国 际 电 信 联 盟

ITU-T X.1541

(09/2017)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

网络安全信息交换 – 活动/事件/探索法交换

事件对象描述交换格式版本2

ITU-T X.1541 建议书

国际电信联盟

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（1）	
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
万维网安全	X.1140–X.1149
安全协议（1）	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	
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（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1360–X.1369
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
安全协议（2）	X.1450–X.1459
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
活动/事件/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
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳实践和指南	X.1640–X.1659
云计算安全实施	X.1660–X.1679
其他云计算安全	X.1680–X.1699

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-TX.1541 建议书

事件对象描述交换格式版本2

摘要

ITU-T X.1541建议书阐述了事件对象描述交换格式（IODEF）版本2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 7970的相关段落和说明它们属于规范性还是资料性实现的。

沿革

版本	建议书	批准日期	研究组	唯一标识符*
1.0	ITU-T X.1541	2012-09-07	17	11.1002/1000/11375
2.0	ITU-T X.1541	2017-09-06	17	11.1002/1000/13264

* 要访问该建议书，请在万维网浏览器的地址栏中输入URL：http://handle.itu.int/，然后输入建议书的唯一标识符。例如，http://handle.itu.int/11.1002/1000/11830-en。

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/。

目录

引言

ITU-T X.1500建议书“网络安全信息交换概述”，为通过本建议书提供的、包括事件和指标的网络安全信息交换提供了指导。事件对象描述交换格式（IODEF）是一种用于描述计算机安全通常交换信息的数据模型，规定了一种XML数据模型表示法，用于在肩负着发起主动防御、矫正修复或监测预警等运营责任的当事方之间传递事件信息。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；

– 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信息交换。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。

ITU-T X.1541 建议书

事件对象描述交换格式版本2

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模式表示的相关数据模型。

一种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 7970] IETF RFC 7970 (2016), *The Incident Object Description Exchange Format Version 2*.
<https://datatracker.ietf.org/doc/rfc7970/>

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）版本2，它直接引用了[IETF RFC 7970]的章节，并为此将有关条文与章节编号保持一致。因而，例如，第6.x条与[IETF RFC 7970]第x节保持了一致，且标题彼此匹配。

6.1 引言

[IETF RFC 7970]第1节为资料性文本。

6.1.1 术语

[IETF RFC 7970]第1.1节为资料性文本。

6.1.2 记法

[IETF RFC 7970]第1.2节为资料性文本。

6.1.3 关于IODEF数据模型

[IETF RFC 7970]第1.3节为资料性文本。

6.1.4 变自RFC 5070

[IETF RFC 7970]第1.4节为资料性文本。

6.2 IODEF数据类型

[IETF RFC 7970]第2节为资料性文本，但其子章节，例如，第2.1-2.15节为规范性文本。它们定义了以下数据类型：

- 整数（[IETF RFC 7970]第2.1节定义之）
- 实数（[IETF RFC 7970]第2.2节定义之）
- 字符和字符串（[IETF RFC 7970]第2.3节定义之）
- 多语言字符串（[IETF RFC 7970]第2.4节定义之）
- 二进制字符串（[IETF RFC 7970]第2.5节定义之）
  - Base64字节（[IETF RFC 7970]第2.5.1节定义之）
  - 十六进制字节（[IETF RFC 7970]第2.5.2节定义之）
- 枚举类型（[IETF RFC 7970]第2.6节定义之）
- 日期-时间字符串（[IETF RFC 7970]第2.7节定义之）
- 时区字符串（[IETF RFC 7970]第2.8节定义之）
- 端口列表（[IETF RFC 7970]第2.9节定义之）
- 邮政地址（[IETF RFC 7970]第2.10节定义之）
- 电话号码（[IETF RFC 7970]第2.11节定义之）
- 电子邮件字符串（[IETF RFC 7970]第2.12节定义之）
- 统一资源定位器字符串（[IETF RFC 7970]第2.13节定义之）
- 标识符和标识符参考（[IETF RFC 7970]第2.14节定义之）

