ICS 35.040
L 80

# 中华人民共和国国家标准

GB/T 28454—2020
代替 GB/T 28454—2012

# 信息技术　安全技术　入侵检测和防御系统（IDPS）的选择、部署和操作

**Information technology—Security techniques—Selection, deployment and operation of intrusion detection and prevention systems (IDPS)**

(ISO/IEC 27039:2015,MOD)

2020-04-28 发布　　2020-11-01 实施

国家市场监督管理总局
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。

本标准代替 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》。与 GB/T 28454—2012 相比，主要技术变化如下：

——修改了入侵检测系统 IDS 为入侵检测和防御系统(IDPS)，将入侵防御系统 IPS 纳入标准范围；

——修改了标准范围，增加标准适用对象(见第 1 章，2012 年版的第 1 章)；

——修改了部分术语和定义，包括“攻击”“拒绝服务攻击”“非军事区”“入侵者”“入侵”“路由器”“交换机”“特洛伊木马”“攻击特征”“防火墙”“主机”“入侵检测系统”“入侵防御系统”“在线升级”“探测器”“测试接入点”，增加了部分术语和定义，包括“分布式拒绝服务攻击”“入侵检测和防御系统”“病毒”“虚拟专用网”“脆弱性”(见第 3 章，2012 年版的第3 章)；

——增加了部分缩略语，包括 AIDPS、DMZ、DDoS、DoS、IDPS、I/O、IODEF、HIDPS、SIEM、VPN，删除缩略语 NIDS、SIM(见第 4 章，2012 年版的第 4 章)；

——删除背景中关于 IDPS 基础知识的介绍(见第 5 章，2012 年版的第 5 章)；

——因增加入侵防御系统，修改“当组织对 IDS 产品有安全等级方面的要求时，见 GB/T 20275”为“当对 IDPS 产品有安全等级方面的要求时，见 GB/T 20275 和 GB/T 28451。”(见 7.3.1，2012 年版的 7.2)；

——增加云计算环境中 IDPS 选择考虑事项(见 7.4.1、7.4.2、7.4.3、7.4.5)和云环境下 IDPS 部署方式、多层级组织中 IDPS 部署方式等(见 8.1)；

——“能力的确认”修改为“能力的验证”(见 7.4.5，2012 年版的 7.3.5)；

——修改 SIEM 功能，增加了事态关联、事态过滤、事态聚合(见 7.5.6，2012 年版的 7.4.6)；

——删除响应中关于 IDS 和 IPS 介绍的相关内容(见 9.5.2)。

本标准使用重新起草法修改采用 ISO/IEC 27039:2015《信息技术　安全技术　入侵检测和防御系统(IDPS)的选择、部署和操作》。

本标准与 ISO/IEC 27039:2015 相比，在结构上增加了第 2 章“规范性引用文件”和第 4 章“缩略语”，将 7.3.1 和 7.3.2 的内容进行调序。

本标准与 ISO/IEC 27039:2015 的技术性差异及其原因如下：

——增加了第 2 章“规范性引用文件”和第 4 章“缩略语”，主要保持与 GB/T 28454—2012 的延续性；

——删除第 3 章背景中关于 IDPS 基础知识的介绍(见第 5 章)，因该内容在附录 A 中有详细介绍；

——增加了“当对 IDPS 产品有安全等级方面的要求时，见 GB/T 20275 和 GB/T 28451”，这主要是考虑对 IDPS 产品安全等级保护要求(见 7.3.1)；

——删除 7.5.2 关于 IDS 和 IPS 的相关内容(见 9.5.2)，因标准将入侵防御系统 IPS 纳入本标准范围，标准对象界定为入侵检测和防御系统 IDPS，故无需再单独介绍；

——增加了云计算环境中 IDPS 选择考虑事项(见 7.4.1、7.4.2、7.4.3、7.4.5)以及云环境下 IDPS 部署、多层级组织中 IDPS 部署，主要是因为目前云计算环境中 IDPS 部署也需要考虑相关事项，但国际标准并未考虑此部分内容(见 8.1)。

本标准做了下列编辑性修改：

——删除 3.8 的注。

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、中国网络安全审查技术与认证中心、陕西省网络与信息安全测评中心、北京天融信网络安全技术有限公司、山东崇弘信息技术有限公司、成都秦川物联网科技股份有限公司。

