

国际电信联盟

ITU-T

国际电信联盟
电信标准化部门

X.1541

(09/2012)

X系列：数据网、开放系统通信和安全性
网络安全信息交换 – 事件/事故/探索法交换

事件对象描述交换格式

ITU-T X.1541建议书

ITU-T



ITU-T X 系列建议书
数据网、开放系统通信和安全性

| | |
|--------------------|----------------------|
| 公用数据网 | X.1–X.199 |
| 开放系统互连 | X.200–X.299 |
| 网间互通 | X.300–X.399 |
| 报文处理系统 | X.400–X.499 |
| 号码簿 | X.500–X.599 |
| OSI组网和系统概貌 | X.600–X.699 |
| OSI管理 | X.700–X.799 |
| 安全 | X.800–X.849 |
| OSI应用 | X.850–X.899 |
| 开放分布式处理 | X.900–X.999 |
| 信息和网络安全 | |
| 一般安全问题 | X.1000–X.1029 |
| 网络安全 | X.1030–X.1049 |
| 安全管理 | X.1050–X.1069 |
| 生物测定安全 | X.1080–X.1099 |
| 安全应用和服务 | |
| 组播安全 | X.1100–X.1109 |
| 家庭网络安全 | X.1110–X.1119 |
| 移动安全 | X.1120–X.1139 |
| 网页安全 | X.1140–X.1149 |
| 安全协议 | X.1150–X.1159 |
| 对等网络安全 | X.1160–X.1169 |
| 网络身份安全 | X.1170–X.1179 |
| IPTV安全 | X.1180–X.1199 |
| 网络空间安全 | |
| 计算网络安全 | X.1200–X.1229 |
| 反垃圾信息 | X.1230–X.1249 |
| 身份管理 | X.1250–X.1279 |
| 安全应用和服务 | |
| 应急通信 | X.1300–X.1309 |
| 泛在传感器网络安全 | X.1310–X.1339 |
| 网络安全信息交换 | |
| 网络安全概述 | X.1500–X.1519 |
| 脆弱性/状态信息交换 | X.1520–X.1539 |
| 事件/事故/探索法交换 | X.1540–X.1549 |
| 政策的交换 | X.1550–X.1559 |
| 探索法和信息请求 | X.1560–X.1569 |
| 标识和发现 | X.1570–X.1579 |
| 确保交换 | X.1580–X.1589 |

欲了解更详细信息，请查阅 ITU-T 建议书目录。

ITU-T X.1541 建议书

事件对象描述交换格式

摘要

ITU-T X.1541建议书阐述了事件对象描述交换格式（IODEF）的信息模型，并提供了一种以XML模式表示的相关数据模型。IODEF具体介绍了共享普遍交换计算机安全或其它事件类型信息的数据模型。这是通过列出IETFREC 5070 的相关段落和说明它们属于规范性还是情况通报性实现的。

沿革

| 版本 | 建议书 | 批准日期 | 研究组 |
|-----|--------------|------------|-----|
| 1.0 | ITU-T X.1541 | 2012-09-07 | 17 |

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：<http://www.itu.int/ITU-T/ipr/>。

© 国际电联 2013

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

| | 页码 |
|---------------------|----|
| 1 范围 | 1 |
| 2 参考文献 | 1 |
| 3 定义 | 1 |
| 3.1 他处定义的术语 | 1 |
| 3.2 本建议书定义的术语 | 1 |
| 4 缩写词和首字母缩略语 | 1 |
| 5 惯例 | 2 |
| 6 事件对象描述交换格式 | 2 |
| 6.1 引言 | 2 |
| 6.2 IODEF数据类型 | 2 |
| 6.3 IODEF数据模型 | 3 |
| 6.4 处理注意事项 | 6 |
| 6.5 扩展IODEF | 6 |
| 6.6 国际化问题 | 6 |
| 6.7 示例 | 7 |
| 6.8 IODEF模式 | 7 |
| 6.9 安全性方面的考虑 | 7 |
| 6.10 IANA的考虑 | 7 |
| 6.11 致谢 | 7 |
| 6.12 参考文献 | 7 |
| 参考资料..... | 8 |

引言

ITU-T X.1500建议书“网络安全交换概述”，为通过本建议书提供的同类包括事件和指标的网络安全交换提供了指导。安全事件对象描述交换格式（**IODEF**）是一种用于描述计算机安全信息的数据模型，规定了一种**XML**数据模型表示法，用于在相关部门中肩负着发起主动防御、矫正修复或监测预警等操作责任的当事方之间传递安全事件信息。该数据模型提供了一种对以下信息进行编码的方法：主机、网络以及在这些系统上运行的服务；利用方法和相关数据；事件影响；以及记录工作流程的有限方法。

