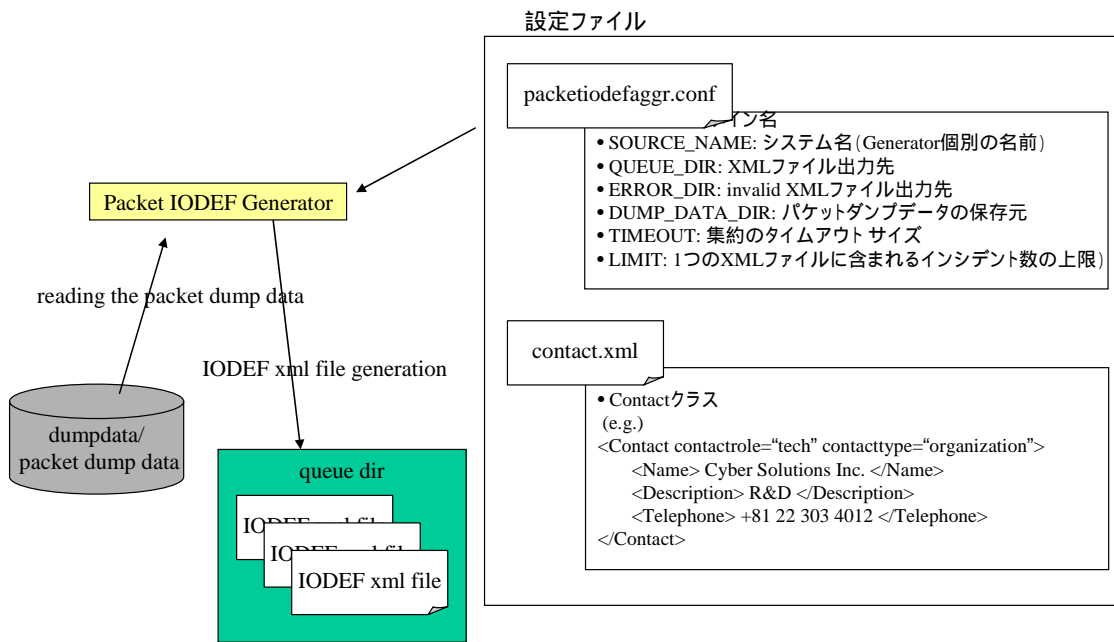


図 14 パケットからの IODEF メッセージ生成

#### 4.5. IODEF Sender

保存されている IODEF XML ファイルを読み込み E メールでセンターに送信するコンポーネントであり，XML 送信設定ファイルにより動作する．概要を以下の

図 15 に示す .

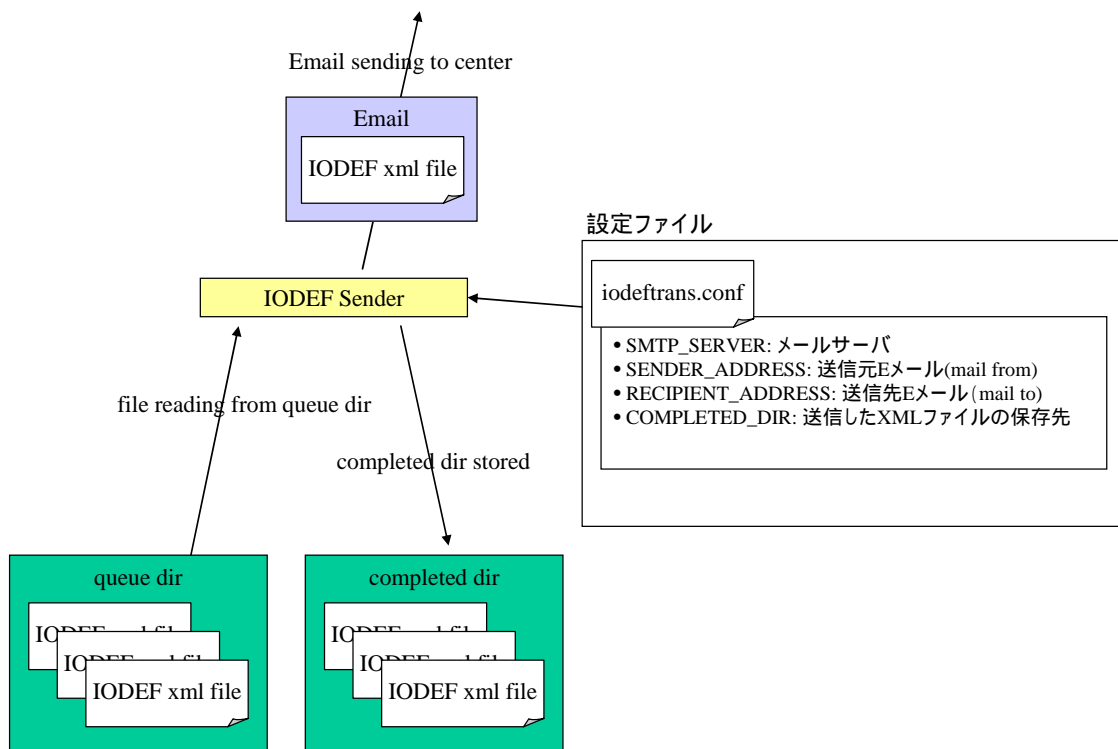


図 15 IODEF Sender の構成

入力：送信する XML ファイル

出力：E メール (XML ファイル添付), 送信した XML ファイル

- IODEF 送信設定 ( config/iodeftrans.conf )
  - ◇ SMTP\_SERVER：メール送信に使用するメールサーバ
  - ◇ SENDER\_ADDERSS：送信元 E メールアドレス
  - ◇ RECIPIENT\_ADDRESS：送信先 E メールアドレス，カンマ区切りで複数の送信先を指定可能
  - ◇ COMPLETED\_DIR：送信した IODEF XML ファイルを保存するディレクトリ

IODEF Sender は IODEF Generator によって作成された IODEF XML ファイルを QUEUE\_DIR より取得して，1つのファイルを1つのメールに添付して指定した送信先に E メールにより送付する．送信した IODEF XML ファイルは指定の COMPLETED\_DIR に移動される．

#### 4.6. IODEF メッセージ生成

以下に IODEF メッセージの各項目の生成仕様を示す。

##### 4.6.1. IncidentID

###### **Name attribute**

ドメイン名を利用する

###### **Value**

Name attribute + システムで一意的な文字列 + sensor ID + alert ID

###### **Example**

```
<IncidentID name="csirt.cysols.com">csirt.cysols.com#1-10</IncidentID>
```

##### 4.6.2. Contact

以下の3項目の要素を含むクラスを生成する。

- name
- Description

- Telephone

### Example

```
<Contact role="tech" type="organization">  
<name> Cyber Solutions Inc. </name>  
<Description> R&D </Description>  
<Telephone> +81 22 303 4012 </Telephone>  
</Contact>
```

#### 4.6.3. Description

本要素は次のような固定値とする 例：“Wide area observation message”

#### 4.6.4. Assessment

本項目はデフォルト値として、次の値をとるものとする。

Assessment -> Impact is static value “unkown”

#### 4.6.5. DetectTime

<DetectTime> class の値は集約されたイベント中の最も早い時刻とする。

#### 4.6.6. StartTime

<StartTime> class の値は<DetectTime.>と同じとする。

#### 4.6.7. EndTime

<EndTime> class の値は集約されたイベント中の最も遅い時刻とする。

#### 4.6.8. ReportTime

<ReportTime> class の値はインシデントメッセージが生成された時刻とする。

#### 4.6.9. Incident specific classes

インシデント固有の属性は、以下に示す IODEF 文書の要素を利用して記述する。

- Observation point
- Source address
- Incident name
- Type of incident
- Records

### Observation point

Sensor ID の値を利用する。

EventData -> Description
--------------------------

### Source address

Source address は集約されたイベントに共通するアドレスを利用する。

Incident -> EventData -> Flow -> System -> Node -> Address
--

Address – addrcat => “iv4-addr”

### Incident name

Incident name は type of event 毎に異なる値となる。 .

Incident -> EventData -> Method -> Description
--

### Type of incident

Type of incident は type of event 毎に異なる値となる。

Incident -> EventData -> Method -> Classification->name
---

Classification – origin => “local”

### Records

Records はイベントの元情報を格納する。

Incident -> EventData -> Record -> RecordData -> RecordItem
---

RecordItem - type => "string"

4.6.10. Values / attributes for each type of incident

### Packet Incident

Incident name は"TCP ack"とする。

Type of incident は"Packet"とする。

属性は以下のように上書きする。

Incident -> EventData -> Flow -> System

System - category => "target"

System- spoofed => "yes"

Records は以下のような文字列型の生情報とする。

```
1117552418.548500  PPPoE      [ses  0x4b65]  IP  219.238.237.12.8600  >
61.211.33.142.43289: R 0:0(0) ack 1075184465 win 0
1117552424.289241  PPPoE      [ses  0x4b65]  IP  219.238.237.12.8600  >
61.211.33.142.43289: R 0:0(0) ack 1 win 0
```

### When type of record is Alert

Incident name は、インシデントを構成するアラートイベントの一意的アラート名を結合したものとする。

Type of incident は"Alert"とする。

属性は以下のように上書きする。

Incident -> EventData -> Flow -> System

System- category => "source"

Records は以下のような文字列型の生情報とする。

[\*\*] [1:2004:7] MS-SQL Worm propagation attempt OUTBOUND [\*\*]

#### 4.7. Manual Authoring

本ツールは、管理者によって、任意にインシデント報告を作成することを支援するためのツールである。センサ側の AP としての位置付けとなり、本ツールで出力される IODEF メッセージはセンサからのものと同様に、マネージャ側の広域シンシデント DB に送信、格納することができる。

##### 4.7.1. 手動 IODEF メッセージ作成ツール

自動でイベントを抽出、処理を実行して IODEF メッセージを送信する既出のもの以外に、ユーザによって手動で IODEF メッセージを作成するツールが提供される。

この GUI ツールは、フィールドに入力された値を元に IODEF メッセージを生成し、妥当性を検証後、ファイル保存及び、メールでの送信機能提供する。図 16 GUI イメージを以下に示す。

IncidentID	ID	Issuer	
Description			
Observation point			
Contact	contactrole ▾	contacttype ▾	
Name			
Email			
Phone			
Time			
ReportTime	<i>auto fill</i>		
StartTime	select with calendar	▾	
EndTime	select with calendar	▾	
DetectTime	select with calendar	▾	
Assessment			
Impact	severity ▾	completion ▾	impacttype ▾
Monetary	severity ▾	currency	value

図 16 Manual Authoring AP の GUI イメージ図

上記の各項目名は IODEF メッセージで定義されている項目であり、逆 で表されているマークは、同じく同 IODEF メッセージ定義中で、選択する項目として定義されている情報項目であり、押下することで、選択肢を表示するものである。

#### 4.7.2. IODEF メッセージ作成

以下に入力必須項目と IODEF メッセージとの対応を示す。下記項目以外は 4.6 節 IODEF メッセージ生成に準じる。

## Type of Incident

“ Report ” 値を利用する

```
Incident -> EventData -> Method -> Classification->name  
  
Classification  origin => “ local ”
```

## Source Address

自ホストのアドレスを利用する .

```
Incident -> EventData -> Flow -> System -> Node -> Address  
  
Address - category => “ipv4-addr”
```

## Incident name

“ Reported by administrator ” 値を利用する

```
Incident -> EventData -> Method -> Description
```

## Observation point

```
EventData -> Description
```

## Purpose of Incident

“ reporting ” 値を利用する .

```
Incident - purpose => “reporting”
```

## 5. IODEF DB manager AP

IODEF DB manager AP はセンサから送られる IODEF メッセージを受信し、広域インシデント DB に格納するとともに、格納されたインシデント情報を検索し、表示する。

