



# 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 .....	III
引言 .....	V
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 缩略语 .....	4
5 背景 .....	5
6 总则 .....	6
7 选择 .....	6
7.1 简介 .....	6
7.2 信息安全风险评估 .....	7
7.3 主机或网络 IDPS .....	7
7.4 考虑事项 .....	7
7.5 补充 IDPS 的工具 .....	12
7.6 可伸缩性 .....	15
7.7 技术支持 .....	15
7.8 培训 .....	15
8 部署 .....	15
8.1 总则 .....	15
8.2 分阶段部署 .....	16
8.3 NIDPS 部署 .....	16
8.4 HIDPS 部署 .....	18
8.5 防护和保护 IDPS 信息安全 .....	18
9 操作 .....	19
9.1 总则 .....	19
9.2 IDPS 调优 .....	19
9.3 IDPS 脆弱性 .....	19
9.4 处理 IDPS 报警 .....	20
9.5 响应选项 .....	21
9.6 法律方面的考虑事项 .....	21
附录 A (资料性附录) 入侵检测和防御系统(IDPS):框架及需要考虑的问题 .....	23
参考文献 .....	38