ICS 35.040
L 80

中华人民共和国国家标准

GB/T 22239—2019
代替 GB/T 22239—2008

信息安全技术
网络安全等级保护基本要求

Information security technology—
Baseline for classified protection of cybersecurity

2019-05-10 发布　　2019-12-01 实施

国家市场监督管理总局
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。

本标准代替 GB/T 22239—2008《信息安全技术　信息系统安全等级保护基本要求》，与 GB/T 22239—2008 相比，主要变化如下：

——将标准名称变更为《信息安全技术　网络安全等级保护基本要求》；

——调整分类为安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理；

——调整各个级别的安全要求为安全通用要求、云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求和工业控制系统安全扩展要求；

——取消了原来安全控制点的 S、A、G 标注，增加一个附录 A 描述等级保护对象的定级结果和安全要求之间的关系，说明如何根据定级结果选择安全要求；

——调整了原来附录 A 和附录 B 的顺序，增加了附录 C 描述网络安全等级保护总体框架，并提出关键技术使用要求。

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：公安部第三研究所(公安部信息安全等级保护评估中心)、国家能源局信息中心、阿里云计算有限公司、中国科学院信息工程研究所(信息安全国家重点实验室)、新华三技术有限公司、华为技术有限公司、启明星辰信息技术集团股份有限公司、北京鼎普科技股份有限公司、中国电子信息产业集团有限公司第六研究所、公安部第一研究所、国家信息中心、山东微分电子科技有限公司、中国电子科技集团公司第十五研究所(信息产业信息安全测评中心)、浙江大学、工业和信息化部计算机与微电子发展研究中心(中国软件评测中心)、浙江国利信安科技有限公司、机械工业仪器仪表综合技术经济研究所、杭州科技职业技术学院。

本标准主要起草人：马力、陈广勇、张振峰、郭启全、葛波蔚、祝国邦、陆磊、曲洁、于东升、李秋香、任卫红、胡红升、陈雪鸿、冯冬芹、王江波、张宗喜、张宇翔、毕马宁、沙森森、李明、黎水林、于晴、李超、刘之涛、袁静、霍珊珊、黄顺京、尹湘培、苏艳芳、陶源、陈雪秀、于俊杰、沈锡镛、杜静、周颖、吴薇、刘志宇、宫月、王昱镔、禄凯、章恒、高亚楠、段伟恒、马闽、贾驰千、陆耿虹、高梦州、赵泰、孙晓军、许凤凯、王绍杰、马红霞、刘美丽。

本标准所代替标准的历次版本发布情况为：

——GB/T 22239—2008。

h) 大数据平台应提供数据分类分级安全管理功能，供大数据应用针对不同类别级别的数据采取不同的安全保护措施；
i) 大数据平台应提供设置数据安全标记功能，基于安全标记的授权和访问控制措施，满足细粒度授权访问控制管理能力要求；
j) 大数据平台应在数据采集、存储、处理、分析等各个环节，支持对数据进行分类分级处置，并保证安全保护策略保持一致；
k) 涉及重要数据接口、重要服务接口的调用，应实施访问控制，包括但不限于数据处理、使用、分析、导出、共享、交换等相关操作；
l) 应在数据清洗和转换过程中对重要数据进行保护，以保证重要数据清洗和转换后的一致性，避免数据失真，并在产生问题时能有效还原和恢复；
m) 应跟踪和记录数据采集、处理、分析和挖掘等过程，保证溯源数据能重现相应过程，溯源数据满足合规审计要求；
n) 大数据平台应保证不同客户大数据应用的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力；
o) 大数据平台应具备对不同类别、不同级别数据全生命周期区分处置的能力。

H.5.4 安全建设管理

本方面控制措施包括：

a) 应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力；
b) 应以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容；
c) 应明确约束数据交换、共享的接收方对数据的保护责任，并确保接收方有足够或相当的安全防护能力。

H.5.5 安全运维管理

本方面控制措施包括：

a) 应建立数字资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括并不限于数据采集、存储、处理、应用、流动、销毁等过程；
b) 应制定并执行数据分类分级保护策略，针对不同类别级别的数据制定不同的安全保护措施；
c) 应在数据分类分级的基础上，划分重要数字资产范围，明确重要数据进行自动脱敏或去标识的使用场景和业务处理流程；
d) 应定期评审数据的类别和级别，如需要变更数据的类别或级别，应依据变更审批流程执行变更。

参 考 文 献

[1] GB/T 18336.1—2015 信息技术 安全技术 信息技术安全评估准则 第1部分:简介和一般模型

[2] GB/T 22080—2016 信息技术 安全技术 信息安全管理体系 要求

[3] GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南

[4] NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
网络安全等级保护基本要求
GB/T 22239—2019
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2019 年 4 月第一版
*
书号:155066·1-62416

GB/T 22239-2019