– 软件（[IETF RFC 7970]第2.15节定义之）
  – SoftwareReference类（[IETF RFC 7970]第2.15.1节定义之）
– 扩展（[IETF RFC 7970]第2.16节定义之）

6.3 IODEF信息模型

[IETF RFC 7970]第3节为资料性文本，但其子章节，例如，第3.1-3.29节为规范性文本。它们定义了以下数据类型：

– IODEF-文档类（[IETF RFC 7970]第3.1节定义之）
– 事件类（[IETF RFC 7970]第3.2节定义之）
– 公共属性（[IETF RFC 7970]第3.3节定义之）
  – 限制属性（[IETF RFC 7970]第3.3.1节定义之）
  – 可观测ID属性（[IETF RFC 7970]第3.3.2节定义之）
– 事件ID类（[IETF RFC 7970]第3.4节定义之）
– 备选ID类（[IETF RFC 7970]第3.5节定义之）
– 相关活动类（[IETF RFC 7970]第3.6节定义之）
– 威胁实施者类（[IETF RFC 7970]第3.7节定义之）
– 活动类（[IETF RFC 7970]第3.8节定义之）
– 联系人类（[IETF RFC 7970]第3.9节定义之）
  – 登记机构代码类（[IETF RFC 7970]第3.9.1节定义之）
  – 邮政地址类（[IETF RFC 7970]第3.9.2节定义之）
  – 电子邮件类（[IETF RFC 7970]第3.9.3节定义之）
  – 电话类（[IETF RFC 7970]第3.9.4节定义之）
– 探索类（[IETF RFC 7970]第3.10节定义之）
  – 检测样式类[IETF RFC 7970]第3.10.1节定义之）
– 方法类（[IETF RFC 7970]第3.11节定义之）
  – 参考类（[IETF RFC 7970]第3.11.1节定义之）
– 评估类（[IETF RFC 7970]第3.12节定义之）
  – 系统影响类（[IETF RFC 7970]第3.12.1节定义之）
  – 业务影响类（[IETF RFC 7970]第3.12.2节定义之）
  – 时间影响类（[IETF RFC 7970]第3.12.3节定义之）
  – 系统影响类（[IETF RFC 7970]第3.12.4节定义之）
  – 信任类（[IETF RFC 7970]第3.12.5节定义之）
– 历史类（[IETF RFC 7970]第3.13节定义之）
  – 历史项目类（[IETF RFC 7970]第3.13.1节定义之）
– 活动数据类（[IETF RFC 7970]第3.14节定义之）
  – 相关事件和活动数据类（[IETF RFC 7970]第3.14.1节定义之）
  – 递归定义活动数据（[IETF RFC 7970]第3.14.2节定义之）
– 期望类（[IETF RFC 7970]第3.15节定义之）
– 流类（[IETF RFC 7970]第3.16节定义之）
– 系统类（[IETF RFC 7970]第3.17节定义之）
– 节点类（[IETF RFC 7970]第3.18节定义之）
  – 地址类（[IETF RFC 7970]第3.18.1节定义之）