IODEF的首要目的是增强**CSIRT**的工作能力和态势感知能力。**IODEF**的普遍采纳有助于简化协作和信息共享，进而能够改进解决事件的能力和传递有关威胁态势意识的的能力。这种**IODEF**的结构化格式可以：

- 通过交换结构性事件信息，提高处理事件信息的自动化程度，无需安全分析人员再对自由形式的文本文件进行分析；
- 减少在来自不同来源的类似数据（即使具有高度结构性）之间建立关联的工作量，从而增强态势感知；以及
- 提供一个通用格式，使事件处理工具和分析工具具有互操作性，当数据来自多个实体时其意义尤为重要。

众多程序、信任、政策和法律方面的因素可能会限制或阻止**CSIRT**或**SP**共享信息。**IODEF**只是一套技术规范，并不试图解决这些问题。不过，在订立信息共享协议时，从操作层面实施**IODEF**以及相关的格式和协议则应从范畴更广的角度考虑上述问题。

事件对象描述交换格式

1 范围

事件对象描述交换格式（IODEF）规定了一种数据模型表示法，可用于共享通常交换的有关计算机安全或其它类型事件的信息。本建议书描述了IODEF的信息模型，并提供了用XML模式（Schema）表示的相关数据模型。

任何能够实现计算机安全信息或其它类型事件信息共享的数据模型表示法或框架必须符合一切适用的国家及区域性法律、法规和政策。

包括本建议书在内的所有ITU-T建议书及其基础技术的实施者和用户，须遵循一切适用的国家及区域性法律、法规和政策。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时注明的版本为有效版本。所有的建议书和其它参考文献均会得到修订，本建议书的使用者应查证是否有可能使用下列建议书或其它参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

[IETF RFC 5070] IETF RFC 5070 (2007), 事件对象描述交换格式。
<<http://datatracker.ietf.org/doc/rfc5070/>>

3 定义

3.1 他处定义的术语

无。

3.2 本建议书定义的术语

无。

4 缩写词和首字母缩略语

本建议书使用以下缩写词和首字母缩略语：

| | |
|-------|-------------|
| IANA | 互联网域名分配管理机构 |
| IODEF | 事件对象描述交换格式 |

5 惯例

下列术语被视为彼此等同：

- 在国际电联，“shall”和“must”在使用时彼此等同，其反义表达亦视为彼此等同。
- 国际电联使用的“shall”一词与IETF使用的“MUST”一词等同。
- 国际电联使用的“shall not”短语与IETF使用的“MUST NOT”短语等同。

注 – 在IETF，“shall”和“must”（小写）两词用于资料性文本。

6 事件对象描述交换格式

第6条定义了事件对象描述交换格式（IODEF）。该条直接引用了[IETF RFC 5070]，并为此将有关条文与章节编号保持一致，如此第6.x条便与[IETF RFC 5070]第x节保持一致，且标题彼此匹配。