AP の概要を図 17 に示す。

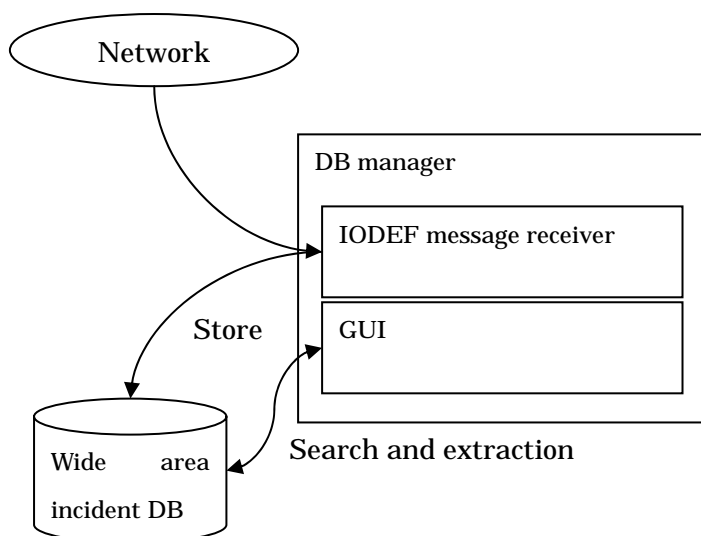


図 17 IODEF DB manager AP の概要

本 AP の目的は以下の 4 つとなる。

- IODEF メッセージの受信と広域インシデント DB への格納
- 格納されたインシデント情報の閲覧
- 格納されたインシデント情報の検索
- 格納されたインシデント情報の選択と、新たな IODEF メッセージの生成

### 5.1. IODEF メッセージの受信と広域インシデント DB への格納

本システムは各観測点にて生成された IODEF XML ファイルを収集し、XML DB<sup>iv</sup>に保存するマネージャ側のシステムである。

#### 5.1.1. IODEF メッセージの送受信

各観測点からは E メール添付で IODEF XML ファイルが送信され、マネージャ側でそのメールを受信、添付の XML ファイルを抽出してインシデントを DB に保存する。メール受信

のための SMTP サーバのプラットフォームとして James<sup>v</sup> ( Java Apache Mail Enterprise Server ) を利用し , その Mailet API を用いてメール受信後の DB 格納を実現する .

図 18 にその概要図を示す .

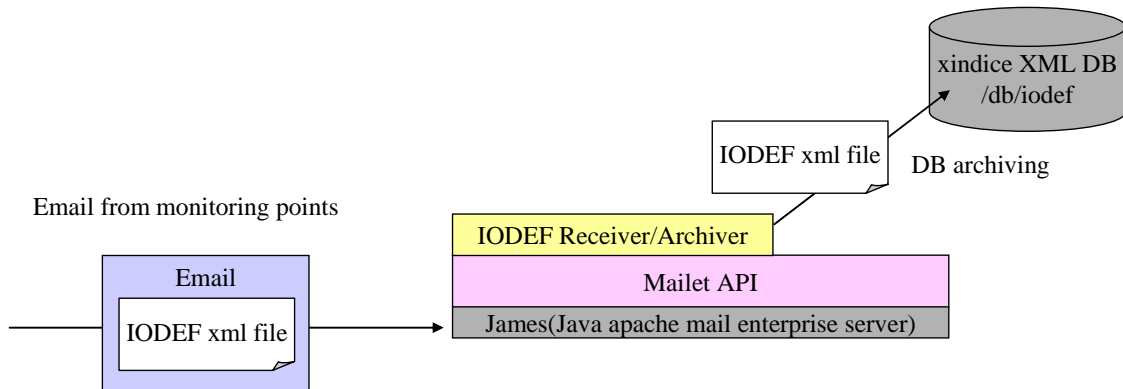


図 18 IODEF メッセージの受信の概要

#### 5.1.2. IODEF メッセージの DB 格納

Mailet API を用いて実装されたメール処理ロジックの実装であり , 受信した E メールから IODEF XML ファイルを抽出し , 含まれるインシデントを XML DB に格納する . 概要を図 19 に示す .

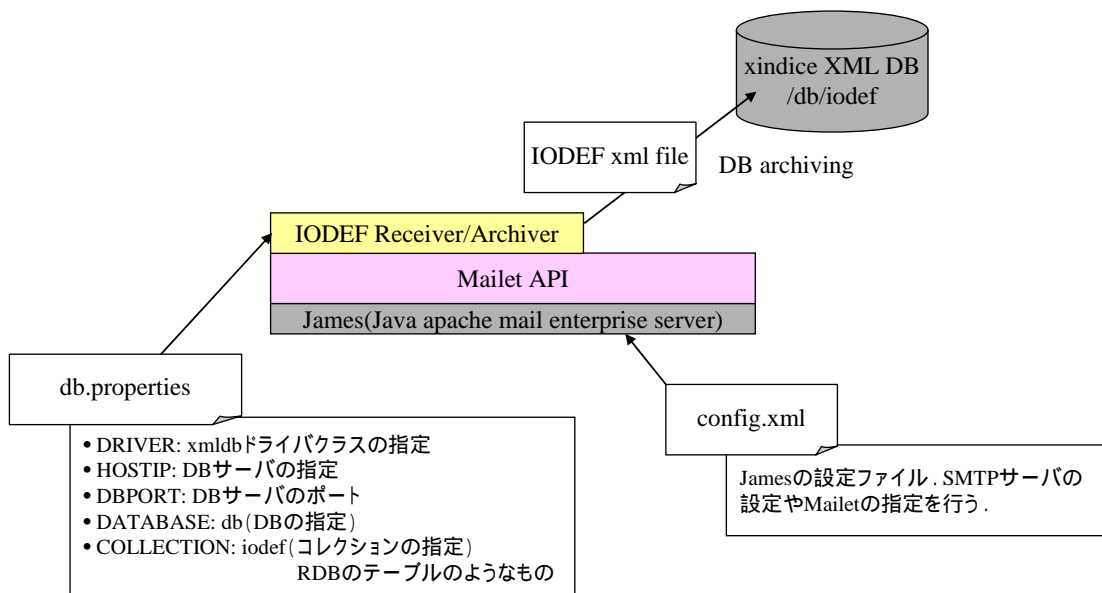


図 19 IODEF メッセージの DB 格納の概要

XML DB サーバとして xindice を利用する .

➤ DB 設定

DB サーバの設定に合わせて以下の DB 接続のパラメータを設定する .

- ◇ DRIVER
- ◇ HOSTIP
- ◇ DBPORT
- ◇ DATABASE

xindice では XML 文書を “ Document ” といい Document は ID がつけられて Collection の下に格納される . Collection は Collection の下に作成することが可能である . 本システムでは図 20 に示す構造を持つ XML データベースを使用する .

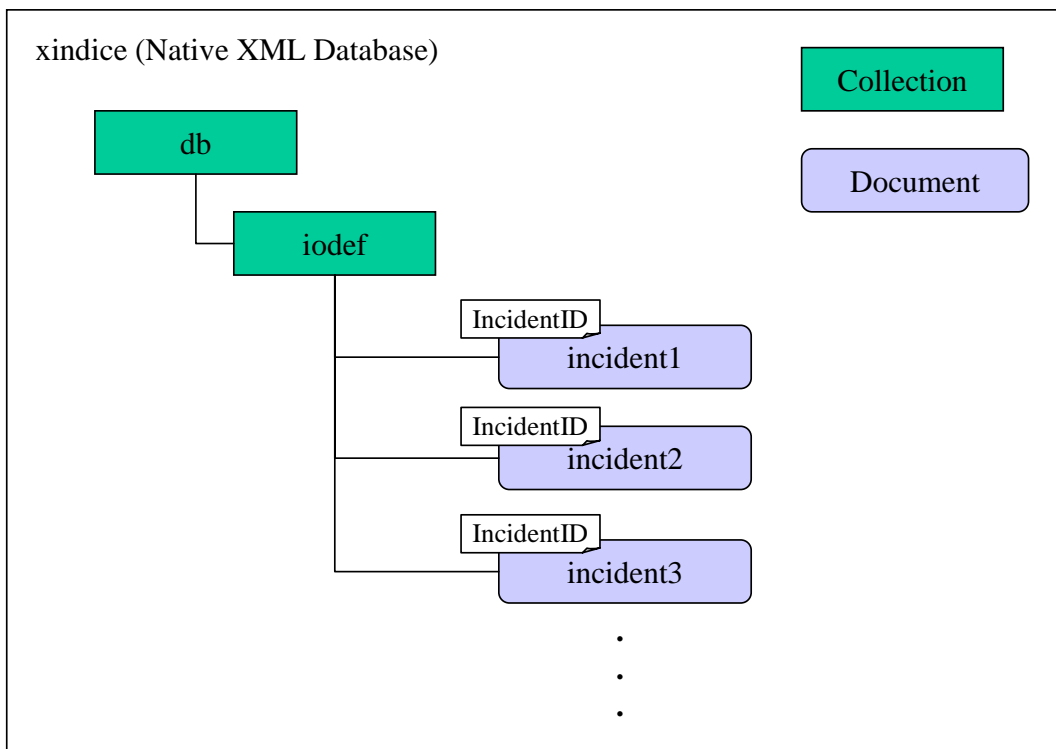


図 20 XML DB 構造

IODEF Receiver/Archiver Mailer は E メールに添付されている IODEF XML ファイルを読み込み , 定義されているインシデントをそれぞれ 1 つの Document として XML DB の iodef Collection 以下に保存する . その際に ID としてそれぞれのインシデントの IncidentID を用いる .

## 5.2. 格納されたインシデント情報の閲覧

基本的に、格納されたすべてのインシデント情報を図 21 のような GUI 上に表示する。

表示された各インシデント情報の全体を表示する機能を有する。

Search Conditions

Period from    DateTime to        DateTime	Observation point Select point <div style="border: 1px solid black; display: inline-block; padding: 2px;">Dropdown</div>	Incident type Select type <div style="border: 1px solid black; display: inline-block; padding: 2px;">Dropdown</div>
--	--	---

Detection Time	Reported Time	Incident Type	Source address	Incident name	Observation point

Publish

図 21 インシデント情報閲覧機能

## 5.3. 格納されたインシデント情報の検索

特定の種類のインシデントを以下のような条件で検索できる機能を有する。

- Period
- Observation point
- Incident type

各条件は”AND”論理演算等によって連携動作する。

### 5.3.1. Period

期間の最初と最後はカレンダー等の UI を使って指定する。

指定された時刻情報は IODEF メッセージの<Incident> -> <DetectionTime>クラスに適用される。

### 5.3.2. Observation point

Observation point は GUI から選択する。

Observation point の情報は IODEF メッセージの<Incident> -> <EventData> -> <Description> class に格納されている。

### 5.3.3. Incident type

Incident type は、ドロップダウンメニューのような UI で指定する。

Incident type 情報は IODEF メッセージの<Incident> -> <EventData> -> <Method> -> <Classification> -> name クラスに格納されている。

### 5.4. 格納されたインシデント情報の選択と、新たな IODEF メッセージの生成

インシデントは以下のように選択され、必要に応じて新たな IODEF メッセージとして出力される。

1. 上記機能を利用して検索し、選択する
2. Publish ボタンの押下
3. 選択したインシデント情報を含んだ新しい IODEF メッセージの生成

## 6. IODEF analyzer AP

IODEF analyzer AP は広域インシデント DB に蓄積されたインシデント情報を複数の観測点にわたって横断的に分析し、可視化する。

本システムでは、以下の 2 点について分析を行う。

1. 世界規模の DoS インシデント
2. 広く試みられている攻撃インシデント

### 6.1. 世界規模の DoS インシデント分析

本分析の目的は世界規模で広域に実施されている DoS 攻撃を検知、分析し、可視化することである。

本分析では、Source address を偽装した DoS 攻撃時に攻撃対象側から発生する応答パケットを入力として、その発生が広域に観測されるかどうかで、DoS 攻撃の有無を分析する。

