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、沙森淼、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。

引　言

为了配合《中华人民共和国网络安全法》的实施，同时适应云计算、移动互联、物联网、工业控制和大数据等新技术、新应用情况下网络安全等级保护工作的开展，需对 GB/T 22239—2008 进行修订，修订的思路和方法是调整原国家标准 GB/T 22239—2008 的内容，针对共性安全保护需求提出安全通用要求，针对云计算、移动互联、物联网、工业控制和大数据等新技术、新应用领域的个性安全保护需求提出安全扩展要求，形成新的网络安全等级保护基本要求标准。

本标准是网络安全等级保护相关系列标准之一。

与本标准相关的标准包括：

——GB/T 25058　信息安全技术　信息系统安全等级保护实施指南；

——GB/T 22240　信息安全技术　信息系统安全等级保护定级指南；

——GB/T 25070　信息安全技术　网络安全等级保护安全设计技术要求；

——GB/T 28448　信息安全技术　网络安全等级保护测评要求；

——GB/T 28449　信息安全技术　网络安全等级保护测评过程指南。

在本标准中，**黑体字部分**表示较高等级中增加或增强的要求。

信息安全技术
网络安全等级保护基本要求

1 范围

本标准规定了网络安全等级保护的第一级到第四级等级保护对象的安全通用要求和安全扩展要求。

本标准适用于指导分等级的非涉密对象的安全建设和监督管理。

注：第五级等级保护对象是非常重要的监督管理对象，对其有特殊的管理模式和安全要求，所以不在本标准中进行描述。

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 17859 计算机信息系统 安全保护等级划分准则

GB/T 22240 信息安全技术 信息系统安全等级保护定级指南

GB/T 25069 信息安全技术 术语

GB/T 31167—2014 信息安全技术 云计算服务安全指南

GB/T 31168—2014 信息安全技术 云计算服务安全能力要求

GB/T 32919—2016 信息安全技术 工业控制系统安全控制应用指南

3 术语和定义

GB 17859、GB/T 22240、GB/T 25069、GB/T 31167—2014、GB/T 31168—2014 和 GB/T 32919—2016 界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了 GB/T 31167—2014、GB/T 31168—2014 和 GB/T 32919—2016 中的一些术语和定义。

3.1

网络安全 cybersecurity

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

3.2

安全保护能力 security protection ability

能够抵御威胁、发现安全事件以及在遭到损害后能够恢复先前状态等的程度。

3.3

云计算 cloud computing

通过网络访问可扩展的、灵活的物理或虚拟共享资源池，并按需自助获取和管理资源的模式。

注：资源实例包括服务器、操作系统、网络、软件、应用和存储设备等。

[GB/T 31167—2014，定义 3.1]