本标准主要起草人:王曙光、王庆升、王凤娇、魏军、公伟、张斌、来永钧、杨帆、杨锐、雷晓峰、邵泽华、樊华、朱琳、高瑞、杨向东、杨斌、权亚强、路征、陈慧勤、刘勘伪、于秀彦、胡鑫磊、王栋、潘海燕、李红胜。

本标准所代替标准的历次版本发布情况为:

——GB/T 28454—2012。

# 引　言

组织在选择、部署入侵检测和防御系统(IDPS)之前,不仅需要知道入侵事件(针对网络、系统或应用)是否发生、何时发生以及如何发生,也需要知道入侵事件利用了何种脆弱性,为防止类似入侵事件发生,未来需要采取何种防护措施或风险处置手段(即风险缓解、风险保留、风险规避、风险分担)。组织需识别并避免基于网络的入侵。从20世纪90年代中期开始,组织为了满足上述需求开始使用入侵检测和防御系统(IDPS)。随着IDPS产品的不断发展,其应用领域不断扩大,满足了组织对入侵检测和防御能力持续增长的需求。

为了使IDPS效益最大化,需要由经过培训、经验丰富的人员精心策划及实施IDPS的选择、部署和操作过程。通过上述过程,使IDPS成为组织预防入侵的重要安全工具(在组织ICT基础设施中作为重要安全设施),帮助组织截获入侵信息。

本标准提供了有效选择、部署和操作IDPS的指南,以及有关IDPS的基础知识。同时本标准还适用于需要外包其IDPS服务的相关组织。关于外包服务级别协议的相关信息参见ISO/IEC 20000的IT服务管理(ITSM)过程。

本标准主要用于帮助组织实现如下目标:

a) 满足GB/T 22080的下列要求:

——应实施过程和控制以便能快速检测和响应安全事件;

——应执行监视、评审过程以及控制以便识别企图的安全危害和既成的安全事件。

b) 实现控制以满足GB/T 22081的下列安全目标:

——能够检测未授权的信息处理活动;

——监视系统并记录信息安全事态,使用操作者日志和默认日志以确保能够识别信息系统问题;

——满足所有适用于监视和记录活动的相关法律要求;

——将系统监视用于检查已实施控制的有效性,以验证访问策略模型是否符合需求。

对满足上述要求而言,部署IDPS并非唯一、完善的解决方案。此外,本标准并不作为诸如信息安全管理体系(ISMS)认证、IDPS服务或产品认证等合格评定的准则。

# 信息技术　安全技术　入侵检测和防御系统（IDPS）的选择、部署和操作

## 1　范围

本标准给出了组织部署入侵检测和防御系统（IDPS）的指南。本标准详细说明了 IDPS 的选择、部署和操作。同时本标准给出了形成这些指南的背景信息。

本标准适用于准备部署入侵检测和防御系统（IDPS）的组织。

## 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　信息技术安全评估准则[ISO/IEC 15408（所有部分）]

GB/T 20275　信息安全技术　网络入侵检测系统技术要求和测试评价方法

GB/T 20985.1—2017　信息技术　安全技术　信息安全事件管理　第 1 部分：事件管理原理（ISO/IEC 27035-1：2006，IDT）

GB/T 25068.2　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 18028-2：2006，IDT）

GB/T 28451　信息安全技术　网络型入侵防御产品技术要求和测试评价方法

GB/T 29246—2017　信息技术　安全技术　信息安全管理体系　概述和词汇（ISO/IEC 27000：2016，IDT）

## 3　术语和定义

GB/T 29246—2017 界定的以及下列术语和定义适用于本文件。

3.1

**攻击　attack**

企图破坏、泄露、篡改、损伤、窃取、未授权访问或未授权使用资产的行为。

[GB/T 29246—2017，定义 2.3]

3.2

**攻击特征　attack signature**

执行某种攻击的计算机活动系列或其变体，通常通过检查网络流量或主机日志加以确定，IDPS 也依其来发现已经发生的攻击。

注：这也可称为一个攻击模式。

3.3

**证明　attestation**

公钥加密而产生的变量，可使 IDPS 软件程序和设备鉴别其远程方的身份。

注：见 3.23 远程证明。