ICS 35.040
L 80

中华人民共和国国家标准

GB/T 28448—2019
代替 GB/T 28448—2012

信息安全技术
网络安全等级保护测评要求

Information security technology—
Evaluation requirement 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 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　等级测评概述 …… 2
5.1　等级测评方法 …… 2
5.2　单项测评和整体测评 …… 3
6　第一级测评要求 …… 3
6.1　安全测评通用要求 …… 3
6.2　云计算安全测评扩展要求 …… 19
6.3　移动互联安全测评扩展要求 …… 22
6.4　物联网安全测评扩展要求 …… 23
6.5　工业控制系统安全测评扩展要求 …… 25
7　第二级测评要求 …… 27
7.1　安全测评通用要求 …… 27
7.2　云计算安全测评扩展要求 …… 64
7.3　移动互联安全测评扩展要求 …… 72
7.4　物联网安全测评扩展要求 …… 75
7.5　工业控制系统安全测评扩展要求 …… 77
8　第三级测评要求 …… 81
8.1　安全测评通用要求 …… 81
8.2　云计算安全测评扩展要求 …… 138
8.3　移动互联安全测评扩展要求 …… 151
8.4　物联网安全测评扩展要求 …… 156
8.5　工业控制系统安全测评扩展要求 …… 162
9　第四级测评要求 …… 167
9.1　安全测评通用要求 …… 167
9.2　云计算安全测评扩展要求 …… 228
9.3　移动互联安全测评扩展要求 …… 242
9.4　物联网安全测评扩展要求 …… 247
9.5　工业控制系统安全测评扩展要求 …… 253
10　第五级测评要求 …… 259
11　整体测评 …… 259

11.1 概述 …… 259
11.2 安全控制点测评 …… 260
11.3 安全控制点间测评 …… 260
11.4 区域间测评 …… 260
12 测评结论 …… 260
12.1 风险分析和评价 …… 260
12.2 等级测评结论 …… 260
附录A（资料性附录） 测评力度 …… 262
附录B（资料性附录） 大数据可参考安全评估方法 …… 264
附录C（规范性附录） 测评单元编号说明 …… 284
参考文献 …… 285

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 28448—2012《信息安全技术　信息系统安全等级保护测评要求》，与 GB/T 28448—2012 相比，主要变化如下：

——将标准名称变更为《信息安全技术　网络安全等级保护测评要求》；

——每个级别增加了云计算安全测评扩展要求、移动互联安全测评扩展要求、物联网安全测评扩展要求和工业控制系统安全测评扩展要求等内容；

——增加了等级测评、测评对象、云服务商和云服务客户等相关术语和定义（见第 3 章，2012 年版的第 3 章）；

——将针对控制点的单元测评细化调整为针对要求项的单项测评，删除了“测评框架”（见 2012 年版的 4.1）和“等级测评内容”（见 2012 年版的 4.2）；

——增加了大数据可参考安全评估方法（见附录 B）和测评单元编号说明（见附录 C）。

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）、中国电子技术标准化研究院、国家信息中心、中国科学院信息工程研究所（信息安全国家重点实验室）、北京大学、新华三技术有限公司、成都科来软件有限公司、中国移动通信集团有限公司、北京鼎普科技股份有限公司、北京微步在线科技有限公司、北京梆梆安全科技有限公司、北京迅达云成科技有限公司、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）、公安部第一研究所、北京信息安全测评中心、国家能源局信息中心（电力行业信息安全等级保护测评中心）、全球能源互联网研究院、北京卓识网安技术股份有限公司、中国电力科学研究院、南京南瑞集团公司、国电南京自动化股份有限公司、南方电网科学研究院、中国电子信息产业集团公司第六研究所、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）、启明星辰信息技术集团股份有限公司、北京烽云互联科技有限公司、华普科工（北京）有限公司。

本标准主要起草人：陈广勇、李明、黎水林、马力、曲洁、于东升、艾春迪、郭启全、葛波蔚、祝国邦、陆磊、张宇翔、毕马宁、沙森森、李升、胡红升、陈雪鸿、袁静、章恒、张益、毛澍、王斌、尹湘培、王勇、高亚楠、焦安春、赵劲涛、于俊杰、徐衍龙、马晓波、江雷、黄顺京、朱建兴、苏艳芳、禄凯、何申、霍珊珊、于运涛、陈震、任卫红、孙惠平、万晓兰、马红霞、薛锋、赵林林、刘金刚、胡越宁、周晓雪、李亚军、杨洪起、孟召瑞、李飞、王江波、阚志刚、刘健、陶源、李秋香、许凤凯、王绍杰、李晨旸、李凌、朱世顺、张五一、陈华军、张洁昕、张彪、李汪蔚、王雪、蔡学琳、胡娟、刘静、周峰、郝鑫、马闽、段伟恒。

本标准所代替标准的历次版本发布情况为：

——GB/T 28448—2012。

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、物联网和工业控制等新技术、新应用情况下网络安全等级保护工作的开展，需对 GB/T 28448—2012 进行修订。同时，作为测评指标进行引用的 GB/T 22239—2008 也启动了修订工作。修订的思路和方法依据 GB/T 22239 调整的内容，针对共性安全保护需求提出安全测评通用要求，针对云计算、移动互联、物联网和工业控制等新技术、新应用领域的个性安全保护需求提出安全测评扩展要求，形成新的《信息安全技术　网络安全等级保护测评要求》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 22239　信息安全技术　网络安全等级保护基本要求；

——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 28449　信息安全技术　网络安全等级保护测评过程指南。

信息安全技术
网络安全等级保护测评要求

1 范围

本标准规定了不同级别的等级保护对象的安全测评通用要求和安全测评扩展要求。

本标准适用于安全测评服务机构、等级保护对象的运营使用单位及主管部门对等级保护对象的安全状况进行安全测评并提供指南，也适用于网络安全职能部门进行网络安全等级保护监督检查时参考使用。

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测评要求，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 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

GB/T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 28449—2018 信息安全技术 网络安全等级保护测评过程指南

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 25069、GB/T 22239—2019、GB/T 25070—2019、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 和 GB/T 31168—2014 中的一些术语和定义。

3.1

访谈 interview

测评人员通过引导等级保护对象相关人员进行有目的的(有针对性的)交流以帮助测评人员理解、澄清或取得证据的过程。

3.2

核查 examine

测评人员通过对测评对象(如制度文档、各类设备及相关安全配置等)进行观察、查验和分析，以帮助测评人员理解、澄清或取得证据的过程。

3.3

测试 test

测评人员使用预定的方法/工具使测评对象(各类设备或安全配置)产生特定的结果，将运行结果与