  - 节点作用类（[IETF RFC 7970]第3.18.2节定义之）
  - 计数器类（[IETF RFC 7970]第3.18.3节定义之）
- 域数据类（[IETF RFC 7970]第3.19节定义之）
  - 名称服务器类（[IETF RFC 7970]第3.19.1节定义之）
  - 域联系人类（[IETF RFC 7970]第3.19.2节定义之）
- 业务类（[IETF RFC 7970]第3.20节定义之）
  - 业务名称类（[IETF RFC 7970]第3.20.1节定义之）
  - 应用报头类（[IETF RFC 7970]第3.20.2节定义之）
- 电子邮件数据类（[IETF RFC 7970]第3.21节定义之）
- 记录类（[IETF RFC 7970]第3.22节定义之）
  - 记录数据类（[IETF RFC 7970]第3.22.1节定义之）
  - 记录样式类（[IETF RFC 7970]第3.22.2节定义之）
- 更改的Windows注册密钥类（[IETF RFC 7970]第3.23节定义之）
  - 密钥类（[IETF RFC 7970]第3.23.1节定义之）
- 认证数据类（[IETF RFC 7970]第3.24节定义之）
  - 认证类（[IETF RFC 7970]第3.24.1节定义之）
- 文件数据类（[IETF RFC 7970]第3.25节定义之）
  - 文件类（[IETF RFC 7970]第3.25.1节定义之）
- 散列数据类（[IETF RFC 7970]第3.26节定义之）
  - 散列类（[IETF RFC 7970]第3.26.1节定义之）
  - 模糊散列类（[IETF RFC 7970]第3.26.2节定义之）
- 签名数据类（[IETF RFC 7970]第3.27节定义之）
- 指标数据类（[IETF RFC 7970]第3.28节定义之）
- 指标类（[IETF RFC 7970]第3.29节定义之）
  - 指标ID类（[IETF RFC 7970]第3.29.1节定义之）
  - 备选指标ID类（[IETF RFC 7970]第3.29.2节定义之）
  - 可观测的类（[IETF RFC 7970]第3.29.3节定义之）
  - 指标表示类（[IETF RFC 7970]第3.29.4节定义之）
  - 带指标表示的表达式（[IETF RFC 7970]第3.29.5节定义之）
  - 可观测的参考类（[IETF RFC 7970]第3.29.6节定义之）
  - 指标参考类（[IETF RFC 7970]第3.29.7节定义之）
  - 攻击阶段类（[IETF RFC 7970]第3.29.8节定义之）

6.4 处理方面的考虑

尽管其部分子章节为资料性文本，但[IETF RFC 7970]第4节为规范性文本，如以下子章节所述：

6.4.1 编码

[IETF RFC 7970]第4.1节为规范性文本。

6.4.2 IODEF命名空间

[IETF RFC 7970]第4.2节为规范性文本。

6.4.3 验证

[IETF RFC 7970]第4.3节为规范性文本。

6.4.4 与版本1的不兼容性

[IETF RFC 7970]第4.4节为资料性文本。

6.5 扩展IODEF

[IETF RFC 7970]第5节为资料性文本。

[b-ITU-T X.1500]建议书“网络安全信息交换概述”，为通过本建议书（ITU-T X.1541）提供的、包括事件和指标的网络安全信息交换提供了指导。根据[b-ITU-T X.1500]建议书，本建议书（ITU-T X.1541）为事件信息交换提供了基础格式，但并未涉及所有使用案例。可能需要开发涉及必要使用案例的扩展。

6.5.1 扩展属性的枚举值

[IETF RFC 7970]第5.1节及其子章节为规范性文本。

6.5.2 扩展类

[IETF RFC 7970]第5.2节及其子章节为规范性文本。

6.6 国际化问题

[IETF RFC 7970]第6节为规范性文本。

6.7 示例

[IETF RFC 7970]第7节及其子章节为资料性文本，用于描述IODEF示例文档。

6.8 IODEF数据模型（XML模式）

[IETF RFC 7970]第8节为规范性文本。

6.9 安全性方面的考虑

[IETF RFC 7970]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证机密性、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方面的考虑

[IETF RFC 7970]第10节为规范性文本。

6.11 参考文献

6.11.1 规范性参考文献

[IETF RFC 7970]第11.1节为资料性文本。

本ITU-T建议书已明确指出，[IETF RFC 7970]第11.1节属于资料性文本，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 7970]明确了一系列规范性参考文献。

6.11.2 资料性参考文献

[IETF RFC 7970]第11.2节为资料性文本。

参考资料

[b-ITU-T X.1500] ITU-T X.1500（2011年）建议书，网络安全信息交换概述。

ITU-T系列建议书

A系列	ITU-T工作的组织
D系列	资费和结算原则及国际电信/ICT的经济和政策问题
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	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、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	交换和信令及相关的测量和测试
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、下一代网络、物联网和智慧城市
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2018年，日内瓦