ICS 35.040
L 80

中华人民共和国国家标准

GB/T 22240—2020
代替 GB/T 22240—2008

信息安全技术
网络安全等级保护定级指南

Information security technology—
Classification guide for classified protection of cybersecurity

2020-04-28 发布 2020-1 1-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 22240—2008《信息安全技术　信息系统安全等级保护定级指南》，与 GB/T 22240—2008 相比，主要技术变化如下：

—修改了等级保护对象、信息系统的定义，增加了网络安全、通信网络设施、数据资源的术语和定义（见第 3 章，2008 年版的第 3 章）；

—增加了通信网络设施和数据资源的定级对象确定方法（见 5.2、5.3）；

—增加了特定定级对象定级说明（见第 7 章）；

—修改了定级流程（见 4.4，2008 年版的 5.1）。

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、亚信科技（成都）有限公司、阿里云计算有限公司、深圳市腾讯计算机系统有限公司、启明星辰信息技术集团股份有限公司、审计署计算机技术中心。

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 22240—2008 进行修订，从等级保护对象定义和定级流程等方面进行补充、细化和完善，形成新的网络安全等级保护定级指南标准。

与本标准相关的国家标准包括：

—GB/T 22239　信息安全技术　网络安全等级保护基本要求；

—GB/T 25058　信息安全技术　网络安全等级保护实施指南；

—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。

信息安全技术
网络安全等级保护定级指南

1 范围

本标准给出了非涉及国家秘密的等级保护对象的安全保护等级定级方法和定级流程。

本标准适用于指导网络运营者开展非涉及国家秘密的等级保护对象的定级工作。

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 29246—2017 信息技术 安全技术 信息安全管理体系 概述和词汇

GB/T 31167—2014 信息安全技术 云计算服务安全指南

GB/T 32919—2016 信息安全技术 工业控制系统安全控制应用指南

GB/T 35295—2017 信息技术 大数据 术语

3 术语和定义

GB 17859—1999、GB/T 22239—2019、GB/T 25069、GB/T 29246—2017、GB/T 31167—2014、GB/T 32919—2016 和 GB/T 35295—2017 界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了上述标准中的某些术语和定义。

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

等级保护对象 targetofclassifiedprotection

网络安全等级保护工作直接作用的对象。

注：主要包括信息系统、通信网络设施和数据资源等。

3.3

信息系统 informationsystem

应用、服务、信息技术资产或其他信息处理组件。

[GB/T 29246—2017,定义 2.39]

注 1：信息系统通常由计算机或者其他信息终端及相关设备组成，并按照一定的应用目标和规则进行信息处理或过程控制。

注 2：典型的信息系统如办公 自动化系统、云计算平台 / 系统、物联网、工业控制系统以及采用移动互联技术的系统等。

3.4

通信网络设施 networkinfrastructure

为信息流通、网络运行等起基础支撑作用的网络设备设施。

注：主要包括电信网、广播电视传输网和行业或单位的专用通信网等。

3.5

数据资源 dataresources

具有或预期具有价值的数据集合。

注：数据资源多以电子形式存在。

3.6

受侵害的客体 objectofinfringement

受法律保护的、等级保护对象受到破坏时所侵害的社会关系。

注：本标准中简称“客体”。

3.7

客观方面 objective

对客体造成侵害的客观外在表现，包括侵害方式和侵害结果等。

4 定级原理及流程

4.1 安全保护等级

根据等级保护对象在国家安全、经济建设、社会生活中的重要程度，以及一旦遭到破坏、丧失功能或者数据被篡改、泄露、丢失、损毁后，对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的侵害程度等因素，等级保护对象的安全保护等级分为以下五级：

a) 第一级，等级保护对象受到破坏后，会对相关公民、法人和其他组织的合法权益造成一般损害，但不危害国家安全、社会秩序和公共利益；

b) 第二级，等级保护对象受到破坏后，会对相关公民、法人和其他组织的合法权益造成严重损害或特别严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全；

c) 第三级，等级保护对象受到破坏后，会对社会秩序和公共利益造成严重危害，或者对国家安全造成危害；

d) 第四级，等级保护对象受到破坏后，会对社会秩序和公共利益造成特别严重危害，或者对国家安全造成严重危害；

e) 第五级，等级保护对象受到破坏后，会对国家安全造成特别严重危害。