ICS 35.040
L 80

中华人民共和国国家标准

GB/T 28454—2012

信息技术　安全技术
入侵检测系统的选择、部署和操作

Information technology—Security techniques—
Selection, deployment and operations of intrusion detection systems

(ISO/IEC 18043:2006, MOD)

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。

本标准修改采用 ISO/IEC 18043:2006《信息安全　安全技术　入侵检测系统的选择、部署和操作》,除编辑性修改外主要变化如下:

a) 修改附录 A.6、A.7 和 A.8 中不符合常用规范的标准章条编号;

b) 术语部分:当 ISO/IEC 18043 中的术语与定义与 GB/T 25069—2010《信息安全技术　术语》表达含义相同,但描述略有不同时,采纳 GB/T 25069—2010《信息安全技术　术语》中的定义,包括:攻击、拒绝服务攻击、非军事区、入侵、路由器、交换机、特洛伊木马等;

c) 标准结构:较原标准文本相比,增加了第 2 章“规范性引用文件”和第 4 章“缩略语”。

d) 标准 7.2 中增加了“当组织对 IDS 产品有安全等级方面的要求时,见 GB/T 20275”。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:山东省标准化研究院、山东省计算中心、中国电子技术标准化研究所、济宁市质量技术监督信息所。

本标准主要起草人:王曙光、董火民、曲发川、朱瑞虹、周鸣乐、李刚、王运福、许玉娜、罗翔、周洋、胡鑫磊、孙大勇、郑伟、林华、戴雯。

引　言

有部署入侵检测系统需求的组织在选择和部署入侵检测系统之前，不仅宜知道其网络、系统或者应用的入侵什么时间发生、是否会发生以及如何发生，也宜知道入侵利用了什么样的脆弱性，以及为了预防类似的入侵，未来宜实施什么防护措施和适当的风险处理手段（即风险转移、风险接受、风险规避）。组织也宜识别并避免基于计算机的入侵。在20世纪中期，组织开始使用入侵检测系统来满足这些需求。随着一系列IDS产品的出现，IDS的应用不断扩大，以满足组织对先进入侵检测能力的需求级别。

为了从IDS得到最大的效益，宜由经过培训、经验丰富的人员谨慎策划和实施选择、部署和操作IDS的过程。当过程实现时，IDS产品能帮助组织获得入侵信息，并能在整个信息和通信技术基础设施中担当重要安全设施的角色。

本标准提供了有效选择、部署和操作IDS的指南，以及IDS的基础知识。同时适用于考虑外包其入侵检测能力的组织。外包服务级别协议的信息可在基于GB/T 24405的IT服务管理过程中找到。

信息技术　安全技术
入侵检测系统的选择、部署和操作

1　范围

本标准给出了帮助组织准备部署 IDS 的指南。特别是，详细说明了 IDS 的选择、部署和操作。同时给出了这些指导方针来源的背景信息。

注：IDS 的部署宜定位在网络节点和边界，最多到系统边界，不宜深入到信息系统内部或监控系统内资源。

本标准的目的是帮助组织：

a）　满足 GB/T 22080—2008 的下列要求：

- 组织应实施能提升检测和响应安全事件能力的程序和其他控制措施；
- 组织应执行监视和评审程序和其他控制措施，以识别潜在的或已经存在的安全漏洞和事件。

b）　在实施控制措施方面，满足 GB/T 22081—2008 的下列安全目标：

- 检测未授权的信息处理活动；
- 宜监视系统并记录信息安全事件；操作日志和故障日志宜用来确保识别信息系统问题；
- 组织宜遵守所有用于监视和记录日志活动的相关法律要求；
- 监视系统宜用于检查所采取控制措施的有效性，并验证访问控制方针模型的符合性。

组织宜认识到对满足上述要求来说，IDS 部署不是唯一的或完善的解决方案。此外，本标准期望作为合格评定的准则，例如信息安全管理体系（ISMS）认证、IDS 服务或产品认证。

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）适用于本文件。

GB/T 18336（所有部分）　信息技术　安全技术　信息技术安全性评估准则[ISO/IEC 15408（所有部分）]

GB/T 20275　信息安全技术　入侵检测系统技术要求和测试评价方法

GB/Z 20985—2007　信息技术　安全技术　信息安全事件管理指南（ISO/IEC TR 18044：2004，MOD）

GB/T 22080—2008　信息技术　安全技术　信息安全管理体系 要求（ISO/IEC 27001：2005，IDT）

GB/T 22081—2008　信息技术　安全技术　信息安全管理实用规则（ISO/IEC 27002：2005，IDT）

GB/T 25068.1—2012　信息技术　安全技术　IT 网络安全　第 1 部分：网络安全管理（ISO/IEC 18028-1：2006，IDT）

GB/T 25068.2—2012　信息技术　安全技术　IT 网络安全　第 2 部分：网络安全体系结构（ISO/IEC 18028-2：2005，IDT）

3　术语和定义

下列术语和定义适用于本文件。