本分析の基本フローを図 22 に示す。本プロトタイプでは TCP-Ack のケースを示しているが、応答として発生しうるすべてのパケットを対象とすることができる。

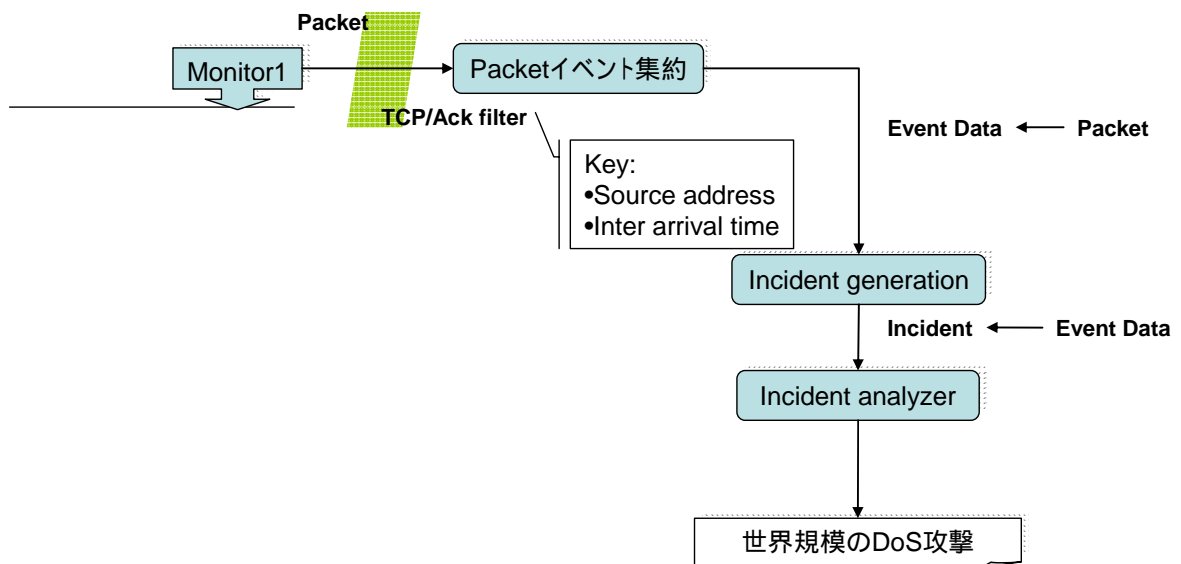


図 22 世界規模の DoS インシデント分析の基本フロー

#### 6.1.1. 分析の基本情報

広域インシデント DB から応答パケットに関連するインシデント情報を抽出し、その広が

り（観測点の数）に応じてソート、表示する。

## 分析アルゴリズム

1. 分析パラメータの指定
  - ・ 分析期間の指定
  - ・ Top N の指定
2. type of incident が“Packet”のインシデントを抽出
3. 各 source address 毎に以下の情報を抽出する
  - ・ イベントの数
  - ・ 観測点の数 (Degree of observation)
  - ・ 観測点のリスト
4. 観測点の数でソート
5. Top N を表示

### 6.1.2. 可視化

以下の 3 種類の可視化機能を有する。

- ・ 表形式
- ・ AS 地図形式
- ・ グラフ形式

## 表形式

本可視化形式では図 23 のような形式で可視化する。各列は、左から攻撃対象となっているサイト、観測されたイベント数、観測した観測点のリスト、同一パケットの数、観測点の数を表している。

DoS target	Number of Events	Points	データ	合計
61.129.115.106	292	em2 em3 em4 em8 em9 em11	合計 / Number of retry 合計 / Degree of ovservation	6 6
222.89.109.73	562	em2 em3 em4 em8 em9 em11	合計 / Number of retry 合計 / Degree of ovservation	0 6
222.33.96.115	55	em2 em3 em4 em8 em9 em11	合計 / Number of retry 合計 / Degree of ovservation	0 6
218.83.153.180	1279	em2 em3 em4 em8 em9 em11	合計 / Number of retry 合計 / Degree of ovservation	759 6
62.221.254.194	101	em0 em3 em4 em5 em11	合計 / Number of retry 合計 / Degree of ovservation	0 5
81.169.185.47	27	em3 em5 em9 em10	合計 / Number of retry 合計 / Degree of ovservation	0 4
202.96.140.88	27	em2 em8 em9 em11	合計 / Number of retry 合計 / Degree of ovservation	0 4
202.97.170.137	54	em0 em3 em10 em11	合計 / Number of retry 合計 / Degree of ovservation	3 4
70.85.216.13	34	em2 em5 em8 em10	合計 / Number of retry 合計 / Degree of ovservation	0 4
67.159.5.193	33	em3 em9 em10 em11	合計 / Number of retry 合計 / Degree of ovservation	0 4
61.187.185.26	69	em0 em3 em10 em11	合計 / Number of retry 合計 / Degree of ovservation	0 4
218.15.21.101	68	em8 em9 em10 em11	合計 / Number of retry 合計 / Degree of ovservation	0 4
61.174.171.195	63	em8 em9 em10 em11	合計 / Number of retry 合計 / Degree of ovservation	73 4
61.152.95.148	22	em8 em9 em10 em11	合計 / Number of retry 合計 / Degree of ovservation	0 4
61.152.252.235	66	em0 em3 em10 em11	合計 / Number of retry 合計 / Degree of ovservation	48 4
61.145.116.211	87	em0 em3 em10 em11	合計 / Number of retry 合計 / Degree of ovservation	87 4

図 23 DoS 攻撃に関連するインシデントの表形式可視化

### AS 地図形式

AS 地図形式では指定された Top N インシデントをネットワークポロジがわかる形式で可視化、表示する。

1. IP アドレスから AS 番号を抽出
2. 該当する AS を AS 地図上でハイライト
  - ・ Top N AS を異なる色でハイライト
  - ・ 深刻度を色で表現する。
    - A) In RGB, R=255, G and B = ( 150 / ( N - 1 ) ) ( n - 1 )
    - B) N is selected max Top N value, n = ranking, n =< N
3. 以下の情報を追加情報として表示する。
  - ・ IP address
  - ・ Country
  - ・ Number of events
  - ・ Number of observation point

## グラフ形式

一日毎のインシデント数（観測された延べインシデント数）を図 24 のように Bar グラフによって可視化する。観測されたソースアドレス毎にその発生数の推移を一日単位で示すものとする。

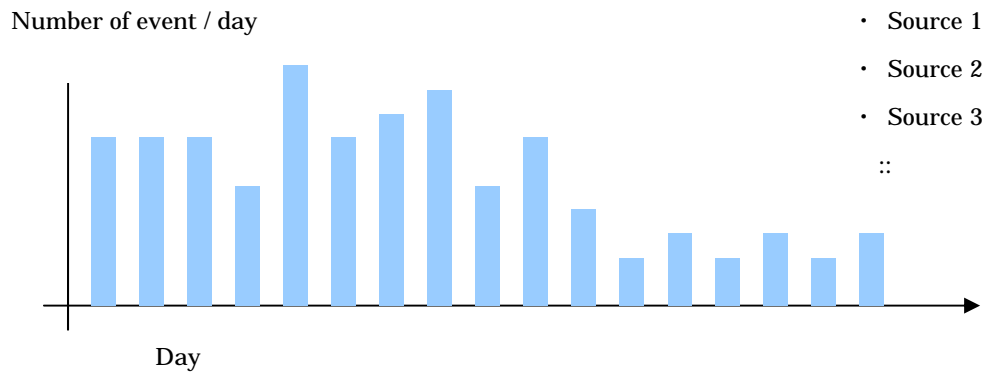


図 24 DoS 攻撃に関連するインシデントのグラフ形式可視化

### 6.2. 広く試みられている攻撃インシデント

本分析の目的は世界規模で広域に実施されている攻撃を検知、分析し、可視化するものである。

本分析では、SNORT によって検知されるアラート情報を入力として、その発生が広域に観測されるかどうかで、その広がりを分析する。

本分析の基本フローを図 25 に示す。

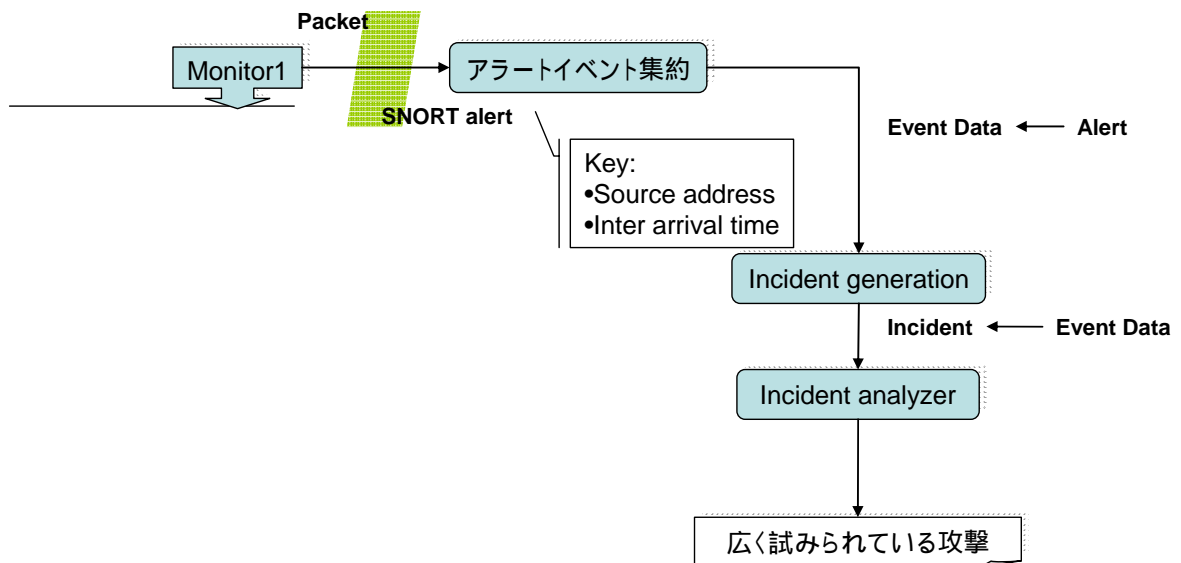


図 25 広く試みられている攻撃インシデント分析の基本フロー

### 6.2.1. 分析の基本情報

広域インシデント DB から応答パケットに関連するインシデント情報（ここでは TCP-A c k）を抽出し、その広がり（観測点の数）に応じてソート、表示する。

### 分析アルゴリズム

1. 分析パラメータの指定
  - ・ 分析期間の指定
  - ・ Top N の指定
2. type of incident が“Packet”のインシデントを抽出
3. 各 source address 毎に以下の情報を抽出する
  - ・ イベントの数
  - ・ 観測点の数 (Degree of observation)
  - ・ 観測点のリスト
  - ・ インシデント名
4. 観測点の数でソート
5. Top N を表示

### 6.2.2. 可視化

以下の 3 種類の可視化機能を有する。

- ・ 表形式
- ・ AS 地図形式
- ・ グラフ形式

## 表形式

本可視化形式では図 26 のような形式で可視化する。各列は、左から攻撃元となっているサイト、観測されたイベント数、観測した観測点のリスト、観測点の数、集約されたアラート種別の数を表している。

Attack Source	Number of Events	Points	データ	合計
64.17.32.7	322	em0 em2 em4 em5 em8 e	合計 / Degree of ovservation 合計 / Number of alert types	8 2
61.159.15.2	354	em0 em2 em4 em5 em8 e	合計 / Degree of ovservation 合計 / Number of alert types	8 2
61.152.144.33	310	em0 em2 em4 em5 em8 e	合計 / Degree of ovservation 合計 / Number of alert types	8 2
140.137.61.224	86	em0 em2 em4 em5 em8 e	合計 / Degree of ovservation 合計 / Number of alert types	8 2
61.129.32.96	144	em0 em2 em4 em5 em8 e	合計 / Degree of ovservation 合計 / Number of alert types	8 2
221.202.129.164	548	em0 em2 em4 em5 em8 e	合計 / Degree of ovservation 合計 / Number of alert types	8 2
218.25.253.19	170	em0 em2 em4 em5 em8 e	合計 / Degree of ovservation 合計 / Number of alert types	8 3
202.100.140.8	240	em0 em2 em4 em5 em8 e	合計 / Degree of ovservation 合計 / Number of alert types	8 2
218.25.230.245	316	em0 em2 em4 em5 em8 e	合計 / Degree of ovservation 合計 / Number of alert types	8 2
209.164.24.9	760	em0 em2 em4 em5 em8 e	合計 / Degree of ovservation 合計 / Number of alert types	8 2
203.121.68.9	296	em0 em2 em4 em5 em8 e	合計 / Degree of ovservation 合計 / Number of alert types	8 2
202.99.177.209	708	em0 em2 em4 em5 em8 e	合計 / Degree of ovservation 合計 / Number of alert types	8 2

