ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25070—2019
代替 GB/T 25070—2010

信息安全技术
网络安全等级保护安全设计技术要求

Information security technology—
Technical requirements of security design 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 25070—2010《信息安全技术　信息系统等级保护安全设计技术要求》，与 GB/T 25070—2010 相比，主要变化如下：

——将标准名称变更为《信息安全技术　网络安全等级保护安全设计技术要求》；

——各个级别的安全计算环境设计技术要求调整为通用安全计算环境设计技术要求、云安全计算环境设计技术要求、移动互联安全计算环境设计技术要求、物联网系统安全计算环境设计技术要求和工业控制系统安全计算环境设计技术要求；

——各个级别的安全区域边界设计技术要求调整为通用安全区域边界设计技术要求、云安全区域边界设计技术要求、移动互联安全区域边界设计技术要求、物联网系统安全区域边界设计技术要求和工业控制系统安全区域边界设计技术要求；

——各个级别的安全通信网络设计技术要求调整为通用安全通信网络设计技术要求、云安全通信网络设计技术要求、移动互联安全通信网络设计技术要求、物联网系统安全通信网络设计技术要求和工业控制系统安全通信网络设计技术要求；

——删除了附录 B 中的 B.2“子系统间接口”和 B.3“重要数据结构”，增加了 B.4“第三级系统可信验证实现机制”。

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：公安部第一研究所、北京工业大学、北京中软华泰信息技术有限责任公司、中国电子信息产业集团有限公司第六研究所、中国信息通信研究院、阿里云计算技术有限公司、中国银行股份有限公司软件中心、公安部第三研究所、国家能源局信息中心、中国电力科学研究院有限公司、中国科学院软件研究所、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)、中国科学院信息工程研究所、启明星辰信息技术集团股份有限公司、浙江中烟工业有限责任公司、中央电视台、北京江南天安科技有限公司、华为技术有限公司、北京航空航天大学、北京理工大学、北京天融信网络安全技术有限公司、北京和利时系统工程有限公司、青岛海天炜业过程控制技术股份有限公司、北京力控华康科技有限公司、石化盈科信息技术有限责任公司、北京华大智宝电子系统有限公司、山东微分电子科技有限公司、北京中电瑞铠科技有限公司、北京广利核系统工程有限公司、北京神州绿盟科技有限公司。

本标准主要起草人：蒋勇、李超、李秋香、赵勇、袁静、徐晓军、宫月、吴薇、黄学臻、陈翠云、刘志宇、陈彦如、王昱镔、张森、卢浩、吕由、林莉、徐进、傅一帆、丰大军、龚炳铮、贡春燕、霍玉鲜、范文斌、魏亮、田慧蓉、李强、李艺、沈锡镛、陈雪秀、任卫红、孙利民、朱红松、阎兆腾、段伟恒、孟雅辉、章志华、李健俊、李威、顾军、陈卫平、琚宏伟、陈冠直、胡红升、陈雪鸿、高昆仑、张锎、张敏、李昊、王宝会、汤世平、雷晓锋、王弢、王晓鹏、刘美丽、陈聪、刘安正、刘利民、龚亮华、方亮、石宝臣、孙郁熙、巩金亮、周峰、郝鑫、梁猛、姜红勇、冯坚、黄敏、张旭武、石秦、孙洪涛。

本标准所代替标准的历次版本发布情况为：

——GB/T 25070—2010。

引　言

GB/T 25070—2010《信息安全技术　信息系统等级保护安全设计技术要求》在开展网络安全等级保护工作的过程中起到了非常重要的作用，被广泛应用于指导各个行业和领域开展网络安全等级保护建设整改等工作，但是随着信息技术的发展，GB/T 25070—2010 在适用性、时效性、易用性、可操作性上需要进一步完善。

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 25070—2010 进行修订，修订的思路和方法是调整原国家标准 GB/T 25070—2010 的内容，针对共性安全保护目标提出通用的安全设计技术要求，针对云计算、移动互联、物联网、工业控制和大数据等新技术、新应用领域的特殊安全保护目标提出特殊的安全设计技术要求。

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 22239　信息安全技术　网络安全等级保护基本要求；

——GB/T 28448　信息安全技术　网络安全等级保护测评要求。

在本标准中，**黑体字部分**表示较低等级中没有出现或增强的要求。

信息安全技术
网络安全等级保护安全设计技术要求

1 范围

本标准规定了网络安全等级保护第一级到第四级等级保护对象的安全设计技术要求。

本标准适用于指导运营使用单位、网络安全企业、网络安全服务机构开展网络安全等级保护安全技术方案的设计和实施，也可作为网络安全职能部门进行监督、检查和指导的依据。

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设计技术要求，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—1999 计算机信息系统 安全保护等级划分准则

GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南

GB/T 25069—2010 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—1999、GB/T 22240—2008、GB/T 25069—2010、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 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。

[GB/T 22239—2019，定义 3.1]

3.2

定级系统 classified system

已确定安全保护等级的系统。定级系统分为第一级、第二级、第三级、第四级和第五级系统。

3.3

定级系统安全保护环境 security environment of classified system

由安全计算环境、安全区域边界、安全通信网络和(或)安全管理中心构成的对定级系统进行安全保护的环境。