注 – 对[b-IETF RFC 5070]的勘误表见[b-Errata ID3333]。

6.1 引言

[b-IETF RFC 5070]第1节为资料性文本。

6.1.1 术语

[b-IETF RFC 5070]第1.1节为资料性文本。

6.1.2 符号

[b-IETF RFC 5070]第1.2节为资料性文本。

6.1.3 关于IODEF数据模型

[b-IETF RFC 5070]第1.3节为资料性文本。

6.1.4 关于IODEF的实施

[b-IETF RFC 5070]第1.4节为资料性文本。

6.2 IODEF数据类型

[b-IETF RFC 5070]第2节为资料性文本。

6.2.1 整数

[IETF RFC 5070]第2.1节为规范性文本。

6.2.2 实数

[IETF RFC 5070]第2.2节为规范性文本。

6.2.3 字符和字符串

[IETF RFC 5070]第2.3节为规范性文本。

6.2.4 多语言字符串

[IETF RFC 5070]第2.4节为规范性文本。

6.2.5 字节

[IETF RFC 5070]第2.5节为规范性文本。

6.2.6 十六进制字节

[IETF RFC 5070]第2.6节为规范性文本。

6.2.7 枚举类型

[IETF RFC 5070]第2.7节为规范性文本。

6.2.8 日期-时间字符串

[IETF RFC 5070]第2.8节为规范性文本。

6.2.9 时区字符串

[IETF RFC 5070]第2.9节为规范性文本。

6.2.10 端口列表

[IETF RFC 5070]第2.10节为规范性文本。

6.2.11 邮政地址

[IETF RFC 5070]第2.11节为规范性文本。

6.2.12 人或机构

[IETF RFC 5070]第2.12节为规范性文本。

6.2.13 电话和传真号码

[IETF RFC 5070]第2.13节为规范性文本。

6.2.14 电子邮件字符串

[IETF RFC 5070]第2.14节为规范性文本。

6.2.15 统一资源定位器字符串

[IETF RFC 5070]第2.15节为规范性文本。

6.3 IODEF数据模型

[b-IETF RFC 5070]第3节为资料性文本。

6.3.1 IODEF-文档类

[IETF RFC 5070]第3.1节为规范性文本。

6.3.2 安全事件类

[IETF RFC 5070]第3.2节为规范性文本。

6.3.3 安全事件ID类

[IETF RFC 5070]第3.3节为规范性文本。

6.3.4 备选ID类

[IETF RFC 5070]第3.4节为规范性文本。

6.3.5 相关活动类

[IETF RFC 5070]第3.5节为规范性文本。

6.3.6 附加数据类

[IETF RFC 5070]第3.6节为规范性文本。

6.3.7 联系人类

[IETF RFC 5070]第3.7节为规范性文本。

6.3.7.1 登记机构代码类

[IETF RFC 5070]第3.7.1节为规范性文本。

6.3.7.2 邮政地址类

[IETF RFC 5070]第3.7.2节为规范性文本。

6.3.7.3 电子邮件类

[IETF RFC 5070]第3.7.3节为规范性文本。

6.3.7.4 电话和传真类

[IETF RFC 5070]第3.7.4节为规范性文本。

6.3.8 时间类

[IETF RFC 5070]第3.8节为规范性文本。

6.3.8.1 开始时间

[IETF RFC 5070]第3.8.1节为规范性文本。

6.3.8.2 结束时间

[IETF RFC 5070]第3.8.2节为规范性文本。

6.3.8.3 检测时间

[IETF RFC 5070]第3.8.3节为规范性文本。

6.3.8.4 报告时间

[IETF RFC 5070]第3.8.4节为规范性文本。

6.3.8.5 日期时间

[IETF RFC 5070]第3.8.5节为规范性文本。

6.3.9 方法类

[IETF RFC 5070]第3.9节为规范性文本。

6.3.9.1 参考类

[IETF RFC 5070]第3.9.1节为规范性文本。

6.3.10 评估类

[IETF RFC 5070]第3.10节为规范性文本。

6.3.10.1 影响类

[IETF RFC 5070]第3.10.1节为规范性文本。

6.3.10.2 时间影响类

[IETF RFC 5070]第3.10.2节为规范性文本。

6.3.10.3 货币影响类

[IETF RFC 5070]第3.10.3节为规范性文本。

6.3.10.4 信心类

[IETF RFC 5070]第3.10.4节为规范性文本。

6.3.11 历史类

[IETF RFC 5070]第3.11节为规范性文本。

6.3.11.1 历史项目类

[IETF RFC 5070]第3.11.1节为规范性文本。

6.3.12 事件数据类

[IETF RFC 5070]第3.12节为规范性文本。

6.3.12.1 在事件和时间数据类之间建立相关

[IETF RFC 5070]第3.12.1节为规范性文本。

6.3.12.2 事件数据的基数

[IETF RFC 5070]第3.12.2节为规范性文本。

6.3.13 期望类

[IETF RFC 5070]第3.13节为规范性文本。

6.3.14 流类

[IETF RFC 5070]第3.14节为规范性文本。

6.3.15 系统类

[IETF RFC 5070]第3.15节为规范性文本。

6.3.16 节点类

[IETF RFC 5070]第3.16节为规范性文本。

6.3.16.1 计数器类

[IETF RFC 5070]第3.16.1节为规范性文本。

6.3.16.2 地址类

[IETF RFC 5070]第3.16.2节为规范性文本。

6.3.16.3 节点作用类