図 26 広く試みられている攻撃に関連するインシデントの表形式可視化

## AS 地図形式

AS 地図形式では指定された Top N インシデントをネットワークポロジがわかる形式で可視化、表示する。

1. IP アドレスから AS 番号を抽出
2. 該当する AS を AS 地図上でハイライト
  - ・ Top N AS を異なる色でハイライト
  - ・ 深刻度を色で表現する。
    - A) In RGB, R=255, G and B = ( 150 / (N -1) ) (n-1)

B) N is selected max Top N value, n = ranking, n =< N

3. 以下の情報を追加情報として表示する。

- IP address
- Country
- Number of events
- Number of observation point

### グラフ形式

一日単位のインシデント数の推移を下図のように示す。観測されたソースアドレス毎にその発生数の推移を一日単位で示すものとする。

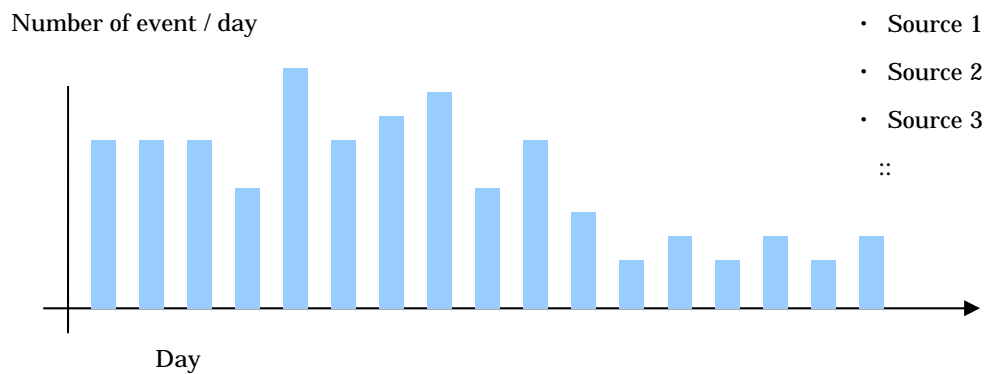


図 27 広く試みられている攻撃に関連するインシデントのグラフ形式可視化

## 7. SNMP-IODEF gateway

SNMP-IODEF gateway は個別に実行されるローカル追跡システムを広域に連携させるために、IODEF メッセージおよび RID メッセージを送受信する。

ローカル追跡システムは、どのような方式を用いたものでも、IODEF-RID を用いて連携することが可能であるが、本システムでは例として、ローカル追跡システムとして、SNMP を利用したシステムを活用し、複数の独立した SNMP を利用したローカル追跡システムを本 SNMP-IODEF gateway によって連携させる。

システムの概要を図 28 に示す。

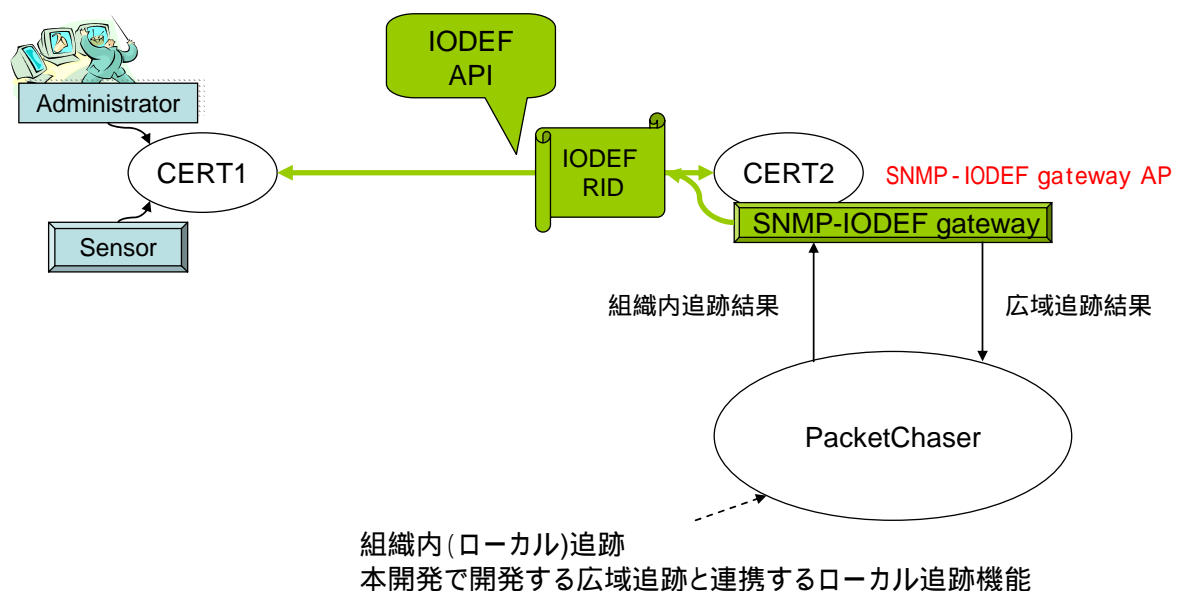


図 28 SNMP-IODEF gateway の概要

### 7.1. 基本メッセージング仕様

以下に、広域不正アクセス追跡のための RID, IODEF メッセージの生成、および SOAP による通信の基本構成を示す。

#### 7.1.1. メッセージ生成

本システムでは、追跡のためのメッセージング方式として、IETF で議論されている広域連携のための IODEF、RID に準拠した XML メッセージを SOAP を利用して転送する方式を利用する。

図 29 に追跡の対象となるパケット情報を含んだ SNMP によるアラートから、広域に Query を出すための SOAP メッセージを生成するための構造を示す。

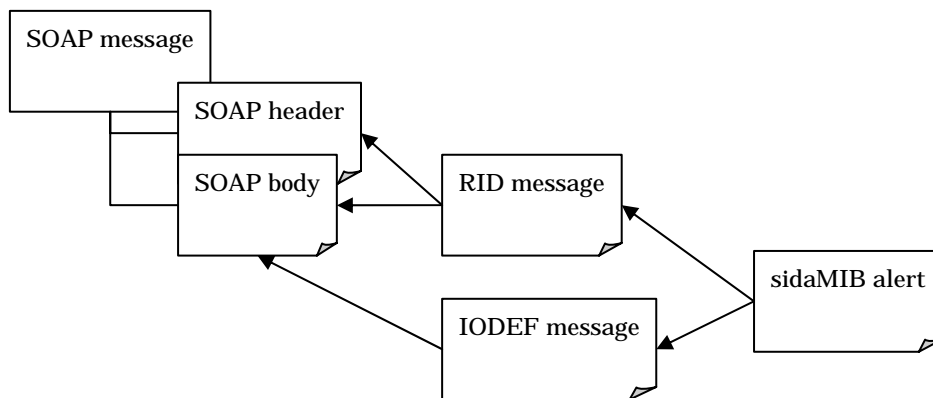


図 29 SOAP によるメッセージ交換のための IODEF,RID メッセージの構造

sidaMIB アラートに含まれている PacketPrint 情報および、時刻、ネットワーク情報から IODEF メッセージを生成し、RID メッセージには問い合わせ種別、問い合わせポリシーを記述する。

RID メッセージを SOAP ヘッダとボディに配し、IODEF メッセージも同じく SOAP ボディに配することで、SOAP メッセージを構成する。

#### 7.1.2. メッセージフロー

問い合わせの基本フローは以下ようになる。基本フローを図 30 に示す。

1. 広域不正アクセス追跡システムは SNORT からのアラートを受信する
2. 広域不正アクセス追跡システムはアラートから PacketPrint 情報を抽出する
3. 広域不正アクセス追跡システムは IODEF-RID メッセージを生成し、他のローカルパケット追跡システムに要求を出す。
4. 広域不正アクセス追跡システムは各ローカルパケット追跡システムからの応答を取得する。
5. 広域不正アクセス追跡システムは結果をネットワーク地図上に表示する。

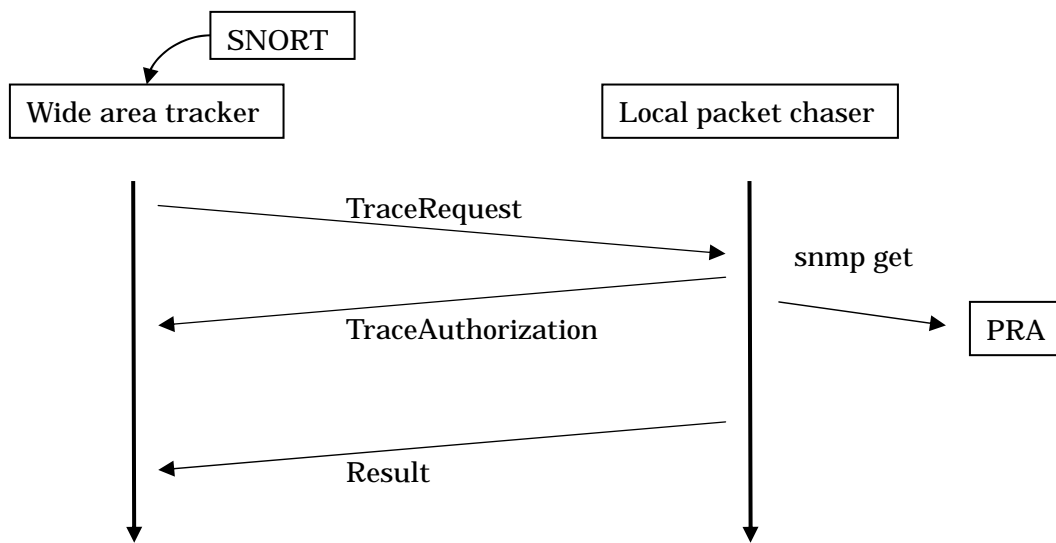


図 30 広域不正アクセス追跡メッセージの基本フロー

## 7.2. TraceRequest

追跡要求メッセージの生成仕様を以下にしめす。

### 7.2.1. IODEF message generation

IODEF 部分の生成を以下に示す。

#### **Element instance**

IncidentID

Prefix は“csrit.cysols.com#PacketChaser-”とする。

また、Query ごとに固有の ID を付与する。

```
<iodef:IncidentID Issuer="csrit.cysols.com">  
    csrit.cysols.com#PacketChaser-1  
</iodef:IncidentID>
```

Description

Description の値は一定とする。

```
<iodef:Description>  
    Host involved in DOS attack  
</iodef:Description>
```

ReportTime

ReportTime の値は“sidaAlertTimeStamp”から生成する。

Assessment

Assessment の属性と値は一定とする。

```
<iodef:Assessment>  
    <iodef:Impact iodef:severity="high"  
        iodef:completion="failed"  
        iodef:impacttype="none"/>
```

```
</iodef:Assessment>
```

## Contact

Contact の値はシステムの所有者とする。

```
<iodef:Contact iodef:contactrole="creator" iodef:contacttype="organization">
  <iodef:name>csrit.cysols.com</iodef:name>
  <iodef:Email>packetchaser@ipa</iodef:Email>
</iodef:Contact>
```

