ICS 35.020
L 09

中华人民共和国国家标准

GB/T 28517—2012

网络安全事件描述和交换格式

Network incident object description and exchange format

2012-06-29 发布　　2012-10-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准是主要参照 IETF(互联网工程任务组)RFC 5070,结合我国计算机网络应急响应体系建设的实际情况而制定的。

本标准由中华人民共和国工业和信息化部提出。

本标准由中国通信标准化协会归口。

本标准起草单位:国家计算机网络应急技术处理协调中心、清华大学。

本标准主要起草人:黄元飞、袁春阳、段海新、孙蔚敏、杨臻、周勇林、焦绪录、纪玉春、梁晟、吴俊华、孙彬。

引　言

随着互联网的发展，计算机网络安全事件突破了国家或地区的边界，跨越多个组织，各应急响应组织间的合作也突破了国界、语言和文化的约束。在此背景下，我国特成立了国家计算机网络应急技术处理协调中心（CNCERT/CC），负责协调国内各计算机安全应急响应组共同处理国家公共互联网上的安全事件；相关电信运营企业、安全服务商、国有大型公司、教育科研机构以及国家有关部门也逐步成立了计算机安全应急响应组（简称应急响应组或 CSIRT）。为了提高各应急响应组对安全事件的响应能力和预防能力，规范我国各应急响应组之间安全事件的描述和交换格式，特制定本标准（IODEF）。

IODEF 主要用于各应急响应组的事件处理系统（IHS）之间信息交换，是一种表示层的通信协议，其应用环境如图 1 所示。

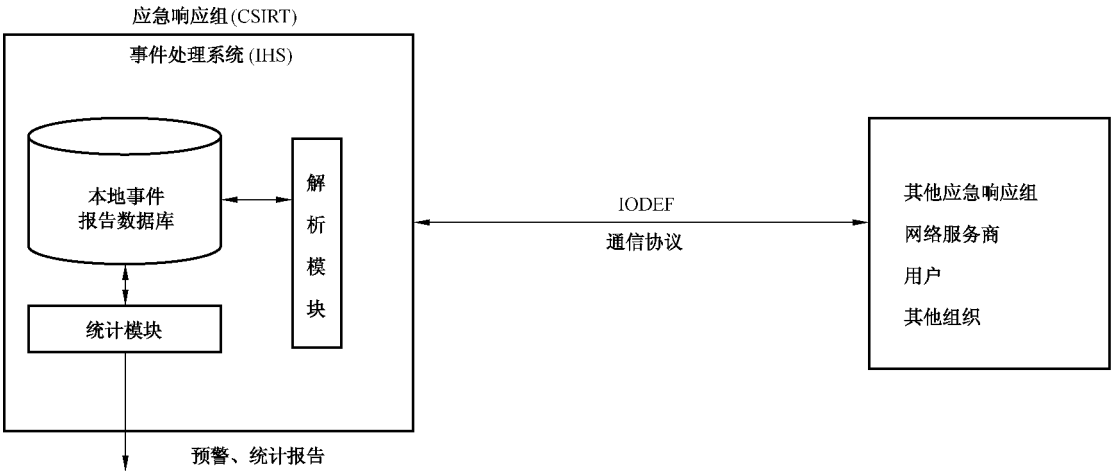

图 1　安全事件描述交换格式的应用环境

一般情况下，应急响应组需要某种软件工具把安全事件相关的信息生成 IODEF 的事件报告，然后通过通信协议（如 HTTP、SMTP 等）发送给其他相关的组织；当 CSIRT 收到其他 CSIRT、网络服务商、用户或其他组织发送过来的 IODEF 文档时，一般需要经过事件处理系统中的 IODEF 解析模块或独立的 IODEF 解析程序生成符合 CSIRT 内部定义的数据格式，然后保存到本地事件报告数据库中，并进入事件处理的流程。

网络安全事件描述和交换格式

1 范围

本标准规定了一种描述计算机网络安全事件的通用数据格式，以便于计算机安全应急响应组间进行网络安全事件交换，并提供了 XML 的参考实现。

本标准适用于计算机安全应急响应组间进行计算机网络安全事件交换，也可供建设和维护计算机网络安全事件处理系统时参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)使用于本文件。

GB/T 12406—2008 表示货币和资金的代码(ISO 4217:2001，IDT)

IETF RFC 1305 网络时间协议规范和执行(Network Time Protocol(Version 3)Specification，Implementation)

IETF RFC 2030 对于 IPv4、IPv6 和 OSI 的简单网络定时协议第 4 版(Simple Network Time Protocol(SNTP)Version 4 for IPv4，IPv6 and OSI)

IETF RFC 2256 对于使用 LADPv3 的 X.500 使用者计划的概述(A Summary of the X.500(96) User Schema for use with LDAPv3)

IETF RFC 2396 统一资源标识符(URI)：一般句法(Uniform Resource Identifiers(URI)：Generic Syntax)

IETF RFC 2822 英特网信息格式(Internet Message Format)

3 术语和定义、缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

攻击 attack

对系统安全的袭击，主要来源于人为的、技术上的威胁。例如，企图逃避安全服务和违背系统安全策略的一次技术上的攻击行为。

攻击可能是主动的，也可能是被动的；可能是来自内部人员，也可能是来自外部人员。

3.1.2

攻击者 attacker

为达到某种(些)目的而尝试一次或多次攻击的个体。在本标准中，攻击者由其网络标识、发起网络或计算机攻击的组织以及物理位置信息(可选)来描述。

3.1.3

计算机安全应急响应组 computer security incident response team；CSIRT

处理计算机网络安全事件和创建安全事件报告的组织。CSIRT 也可能涉及证据的收集和保管、安