[IETF RFC 5070]第3.16.3节为规范性文本。

6.3.17 服务类

[IETF RFC 5070]第3.17节为规范性文本。

6.3.17.1 应用类

[IETF RFC 5070]第3.17.1节为规范性文本。

6.3.18 操作系统类

[IETF RFC 5070]第3.18节为规范性文本。

6.3.19 记录类

[IETF RFC 5070]第3.19节为规范性文本。

6.3.19.1 记录数据类

[IETF RFC 5070]第3.19.1节为规范性文本。

6.3.19.2 记录模式类

[IETF RFC 5070]第3.19.2节为规范性文本。

6.3.19.3 记录项目类

[IETF RFC 5070]第3.19.3节为规范性文本。

6.4 处理注意事项

[b-IETF RFC 5070]第4节为资料性文本。

6.4.1 编码

[IETF RFC 5070]第4.1节为规范性文本。

6.4.2 IODEF命名空间

[IETF RFC 5070]第4.2节为规范性文本。

6.4.3 验证

[IETF RFC 5070]第4.3节为规范性文本。

6.5 扩展IODEF

[b-IETF RFC 5070]第5节为资料性文本。

ITU-T X.1500建议书“网络安全交换概述”，为通过本建议书提供的同类包括事件和指标的网络安全交换提供了指导。根据ITU-T X.1500建议书，本建议书为时间信息交换提供了基础格式，但并未涉及所有用户案例。可能需要开发涉及必要用户案例的扩展。

6.5.1 扩展属性的枚举值

[IETF RFC 5070]第5.1节为规范性文本。

6.5.2 扩展类

[IETF RFC 5070]第5.2节为规范性文本。

6.6 国际化问题

[IETF RFC 5070]第6节为规范性文本。

6.7 示例

[b-IETF RFC 5070]第7节为资料性文本。

6.7.1 蠕虫

[b-IETF RFC 5070]第7.1节为资料性文本。

6.7.2 侦察

[b-IETF RFC 5070]第7.2节为资料性文本。

6.7.3 僵尸网报告

[b-IETF RFC 5070]第7.3节为资料性文本。

6.7.4 监测名单

[b-IETF RFC 5070]第7.4节为资料性文本。

6.8 IODEF模式

[IETF RFC 5070]第8节为规范性文本。

6.9 安全性方面的考虑

[IETF RFC 5070]第9节为规范性文本。

在按照ITU-T的要求实施该内容时，用于交换IODEF实例的基本消息格式和协议须适当保障机密性、完整性和真实性。

注 – 在IETF，“must”（小写）一词用于资料性文本。

6.10 IANA的考虑

[IETF RFC 5070]第10节为规范性文本。

6.11 致谢

[b-IETF RFC 5070]第11节为资料性文本。

6.12 参考文献

6.12.1 规范性参考文献

[b-IETF RFC 5070]第12.1节为资料性文本。

本ITU-T建议书已明确指出，[IETF RFC 5070]第12节属于资料性内容，原因在于ITU-T并未确定本建议书中任何参考文献的性质。但IETF已经为[IETF RFC 5070]明确了一系列规则性参考文献。

6.12.2 资料性参考文献

[b-IETF RFC 5070]第12.2节为资料性文本。

参考资料

- [b-ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange*.
- [b-Errata ID3333] IETF RFC Errata ID: 3333, *IETF RFC5070, "The Incident Object Description Exchange Format", December 2007; Status: Held for Document Update; Type: Editorial; Date Reported: 2012-09-02.* <http://www.rfc-editor.org/errata_search.php?eid=3333>
- [b-IETF RFC 5070] IETF RFC 5070 (2007), *The Incident Object Description Exchange Format (IODEF)*. <[https://datatracker.ietf.org/doc/RFC 5070/](https://datatracker.ietf.org/doc/RFC%205070/)>

ITU-T 系列建议书

| | |
|------------|-------------------------|
| A系列 | ITU-T工作的组织 |
| D系列 | 一般资费原则 |
| E系列 | 综合网络运行、电话业务、业务运行和人为因素 |
| F系列 | 非话电信业务 |
| G系列 | 传输系统和媒质、数字系统和网络 |
| H系列 | 视听及多媒体系统 |
| I系列 | 综合业务数字网 |
| J系列 | 有线网络和电视、声音节目及其它多媒体信号的传输 |
| K系列 | 干扰的防护 |
| L系列 | 电缆和外部设备其它组件的结构、安装和保护 |
| M系列 | 电信管理，包括TMN和网络维护 |
| N系列 | 维护：国际声音节目和电视传输电路 |
| O系列 | 测量设备的技术规范 |
| P系列 | 电话传输质量、电话设施及本地线路网络 |
| Q系列 | 交换和信令 |
| R系列 | 电报传输 |
| S系列 | 电报业务终端设备 |
| T系列 | 远程信息处理业务的终端设备 |
| U系列 | 电报交换 |
| V系列 | 电话网上的数据通信 |
| X系列 | 数据网、开放系统通信和安全性 |
| Y系列 | 全球信息基础设施、互联网协议问题和下一代网络 |
| Z系列 | 用于电信系统的语言和一般软件问题 |