## Entire example

```
<?xml version="1.0" encoding="UTF-8"?>

<iodef:IODEF-Document version="0.40"
  xmlns:iodef="draft-ietf-inch-iodef-043.xsd">

  <iodef:Incident iodef:restriction="need-to-know" iodef:purpose="traceback">
    <iodef:IncidentID Issuer="csrit.cysols.com">
      csrit.cysols.com#PacketChaser-1
    </iodef:IncidentID>
    <iodef:Description>Host involved in DOS attack</iodef:Description>
    <iodef:Contact iodef:contactrole="creator" iodef:contacttype="organization">
      <iodef:name>csrit.cysols.com</iodef:name>
      <iodef:Email>packetchaser@ipa</iodef:Email>
    </iodef:Contact>
    <iodef:ReportTime>2004-02-02T23:20:24+00:00</iodef:ReportTime>
    <iodef:Assessment>
      <iodef:Impact iodef:severity="high"
        iodef:completion="failed"
        iodef:impacttype="none"/>
    </iodef:Assessment>
  </iodef:Incident>
</iodef:IODEF-Document>
```

## 7.2.2. RID message generation

RID 部分の生成を以下に示す。

### Element instance

IPVersion

IPVersion の値は一定とする。

```
<iodef-rid:IPVersion>IPv4</iodef-rid:IPVersion>
```

HexPacket

HexPacket の値は Snort アラートの“sidaAlertPacketPrint”から抽出するものとする。

NPPath

NPPath クラスのメンバーは IODEF の子要素からなる。

Query を生成するシステムはふたつの NPPath クラスが必要となる。ひとつは Query を生成するシステム用、一方は受信するシステム用とする。

iodef:name と iodef:Email は一定とし、システムの所有者の情報とする。

iodef:Node クラスは iodef:Address クラスを含む。iodef:Address の値と属性は Query を生成するシステムのものとする。

次の NPPath クラスは query 受信者と同じ情報を含む。

```
<iodef-rid:NPPath>
  <iodef:name>Cyber Solutions Inc.</iodef:name>
  <iodef:Node>
    <iodef:Address
      iodef:addrcat="ipv4-addr">172.17.1.2
    </iodef:Address>
  </iodef:Node>
  <iodef:Email>packetchaser@ipa</iodef:Email>
</iodef-rid:NPPath>
<iodef-rid:NPPath>
```

```
<iodef:name>WIDE</iodef:name>
<iodef:Node>
  <iodef:Address
    iodef:addrcat="ipv4-addr">192.154.3.1
  </iodef:Address>
</iodef:Node>
<iodef:Email>packetchaser@wide</iodef:Email>
</iodef-rid:NPPath>
```

## RIDPolicy

MsgType の値は“TraceRequest”とする。

MsgDestination の値は“RIDSystem”で一定とする。

iodef:Node の値はメッセージを受信するシステムの IP address とする。本システムではローカル追跡システムのアドレスとする。

PolicyRegion の値は“InterConsortium”で一定とする。

TrafficType の値は“Attack”で一定とする。

incidentID の値は 7.2.1 の IncidentID の値と同じでなければならない。

```
<iodef-rid:RIDPolicy iodef:dtype="xml">
  <iodef-rid:MsgType>TraceRequest</iodef-rid:MsgType>
  <iodef-rid:MsgDestination>RIDSystem
</iodef-rid:MsgDestination>
  <iodef:Node>
    <iodef:Address iodef:addrcat="ipv4-addr">172.20.1.2
  </iodef:Address>
  </iodef:Node>
  <iodef-rid:PolicyRegion>InterConsortium
</iodef-rid:PolicyRegion>
  <iodef-rid:TrafficType>Attack</iodef-rid:TrafficType>
  <iodef:IncidentID
    Issuer="csrit.cysols.com">csrit.cysols.com#PacketChaser-1
  </iodef:IncidentID>
```

```
</iodef-rid:RIDPolicy>
```

## Entire example

```
<?xml version="1.0" encoding="UTF-8"?>

<iodef-rid:RID iodef:dtype="xml"
  xmlns:iodef-rid="draft-ietf-inch-iodef-rid-05.xsd"
  xmlns:iodef="draft-ietf-inch-iodef-043.xsd">

  <iodef-rid:IPPacket>
    <iodef-rid:IPVersion>IPv4</iodef-rid:IPVersion>
    <iodef-rid:HexPacket>450000522ad90000ff06c41fc0a801020
a010102976d0050103e020810d94a1350021000ad6700005468616
e6b20796f7520666f722063617265666756c6c792072656164696e6
72074686973205246432e0a </iodef-rid:HexPacket>
  </iodef-rid:IPPacket>
  <iodef-rid:NPPath>
    <iodef:name>Cyber Solutions Inc.</iodef:name>
    <iodef:Node>
      <iodef:Address
        iodef:addrcat="ipv4-addr">172.17.1.2
      </iodef:Address>
    </iodef:Node>
    <iodef:Email>packetchaser@ipa</iodef:Email>
  </iodef-rid:NPPath>
  <iodef-rid:RIDPolicy iodef:dtype="xml">
    <iodef-rid:MsgType>TraceRequest</iodef-rid:MsgType>
    <iodef-rid:MsgDestination>RIDSsystem
  </iodef-rid:MsgDestination>
    <iodef:Node>
      <iodef:Address iodef:addrcat="ipv4-addr">172.20.1.2
    </iodef:Address>
    </iodef:Node>
    <iodef-rid:PolicyRegion>InterConsortium
  </iodef-rid:PolicyRegion>
```

```
<iodef-rid:TrafficType>Attack</iodef-rid:TrafficType>
<iodef:IncidentID
  Issuer="csrit.cysols.com">csrit.cysols.com#PacketChaser-1
</iodef:IncidentID>
</iodef-rid:RIDPolicy>
</iodef-rid:RID>
```

### 7.2.3. Soap message generation

SOAP message は以下の内容を含む SOAP envelop で構成される。

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope
  xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/">
HEADER
BODY
</SOAP:Envelope>
```

#### Soap header

SOAP header は 7.2.2 で生成した RID XML instance 全体を含む。

#### Soap body

SOAP body は 7.2.1 で生成した IODEF XML instance と 7.2.2 で生成した RID XML instance の両方を含む。

### 7.3. TraceAuthorization

ローカル追跡システムは traceRequest を受信し、Ack と状態情報を返す。

メッセージは応答用 RID メッセージとオリジナルの IODEF メッセージで構成される。

MsgType

MsgType class の値を以下のようにする。

```
<iodef-rid:MsgType>TraceAuthorization</iodef-rid:MsgType>
```

TraceStatus

TraceStatus 要素を RID message に挿入する。

```
<iodef-rid:TraceStatus>  
  <iodef-rid:AuthorizationStatus>  
    Approved  
  </iodef-rid:AuthorizationStatus>  
</iodef-rid:TraceStatus>
```

## 7.4. Result

ローカル追跡システムは traceRquest を受信し、Approved 状態を返す。その後受け取ったパケット情報を元にローカルでの追跡を実行する。

メッセージは応答用 RID メッセージとオリジナルの IODEF メッセージで構成される。

### 7.4.1. Local tracking

ローカル追跡の結果は以下のような情報として出力される。

Network	Found/NotFound
192.168.0.0/24	Yes
192.168.1.0/24	No
192.168.2.0/24	No

### 7.4.2. Generate Result

ローカル追跡システムは最終的な結果を RID XML メッセージとして生成する。

#### Template

Result メッセージは TraceAuthorization を基盤とする。

MsgType

MsgType class

```
<iodef-rid:MsgType>Result</iodef-rid:MsgType>
```

IncidentSource

ローカル追跡システムは 7.4.1 の結果を参照し、IncidentSource クラスを生成する。生成されたクラスは RID メッセージに挿入される。

IncidentSource class は 7.4.1 の各行から以下のように生成される。

If the result is positive “Yes”, then

The value of SourceFound is true

else

The value of SrouceFound is false

If SourceFound is true, then

The address information is listed by iodef:Node class under IncidentSource class

```
<iodef-rid:IncidentSource>
  <iodef-rid:SourceFound>true</iodef-rid:SourceFound>
  <iodef:Node>
    <iodef:Address
      iodef:addrcat="ipv4-net">192.168.0.0/24
    </iodef:Address>
    <iodef:NodeRole noderolecat="server-public"/>
  </iodef:Node>
  <iodef:Node>
    <iodef:Address
      iodef:addrcat="ipv4-addr">192.168.1.10
    </iodef:Address>
    <iodef:NodeRole noderolecat="server-internal"/>
  </iodef:Node>
</iodef-rid:IncidentSource>

<iodef-rid:IncidentSource>
  <iodef-rid:SourceFound>false</iodef-rid:SourceFound>
  <iodef:Node>
    <iodef:Address
      iodef:addrcat="ipv4-net">192.168.1.0/24
    </iodef:Address>
    <iodef:NodeRole noderolecat="server-public"/>
  </iodef:Node>
  <iodef:Node>
    <iodef:Address
      iodef:addrcat="ipv4-addr">192.168.1.11
    </iodef:Address>
    <iodef:NodeRole noderolecat="server-internal"/>
  </iodef:Node>
</iodef-rid:IncidentSource>
```

```
</iodef:Node>
</iodef-rid:IncidentSource>

<iodef-rid:IncidentSource>
  <iodef-rid:SourceFound>>false</iodef-rid:SourceFound>
  <iodef:Node>
    <iodef:Address
      iodef:addrcat="ipv4-net">192.168.2.0/24
    </iodef:Address>
    <iodef:NodeRole noderolecat="server-public"/>
  </iodef:Node>
  <iodef:Node>
    <iodef:Address
      iodef:addrcat="ipv4-addr">192.168.1.12
    </iodef:Address>
    <iodef:NodeRole noderolecat="server-internal"/>
  </iodef:Node>
</iodef-rid:IncidentSource>
```

## 7.5. 可視化

基本となる GUI を以下の地図表示となる。

### 7.5.1. Global map

システムは AS を基本とした地図を用いた UI を有し、追跡結果として攻撃が検知された AS を図 31 のようにハイライト表示する。

各 AS は、情報がある場合には詳細地図情報を保持する機能を有する。

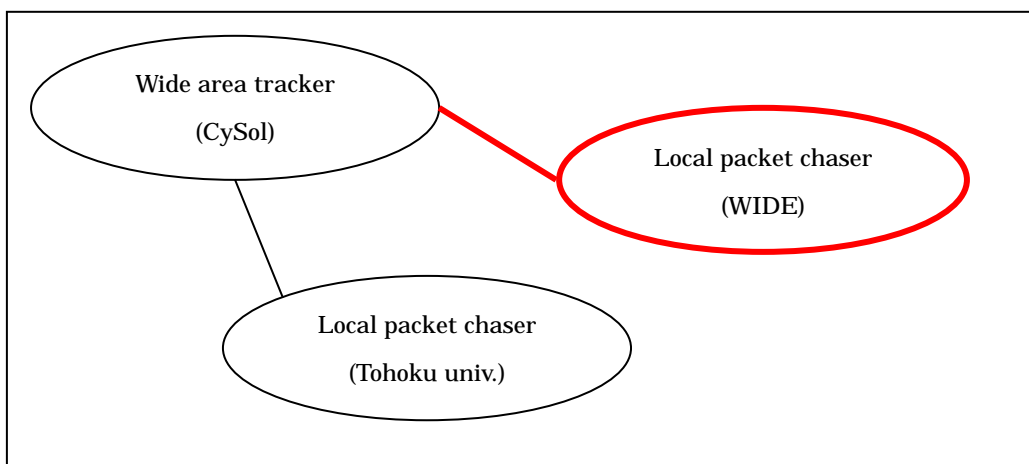


図 31 追跡結果の AS 地図表示

### 7.5.2. Detail map

追跡結果の IncidentSource クラスの情報を以下の図 32 のように表示する。

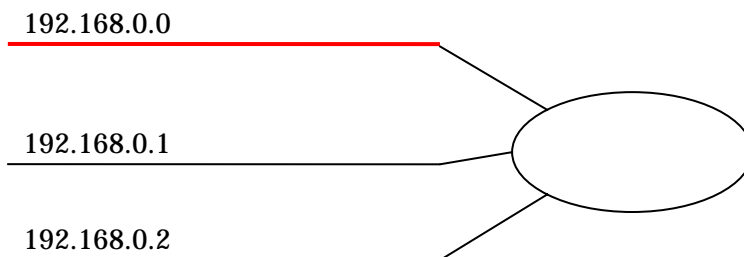


図 32 追跡結果の詳細地図表示

## 8. Appendix

本システムの開発にあたり、最新の標準案を活用したが、標準化過程のものであり、多くの変更、修正を行った。以下に本システムで対応している IODEF 関連メッセージの Schema を記載する。

### 8.1. IODEF Schema

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="draft-ietf-inch-iodef-043.xsd"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified"
  xmlns:iodef="draft-ietf-inch-iodef-043.xsd"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
  schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"/>

<!--
*****
*****
*** Incident Object Description and Exchange Format XML Schema ***
***           Version 04, August 2005           ***
***           draft-ietf-inch-iodef-04           ***
*****
*****
-->

<!--
=====
==  Element definitions                               ==
=====
-->
```

```

<!--
=====
== IODEF-Document class                                ==
=====
-->
<xs:annotation>
  <xs:documentation>Root Element IODEF-Document</xs:documentation>
</xs:annotation>
<xs:element name="IODEF-Document">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="iodef:Incident" maxOccurs="unbounded"/>
      <xs:element ref="ds:Signature" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="version" type="xs:string" fixed="0.40"/>
  </xs:complexType>
</xs:element>

<!--
=====
=== Incident class                                    ===
=====
-->
<xs:element name="Incident">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="iodef:IncidentID"/>
      <xs:element ref="iodef:AlternativeID" minOccurs="0"/>
      <xs:element ref="iodef:RelatedActivity" minOccurs="0"/>
      <xs:element ref="iodef:Description" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="iodef:Contact" maxOccurs="unbounded"/>
      <xs:element ref="iodef:ReportTime"/>
      <xs:element ref="iodef:DetectTime" minOccurs="0"/>
      <xs:element ref="iodef:StartTime" minOccurs="0"/>
      <xs:element ref="iodef:EndTime" minOccurs="0"/>
      <xs:element ref="iodef:Expectation" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

```

```

    <xs:element ref="iodef:Method" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element ref="iodef:Assessment" maxOccurs="unbounded"/>
    <xs:element ref="iodef:EventData" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element ref="iodef:History" minOccurs="0"/>
    <xs:element ref="iodef:AdditionalData" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute ref="iodef:restriction" default="private"/>
  <xs:attribute ref="iodef:purpose" use="required"/>
</xs:complexType>
</xs:element>
<!--
=====
== IncidentID class ==
=====
-->
<xs:element name="IncidentID" type="iodef:IncidentIDType"/>
<xs:complexType name="IncidentIDType" mixed="true">
  <xs:attribute name="Issuer" type="xs:string" use="required"/>
  <xs:attribute ref="iodef:restriction"/>
</xs:complexType>
<!--
=====
== AlternativeID class ==
=====
-->
<xs:element name="AlternativeID">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="iodef:IncidentID" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute ref="iodef:restriction"/>
  </xs:complexType>
</xs:element>
<!--
=====
== RelatedActivity class ==
=====

```

```

=====
-->
<xs:element name="RelatedActivity">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="iodef:IncidentID" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute ref="iodef:restriction"/>
  </xs:complexType>
</xs:element>
<!--
=====

===  AdditionalData class                                ===
=====

-->
<xs:element name="AdditionalData" type="iodef:AdditionalDataType"/>
<xs:complexType name="AdditionalDataType" mixed="true">
  <xs:sequence>
    <xs:any      namespace="##any"      processContents="lax"      minOccurs="0"
maxOccurs="unbounded"/>
    <!-- (0,unbounded) elements from any (target and external) namespace -->
  </xs:sequence>
  <xs:attribute ref="iodef:dtype" use="required"/>
  <xs:attribute name="meaning" type="xs:string"/>
</xs:complexType>
<!--
=====

===  Contact class                                ===
===  - Name
===  - RegistryHandle
===  - PostalAddress
===  - Email
===  - Telephone
===  - Fax
===  - TimeZone
===  - Contact (recursive)

```

```

=====
-->
<xs:element name="Contact">
  <xs:complexType>
    <xs:sequence>
      <!-- <xs:element ref="iodef:NameIdentifier" minOccurs="0"/> -->
      <xs:element ref="iodef:name" minOccurs="0"/>
      <xs:element ref="iodef:Description" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="iodef:RegistryHandle" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="iodef:PostalAddress" minOccurs="0"/>
      <xs:element ref="iodef:Email" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="iodef:Telephone" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="iodef:Fax" minOccurs="0"/>
      <xs:element ref="iodef:TimeZone" minOccurs="0"/>
      <xs:element ref="iodef:Contact" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute ref="iodef:contactrole" use="required"/>
    <xs:attribute ref="iodef:contacttype" use="required"/>
    <xs:attribute ref="iodef:restriction"/>
  </xs:complexType>
</xs:element>
<!--<xs:attribute ref="iodef:format"/> -->
<xs:element name="RegistryHandle">
  <xs:complexType mixed="true">
    <xs:attribute ref="iodef:registrytype" use="required"/>
  </xs:complexType>
</xs:element>
<xs:element name="PostalAddress">
  <xs:complexType mixed="true">
    <xs:attribute name="lang" type="xs:language"/>
  </xs:complexType>
</xs:element>
<xs:element name="Email" type="xs:string"/>
<xs:element name="Telephone" type="xs:string"/>
<xs:element name="Fax" type="xs:string"/>
<!--

```

```

=====
===  Time-based classes                               ===
=====

-->
<xs:element name="DateTime" type="xs:dateTime"/>
<xs:element name="ReportTime" type="xs:dateTime"/>
<xs:element name="DetectTime" type="xs:dateTime"/>
<xs:element name="StartTime" type="xs:dateTime"/>
<xs:element name="EndTime" type="xs:dateTime"/>
<xs:element name="TimeZone" type="iodef:TimeZoneType"/>
<xs:simpleType name="TimeZoneType">
  <xs:restriction base="xs:string">
    <xs:pattern value="[+¥-][0-9][0-9][0-9][0-9]"/>
  </xs:restriction>
</xs:simpleType>
<!--

=====
===  History class                                   ===
===    - HistoryItem                                ===
=====

-->
<xs:element name="History">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="iodef:HistoryItem" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute ref="iodef:restriction" default="default"/>
  </xs:complexType>
</xs:element>
<xs:element name="HistoryItem">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="iodef:DateTime"/>
      <xs:element ref="iodef:IncidentID" minOccurs="0"/>
      <xs:element ref="iodef:Description" maxOccurs="unbounded"/>
    </xs:sequence>

```

```

    <xs:attribute ref="iodef:restriction"/>
    <xs:attribute ref="iodef:historycat" default="other"/>
  </xs:complexType>
</xs:element>
<!--
=====
=== Expectation class                               ===
=====
-->
<xs:element name="Expectation">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="iodef:Description" maxOccurs="unbounded"/>
      <xs:element ref="iodef:Contact" minOccurs="0"/>
      <xs:element ref="iodef:StartTime" minOccurs="0"/>
      <xs:element ref="iodef:EndTime" minOccurs="0"/>
    </xs:sequence>
    <xs:attribute ref="iodef:restriction" default="default"/>
    <xs:attribute ref="iodef:priority"/>
    <xs:attribute ref="iodef:expectcat"/>
  </xs:complexType>
</xs:element>
<!--
=====
=== Method class                                   ===
=== - Classification                               ===
=====
-->
<xs:element name="Method">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="iodef:Classification" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="iodef:Description" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute ref="iodef:restriction"/>
  </xs:complexType>

```

```

</xs:element>
<xs:element name="Classification">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="iodef:name"/>
      <xs:element ref="iodef:url" minOccurs="0"/>
    </xs:sequence>
    <xs:attribute ref="iodef:origin" use="required"/>
  </xs:complexType>
</xs:element>
<!--
=====

===  Assessment class                                ===
===  - Impact
===  - TimeImpact
===  - MonetaryImpact
===  - Confidence
=====

-->
<xs:element name="Assessment">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="iodef:Impact" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="iodef:TimeImpact" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element          ref="iodef:MonetaryImpact"          minOccurs="0"
maxOccurs="unbounded"/>
      <xs:element ref="iodef:Confidence" minOccurs="0"/>
    </xs:sequence>
    <xs:attribute ref="iodef:restriction"/>
  </xs:complexType>
</xs:element>
<xs:element name="Impact">
  <xs:complexType mixed="true">
    <xs:attribute ref="iodef:severity"/>
    <xs:attribute ref="iodef:completion"/>
    <xs:attribute ref="iodef:impacttype" use="optional" default="unknown"/>

```

```

    <xs:attribute name="lang" type="xs:language"/>
  </xs:complexType>
</xs:element>
<xs:element name="TimeImpact">
  <xs:complexType mixed="true">
    <xs:attribute ref="iodef:severity"/>
    <xs:attribute name="unit" use="required">
      <xs:simpleType>
        <xs:restriction base="xs:NMTOKEN">
          <xs:enumeration value="labor"/>
          <xs:enumeration value="elapsed"/>
          <xs:enumeration value="downtime"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:attribute>
    <xs:attribute name="metric" use="required">
      <xs:simpleType>
        <xs:restriction base="xs:NMTOKEN">
          <xs:enumeration value="days"/>
          <xs:enumeration value="hours"/>
          <xs:enumeration value="minutes"/>
          <xs:enumeration value="seconds"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:attribute>
  </xs:complexType>
</xs:element>
<xs:element name="MonetaryImpact">
  <xs:complexType mixed="true">
    <xs:attribute ref="iodef:severity"/>
    <xs:attribute name="currency" type="xs:string"/>
  </xs:complexType>
</xs:element>
<xs:element name="Confidence">
  <xs:complexType>
    <xs:attribute ref="iodef:rating" use="required"/>
  </xs:complexType>

```

```

    </xs:complexType>
  </xs:element>
<!--
=====
===  EventData class                                ===
=====
-->
<xs:element name="EventData">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="iodef:Description" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="iodef:Contact" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="iodef:DetectTime" minOccurs="0"/>
      <xs:element ref="iodef:StartTime" minOccurs="0"/>
      <xs:element ref="iodef:EndTime" minOccurs="0"/>
      <xs:element ref="iodef:Flow" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="iodef:System" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="iodef:Method" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="iodef:Assessment" minOccurs="0"/>
      <xs:element ref="iodef:EventData" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="iodef:Record" minOccurs="0"/>
      <xs:element ref="iodef:AdditionalData" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute ref="iodef:restriction" default="default"/>
  </xs:complexType>
</xs:element>
<!--
=====
===  Flow class                                    ===
=====
-->
<xs:element name="Flow">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="iodef:System" maxOccurs="unbounded"/>
    </xs:sequence>

```

```

</xs:complexType>
</xs:element>
<!--
=====
===  System class                                ===
=====
-->
<xs:element name="System">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="iodef:Node"/>
      <xs:element ref="iodef:Service" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="iodef:OperatingSystem" minOccurs="0"/>
      <xs:element ref="iodef:Counter" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute ref="iodef:restriction"/>
    <xs:attribute name="interface" type="xs:string"/>
    <xs:attribute ref="iodef:systemcat"/>
    <xs:attribute ref="iodef:spoofed" default="unknown"/>
  </xs:complexType>
</xs:element>

<!--
=====
===  Node class                                  ===
=====
-->
<xs:element name="Node">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="iodef:DateTime" minOccurs="0"/>
      <xs:element ref="iodef:name" minOccurs="0"/>
      <xs:element ref="iodef:Address" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="iodef:Location" minOccurs="0"/>
      <xs:element ref="iodef:NodeRole" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="iodef:Counter" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

```

```

    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="Address">
  <xs:complexType mixed="true">
    <xs:attribute ref="iodef:addrcat" use="required"/>
    <xs:attribute name="vlan-name" type="xs:string"/>
    <xs:attribute name="vlan-num" type="xs:string"/>
  </xs:complexType>
</xs:element>
<xs:element name="Location" type="xs:string"/>
<xs:element name="NodeRole">
  <xs:complexType mixed="true">
    <xs:attribute ref="iodef:noderolecat" use="required"/>
    <xs:attribute name="lang" type="xs:language"/>
  </xs:complexType>
</xs:element>
<!--
=====
===  Service Class                                ===
=====
-->
<xs:element name="Service">
  <xs:complexType>
    <xs:sequence>
      <xs:choice>
        <xs:element ref="iodef:port"/>
        <xs:element ref="iodef:portlist"/>
      </xs:choice>
      <xs:element ref="iodef:Application" minOccurs="0"/>
    </xs:sequence>
    <!-- Added attributes by CySOI -->
    <xs:attribute name="ip_version" type="xs:integer" use="required"/>
    <xs:attribute name="ip_protocol" type="xs:integer" use="required"/>
  </xs:complexType>
</xs:element>

```

```

<xs:element name="port" type="xs:string"/>
<xs:element name="portlist" type="xs:string"/>

<!--
=====
===  Application class                                ===
=====
-->
<xs:element name="Application">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="iodef:url" minOccurs="0"/>
      <xs:element ref="iodef:name" minOccurs="0"/>
    </xs:sequence>
    <xs:attribute name="appid" type="xs:string" default="0"/>
    <xs:attribute name="configid" type="xs:string" default="0"/>
    <xs:attribute name="vendor" type="xs:string"/>
    <xs:attribute name="version" type="xs:string"/>
  </xs:complexType>
</xs:element>

<!--
=====
===  OperatingSystem class                            ===
=====
-->
<xs:element name="OperatingSystem">
  <xs:complexType>
    <xs:attribute name="vendor" type="xs:string"/>
    <xs:attribute name="version" type="xs:string"/>
    <xs:attribute name="patch" type="xs:string"/>
  </xs:complexType>
</xs:element>

<!--
=====
===  Counter class                                    ===
=====

```

```

=====
-->
<xs:element name="Counter">
  <xs:complexType>
    <xs:attribute ref="iodef:countertype" default="other"/>
    <xs:attribute name="meaning" type="xs:string" use="optional"/>
  </xs:complexType>
</xs:element>
<!--
=====

=== Record class ===
=====

-->
<xs:element name="Record">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="iodef:RecordData" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute ref="iodef:restriction"/>
  </xs:complexType>
</xs:element>
<xs:element name="RecordData">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="iodef:DateTime" minOccurs="0"/>
      <xs:element ref="iodef:Description" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="iodef:Application" minOccurs="0"/>
      <xs:element ref="iodef:RecordItem" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute ref="iodef:restriction"/>
  </xs:complexType>
</xs:element>
<xs:element name="RecordSource" type="iodef:RecordSourceType"/>
<xs:complexType name="RecordSourceType" mixed="true">
  <xs:attribute name="recsourcetype" type="xs:string" use="optional"/>
</xs:complexType>

```

```

<xs:element name="Pattern" type="xs:string"/>
<xs:element name="PatternLocation" type="iodef:PatternLocationType"/>
<xs:complexType name="PatternLocationType" mixed="true">
  <xs:attribute name="recdtype" type="xs:string" use="optional"/>
</xs:complexType>
<!-- <xs:element name="Count" type="xs:integer"/> -->
<!--Element Analyzer of IODEF is re-used from IDMEF (4.2.4.1) -->
<xs:element name="Sensor">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="iodef:Node" minOccurs="0"/>
      <!-- removed in expectation of Analyser simplification -->
      <!-- <xs:element ref="iodef:Process" minOccurs="0"/> -->
      <xs:element ref="iodef:Process" minOccurs="0"/>
    </xs:sequence>
    <xs:attribute name="analyzerid" type="xs:string" default="0"/>
    <xs:attribute name="manufacturer" type="xs:string"/>
    <xs:attribute name="model" type="xs:string"/>
    <xs:attribute name="version" type="xs:string"/>
    <xs:attribute name="class" type="xs:string"/>
    <xs:attribute name="ostype" type="xs:string"/>
    <xs:attribute name="osversion" type="xs:string"/>
  </xs:complexType>
</xs:element>
<xs:element name="Process">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="iodef:name" minOccurs="0"/>
      <xs:element name="arg" type="xs:string" minOccurs="0"/>
      <xs:element name="env" type="xs:string" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="RecordItem" type="iodef:AdditionalDataType"/>
<!--

```

```

=====
=== Description class                                     ===
=== (contains attribute "transform" to preserve non-UTF-8 text encoding)
=====

-->
<xs:element name="Description" type="iodef:MultilingTextType"/>
<xs:complexType name="MultilingTextType" mixed="true">
  <xs:complexContent mixed="true">
    <xs:extension base="iodef:TextAbstractType">
      <xs:attribute ref="iodef:preserve"/>
      <xs:attribute ref="iodef:transform"/>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
<!-- <xs:element name="Text" type="iodef:TextAbstractType"/> -->
<xs:complexType name="TextAbstractType" mixed="true">
  <xs:annotation>
    <xs:documentation xml:lang="en">Textual description, may use local languages.
    For particular use may be extended with optional attributes "preserve"={0,1} and
"transformation"
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent mixed="true">
    <xs:restriction base="xs:anyType">
      <xs:sequence>
        <xs:any processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
      <xs:attribute name="lang" type="xs:language"/>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>
<!--
| Values for the Description.preserve attributes
-->
<xs:attribute name="preserve">
  <xs:simpleType>

```

```

    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="no"/>
      <xs:enumeration value="yes"/>
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>
<xs:attribute name="transform">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="none"/>
      <xs:enumeration value="Base64"/>
      <xs:enumeration value="QP"/>
      <xs:enumeration value="stringprep"/>
      <xs:enumeration value="zip"/>
      <xs:enumeration value="URI"/>
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>
<!--
=====
=== Miscellaneous simple classes                               ===
===   - name                                                    ===
===   - url                                                      ===
  <xs:element name="name" type="MultilingTextType"/>
  <xs:element name="name" type="xs:string"/>
  <xs:element name="name" type="NameidType"/>
  <xs:complexType name="NameidType">
    <xs:complexContent>
      <xs:extension base="iodef:MultilingTextType"/>
    </xs:complexContent>
  </xs:complexType>

=====
-->
  <xs:element name="name" type="iodef:MultilingTextType"/>
  <xs:element name="number" type="xs:string"/>

```

```

<xs:element name="url" type="xs:string"/>
<!--
=====
=== Attribute list declarations.          ===
=====
-->
<!--
| Attributes of the IODEF element.  In general, the fixed value
| of this attribute will change each time a new version of
| the DTD is released.
-->
<!--
| Values for the Address.category attribute.
-->
<xs:attribute name="addrcat">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="asn"/>
      <xs:enumeration value="atm"/>
      <xs:enumeration value="e-mail"/>
      <xs:enumeration value="mac"/>
      <xs:enumeration value="ipv4-addr"/>
      <xs:enumeration value="ipv4-net"/>
      <xs:enumeration value="ipv4-net-mask"/>
      <xs:enumeration value="ipv6-addr"/>
      <xs:enumeration value="ipv6-net"/>
      <xs:enumeration value="ipv6-net-mask"/>
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>
<!--
| Values for the Impact.completion attribute.
-->
<xs:attribute name="completion">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">

```

```

    <xs:enumeration value="failed"/>
    <xs:enumeration value="succeeded"/>
  </xs:restriction>
</xs:simpleType>
</xs:attribute>
<!--
| Values for the Contact.role attribute.
-->
<xs:attribute name="contactrole">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="creator"/>
      <xs:enumeration value="admin"/>
      <xs:enumeration value="tech"/>
      <xs:enumeration value="irt"/>
      <xs:enumeration value="cc"/>
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>
<!--
| Values for the Contact.type attribute.
-->
<xs:attribute name="contacttype">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="person"/>
      <xs:enumeration value="organization"/>
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>
<!--
| Values for the Counter.type attribute.
-->
<xs:attribute name="countertype">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">

```

```

    <xs:enumeration value="packet"/>
    <xs:enumeration value="session"/>
    <xs:enumeration value="event"/>
    <xs:enumeration value="other"/>
  </xs:restriction>
</xs:simpleType>
</xs:attribute>
<!--
| Values for the RecordItem.type attribute
-->
<xs:attribute name="dtype">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="boolean"/>
      <xs:enumeration value="byte"/>
      <xs:enumeration value="character"/>
      <xs:enumeration value="date-time"/>
      <xs:enumeration value="integer"/>
      <xs:enumeration value="ntpstamp"/>
      <xs:enumeration value="portlist"/>
      <xs:enumeration value="real"/>
      <xs:enumeration value="string"/>
      <xs:enumeration value="file"/>
      <xs:enumeration value="path"/>
      <xs:enumeration value="frame"/>
      <xs:enumeration value="packet"/>
      <xs:enumeration value="ipv4-packet"/>
      <xs:enumeration value="ipv6-packet"/>
      <xs:enumeration value="url"/>
      <xs:enumeration value="xml"/>
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>
<!--
| Values for the Expectation.expectcat attributes
-->

```

```

<xs:attribute name="expectcat">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="nothing"/>
      <xs:enumeration value="contact-site"/>
      <xs:enumeration value="contact-me"/>
      <xs:enumeration value="block"/>
      <xs:enumeration value="investigate"/>
      <xs:enumeration value="other"/>
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>
<!--
| Values for the File.category attribute.
-->
<xs:attribute name="filecat">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="current"/>
      <xs:enumeration value="original"/>
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>
<!--
| Values for the NameIdentifier.format attribute.
-->
<xs:attribute name="format">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="emailAddress"/>
      <xs:enumeration value="x509NameQualifier"/>
      <xs:enumeration value="urn"/>
      <xs:enumeration value="local"/>
      <xs:enumeration value="other"/>
    </xs:restriction>
  </xs:simpleType>

```

```

</xs:attribute>
<!--
| Values for the History.type attribute.
-->
<xs:attribute name="historycat">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="triaged"/>
      <xs:enumeration value="notification"/>
      <xs:enumeration value="shared-info"/>
      <xs:enumeration value="received-info"/>
      <xs:enumeration value="remediation"/>
      <xs:enumeration value="other"/>
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>
<!--
| Values for the Impact.type attribute.
-->
<xs:attribute name="impacttype">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="none"/>
      <xs:enumeration value="admin"/>
      <xs:enumeration value="dos"/>
      <xs:enumeration value="file"/>
      <xs:enumeration value="recon"/>
      <xs:enumeration value="user"/>
      <xs:enumeration value="unknown"/>
      <xs:enumeration value="other"/>
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>
<!--
| Values for the NodeRole.category attribute.
-->

```

```

<xs:attribute name="noderolecat">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="client"/>
      <xs:enumeration value="server-internal"/>
      <xs:enumeration value="server-public"/>
      <xs:enumeration value="www"/>
      <xs:enumeration value="mail"/>
      <xs:enumeration value="messaging"/>
      <xs:enumeration value="streaming"/>
      <xs:enumeration value="voice"/>
      <xs:enumeration value="file"/>
      <xs:enumeration value="ftp"/>
      <xs:enumeration value="p2p"/>
      <xs:enumeration value="name"/>
      <xs:enumeration value="directory"/>
      <xs:enumeration value="credential"/>
      <xs:enumeration value="print"/>
      <xs:enumeration value="application"/>
      <xs:enumeration value="database"/>
      <xs:enumeration value="infra"/>
      <xs:enumeration value="log"/>
      <xs:enumeration value="other"/>
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>
<!--
| Values for the Classification.origin attribute.
-->
<xs:attribute name="origin">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="bugtraqid"/>
      <xs:enumeration value="cve"/>
      <xs:enumeration value="certcc"/>
      <xs:enumeration value="vendor"/>
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>

```

```

        <xs:enumeration value="local"/>
        <xs:enumeration value="other"/>
    </xs:restriction>
</xs:simpleType>
</xs:attribute>
<!--
| Values for the Expectation.priority attributes
-->
<xs:attribute name="priority">
    <xs:simpleType>
        <xs:restriction base="xs:NMTOKEN">
            <xs:enumeration value="low"/>
            <xs:enumeration value="medium"/>
            <xs:enumeration value="high"/>
        </xs:restriction>
    </xs:simpleType>
</xs:attribute>
<!--
| Defines purpose of the Incident
-->
<xs:attribute name="purpose">
    <xs:simpleType>
        <xs:restriction base="xs:NMTOKEN">
            <xs:enumeration value="traceback"/>
            <xs:enumeration value="mitigation"/>
            <xs:enumeration value="reporting"/>
            <xs:enumeration value="other"/>
        </xs:restriction>
    </xs:simpleType>
</xs:attribute>
<!--
| Values for the Confidence.rating attribute.
-->
<xs:attribute name="rating">
    <xs:simpleType>
        <xs:restriction base="xs:NMTOKEN">

```

```

    <xs:enumeration value="low"/>
    <xs:enumeration value="medium"/>
    <xs:enumeration value="high"/>
    <xs:enumeration value="numeric"/>
    <xs:enumeration value="unknown"/>
  </xs:restriction>
</xs:simpleType>
</xs:attribute>
<!--
| Values for the RegistryHandle.type attribute.
-->
<xs:attribute name="registrytype">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="internic"/>
      <xs:enumeration value="apnic"/>
      <xs:enumeration value="arin"/>
      <xs:enumeration value="lacnic"/>
      <xs:enumeration value="ripencc"/>
      <xs:enumeration value="ti"/>
      <xs:enumeration value="local"/>
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>
<!--
| Defines restriction on access to an element's content
-->
<xs:attribute name="restriction">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="default"/>
      <xs:enumeration value="public"/>
      <xs:enumeration value="need-to-know"/>
      <xs:enumeration value="private"/>
    </xs:restriction>
  </xs:simpleType>

```

```

</xs:attribute>
<!--
| Values for the Impact.severity attribute.
-->
<xs:attribute name="severity">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="low"/>
      <xs:enumeration value="medium"/>
      <xs:enumeration value="high"/>
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>
<!--
| Values for the System.spoofed attributes
-->
<xs:attribute name="spoofed">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="unknown"/>
      <xs:enumeration value="yes"/>
      <xs:enumeration value="no"/>
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>
<!--
| Values for the System.category attribute
-->
<xs:attribute name="systemcat">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="source"/>
      <xs:enumeration value="target"/>
      <xs:enumeration value="intermediate"/>
    </xs:restriction>
  </xs:simpleType>

```

</xs:attribute>

<!--

#### Full Copyright Statement

Copyright (C) The Internet Society (2002). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

#### Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

-->

```
</xs:schema>
```

## 8.2. RID Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XMLSPY v2004 rel. 3 U (http://www.xmlspy.com) by
      Kathleen M Moriarty (MIT Lincoln Laboratory) -->
<xs:schema xmlns:iodef-rid="draft-ietf-inch-iodef-rid-05.xsd"
  xmlns:iodef="draft-ietf-inch-iodef-043.xsd"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:ns1="draft-ietf-inch-iodef-rid-05.xsd"
  targetNamespace="draft-ietf-inch-iodef-rid-05.xsd"
  elementFormDefault="qualified" attributeFormDefault="unqualified">
<xs:import namespace="draft-ietf-inch-iodef-043.xsd"
  schemaLocation="http://www.cysol.co.jp/~kohei/draft-ietf-inch-iodef-044-5.xsd"/>
<xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
  schemaLocation=
    "http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"/>
<!-- *****
*****
*** Incident Object Description and Exchange Format XML Schema ***
***                               Version 02, April 2005                               ***
*****
*** Real-time Inter-network Defense - RID XML Schema ***
***   Namespace - iodef-rid, July 2005   ***
***   The namespace is defined to support transport of IODEF ***
***   documents for exchanging incident information ***
*****
-->
<!--RID acts as an envelope for IODEF documents to support the exchange
      of messages-->
<!--
===== Real-Time Inter-network Defense - RID =====
===== Suggested definition for RID messaging =====
-->
```

```

<xs:annotation>
  <xs:documentation>XML Schema wrapper for IODEF</xs:documentation>
</xs:annotation>
<xs:element name="RID" type="iodef-rid:RIDType"/>
  <xs:complexType name="RIDType">
    <xs:sequence>
      <xs:element ref="iodef-rid:IPPacket" minOccurs="0"/>
      <xs:element ref="iodef-rid:NPPath" maxOccurs="unbounded"/>
      <xs:element ref="iodef-rid:TraceStatus" minOccurs="0"/>
      <xs:element ref="iodef-rid:IncidentSource" minOccurs="0"/>
      <xs:element ref="iodef-rid:RIDPolicy"/>
    </xs:sequence>
    <xs:attribute ref="iodef:dtype" use="required"/>
    <xs:attribute name="meaning" type="xs:string"/>
  </xs:complexType>
  <!--The IP Packet to be traced with RID-->
  <xs:element name="IPPacket" type="iodef-rid:IPPacketType"/>
    <xs:complexType name="IPPacketType">
      <xs:sequence>
        <xs:element name="IPVersion" type="xs:string" default="IPv4"/>
        <xs:element name="HexPacket" type="xs:hexBinary"/>
        <xs:element ref="iodef-rid:IPPacket"
          minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
      <xs:attribute ref="iodef:restriction" default="default"/>
    </xs:complexType>
    <xs:element name="IPVersion"/>
    <xs:element name="HexPacket"/>

  <!--Path of the RID trace includes information on each NP
    involved in the upstream trace-->
  <xs:element name="NPPath" type="iodef-rid:NPPathType"/>
    <xs:complexType name="NPPathType">
      <xs:sequence>
        <xs:element ref="iodef:name" minOccurs="0"/>
        <xs:element ref="iodef:RegistryHandle" minOccurs="0"

```

```

        maxOccurs="unbounded"/>
<xs:element ref="iodef:Node"/>
<xs:element ref="iodef:Email" minOccurs="0"
        maxOccurs="unbounded"/>
<xs:element ref="iodef:Telephone" minOccurs="0"
        maxOccurs="unbounded"/>
<xs:element ref="iodef:Fax" minOccurs="0"/>
<xs:element ref="iodef:TimeZone" minOccurs="0"/>
<xs:element ref="iodef-rid:NPPPath" minOccurs="0" maxOccurs="unbounded"/>
</xs:sequence>
<xs:attribute name="restriction" type="xs:NMTOKEN"/>
<!-- Edited by CySol
<xs:attribute name="NPPPath" type="xs:NMTOKEN" use="required"/>
-->
</xs:complexType>
<xs:element name="TimeZone"/>
<!--Used in Trace Authorization Message for RID-->
<xs:element name="TraceStatus" type="iodef-rid:TraceStatusType"/>
<xs:complexType name="TraceStatusType">
  <xs:sequence>
    <xs:element name="AuthorizationStatus" default="Approved">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:whiteSpace value="collapse"/>
          <xs:enumeration value="Approved"/>
          <xs:enumeration value="Denied"/>
          <xs:enumeration value="Pending"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
  </xs:sequence>
  <xs:attribute name="restriction" type="xs:NMTOKEN"/>
</xs:complexType>
<xs:element name="AuthorizationStatus" type="xs:decimal"/>
<!--Values for the NPPPath.type attribute-->
<xs:attribute name="NPPPath" type="xs:NMTOKEN"/>

```

```

<xs:attribute name="vlan-name" type="xs:string"/>
<xs:attribute name="vlan-num" type="xs:string"/>
<!-- Incident Source Information for Result Message -->
<xs:element name="IncidentSource" type="iodef-rid:IncidentSourceType"/>
  <xs:complexType name="IncidentSourceType">
    <xs:sequence>
      <xs:element ref="iodef-rid:SourceFound"/>
      <xs:element ref="iodef:Node" minOccurs="0"
        maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
  <xs:element name="SourceFound" type="xs:boolean"/>
<!--
===== Real-Time Inter-network Defense Policy - RIDPolicy =====
===== Suggested definition for RIDPolicy for messaging
-->
<xs:annotation>
  <xs:documentation>RID Policy used in SOAP header for transport of
    messages</xs:documentation>
</xs:annotation>
<!-- RidPolicy information with setting information listed in RID
    documentation -->
<xs:element name="RIDPolicy" type="iodef-rid:RIDPolicyType"/>
  <xs:complexType name="RIDPolicyType">
    <xs:sequence>
      <xs:element ref="iodef-rid:MsgType"/>
      <xs:element ref="iodef-rid:MsgDestination"/>
      <xs:element ref="iodef:Node"/>
      <xs:element ref="iodef-rid:PolicyRegion" maxOccurs="unbounded"/>
      <xs:element ref="iodef-rid:TrafficType" maxOccurs="unbounded"/>
      <xs:element ref="iodef:IncidentID"/>
    </xs:sequence>
    <xs:attribute ref="iodef:dtype" use="required"/>
  </xs:complexType>
  <xs:element name="MsgType" default="Report">
    <xs:simpleType>

```

```

<xs:restriction base="xs:string">
  <xs:whiteSpace value="collapse"/>
  <xs:enumeration value="TraceRequest"/>
  <xs:enumeration value="TraceAuthorization"/>
  <xs:enumeration value="Result"/>
  <xs:enumeration value="Investigation"/>
  <xs:enumeration value="Report"/>
  <xs:enumeration value="IncidentQuery"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name="MsgDestination" default="RIDSsystem">
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:whiteSpace value="collapse"/>
      <xs:enumeration value="RIDSsystem"/>
      <xs:enumeration value="SourceOfIncident"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>
<xs:element name="PolicyRegion">
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:whiteSpace value="collapse"/>
      <xs:enumeration value="ClientToNP"/>
      <xs:enumeration value="NPToClient"/>
      <xs:enumeration value="InterConsortium"/>
      <xs:enumeration value="PeerToPeer"/>
      <xs:enumeration value="BetweenConsortiums"/>
      <xs:enumeration value="AcrossNationalBoundaries"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>
<xs:element name="TrafficType" default="Attack">
  <xs:simpleType>
    <xs:restriction base="xs:string">

```

```
<xs:whiteSpace value="collapse"/>
  <xs:enumeration value="Attack"/>
  <xs:enumeration value="Network"/>
  <xs:enumeration value="Content"/>
  <xs:enumeration value="OfficialBusiness"/>
  <xs:enumeration value="Other"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
</xs:schema>
```

<sup>i</sup> 独立行政法人 情報処理推進機構, “「インターネット定点観測システム」について”, <http://www.ipa.go.jp/about/press/20040511.html>, 2004 年 5 月 11 日

<sup>ii</sup> Yuri Demchenko, Hiroyuki Ohno, Roman Danyliw, Glenn M Keeni, “Requirements for the Format for INcident information Exchange (FINE)”, Internet-Draft, Work in progress, September 7, 2005

<sup>iii</sup> Kathleen M. Moriarty, “Incident Handling: Real-time Inter-network Defense”, Internet-Draft, Work in progress, September 19, 2005

<sup>iv</sup> xindice: <http://xml.apache.org/xindice/> ネイティブ XML データベースの実装 .

<sup>v</sup> James: <http://james.apache.org/> Maillet とは, 各々に応じた電子メールサーバーの処理用に組み込まれている独立したメール処理ロジックです . この、書きやすく使いやすい手法により, 開発者はカスタマイズ可能な強力なメールシステムを構築することが出来るようになります . Maillet が可能とするサービスの例を挙げると : メール->FAX あるいはメール->電話 への変換 / メールフィルタリング / メール翻訳 / メールリングリスト管理などです . Maillet のうちの一部が JAMES の配布版に含まれています .