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。

# 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]

3.4

**云服务商　cloud service provider**

云计算服务的供应方。

注：云服务商管理、运营、支撑云计算的计算基础设施及软件，通过网络交付云计算的资源。

[GB/T 31167—2014，定义 3.3]

3.5

**云服务客户　cloud service customer**

为使用云计算服务同云服务商建立业务关系的参与方。

[GB/T 31168—2014，定义 3.4]

3.6

**云计算平台/系统　cloud computing platform/system**

云服务商提供的云计算基础设施及其上的服务软件的集合。

3.7

**虚拟机监视器　hypervisor**

运行在基础物理服务器和操作系统之间的中间软件层，可允许多个操作系统和应用共享硬件。

3.8

**宿主机　host machine**

运行虚拟机监视器的物理服务器。

3.9

**移动互联　mobile communication**

采用无线通信技术将移动终端接入有线网络的过程。

3.10

**移动终端　mobile device**

在移动业务中使用的终端设备，包括智能手机、平板电脑、个人电脑等通用终端和专用终端设备。

3.11

**无线接入设备　wireless access device**

采用无线通信技术将移动终端接入有线网络的通信设备。

3.12

**无线接入网关　wireless access gateway**

部署在无线网络与有线网络之间，对有线网络进行安全防护的设备。

3.13

**移动应用软件　mobile application**

针对移动终端开发的应用软件。

3.14

**移动终端管理系统　mobile device management system**

用于进行移动终端设备管理、应用管理和内容管理的专用软件，包括客户端软件和服务端软件。

3.15

**物联网　internet of things**

将感知节点设备通过互联网等网络连接起来构成的系统。

3.16

**感知节点设备　sensor node**

对物或环境进行信息采集和/或执行操作，并能联网进行通信的装置。

3.17

**感知网关节点设备　sensor layer gateway**

将感知节点所采集的数据进行汇总、适当处理或数据融合，并进行转发的装置。

3.18

**工业控制系统　industrial control system**

工业控制系统(ICS)是一个通用术语，它包括多种工业生产中使用的控制系统，包括监控和数据采集系统(SCADA)、分布式控制系统(DCS)和其他较小的控制系统，如可编程逻辑控制器(PLC)，现已广泛应用在工业部门和关键基础设施中。

[GB/T 32919—2016，定义 3.1]

## 4　缩略语

下列缩略语适用于本文件。

AP：无线访问接入点(Wireless Access Point)

DCS：集散控制系统(Distributed Control System)

DDoS：拒绝服务 (Distributed Denial of Service)

ERP：企业资源计划(Enterprise Resource Planning)

FTP：文件传输协议(File Transfer Protocol)

HMI：人机界面(Human Machine Interface)

IaaS：基础设施即服务(Infrastructure-as-a-Service)

ICS：工业控制系统(Industrial Control System)

IoT：物联网(Internet of Things)

IP：互联网协议(Internet Protocol)

IT：信息技术(Information Technology)

MES：制造执行系统(Manufacturing Execution System)

PaaS：平台即服务(Platform-as-a-Service)

PLC：可编程逻辑控制器(Programmable Logic Controller)

RFID：射频识别(Radio Frequency Identification)

SaaS：软件即服务(Software-as-a-Service)

SCADA：数据采集与监视控制系统(Supervisory Control and Data Acquisition System)

SSID：服务集标识(Service Set Identifier)

TCB：可信计算基(Trusted Computing Base)

USB：通用串行总线(Universal Serial Bus)

WEP：有线等效加密(Wired Equivalent Privacy)

WPS：WiFi 保护设置(WiFi Protected Setup)

## 5　网络安全等级保护概述

### 5.1　等级保护对象

等级保护对象是指网络安全等级保护工作中的对象，通常是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统，主要包括基础信息网络、云计算平台/系统、大数据应用/平台/资源、物联网(IoT)、工业控制系统和采用移动互联技术的

系统等。等级保护对象根据其在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、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危害程度等，由低到高被划分为五个安全保护等级。

保护对象的安全保护等级确定方法见 GB/T 22240。

### 5.2 不同级别的安全保护能力

不同级别的等级保护对象应具备的基本安全保护能力如下：

第一级安全保护能力：应能够防护免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾难，以及其他相当危害程度的威胁所造成的关键资源损害，在自身遭到损害后，能够恢复部分功能。

第二级安全保护能力：应能够防护免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难，以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和处置安全事件，在自身遭到损害后，能够在一段时间内恢复部分功能。

第三级安全保护能力：应能够在统一安全策略下防护免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难，以及其他相当危害程度的威胁所造成的主要资源损害，能够及时发现、监测攻击行为和处置安全事件，在自身遭到损害后，能够较快恢复绝大部分功能。

第四级安全保护能力：应能够在统一安全策略下防护免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难，以及其他相当危害程度的威胁所造成的资源损害，能够及时发现、监测发现攻击行为和安全事件，在自身遭到损害后，能够迅速恢复所有功能。

第五级安全保护能力：略。

### 5.3 安全通用要求和安全扩展要求

由于业务目标的不同、使用技术的不同、应用场景的不同等因素，不同的等级保护对象会以不同的形态出现，表现形式可能称之为基础信息网络、信息系统（包含采用移动互联等技术的系统）、云计算平台/系统、大数据平台/系统、物联网、工业控制系统等。形态不同的等级保护对象面临的威胁有所不同，安全保护需求也会有所差异。为了便于实现对不同级别的和不同形态的等级保护对象的共性化和个性化保护，等级保护要求分为安全通用要求和安全扩展要求。

安全通用要求针对共性化保护需求提出，等级保护对象无论以何种形式出现，应根据安全保护等级实现相应级别的安全通用要求；安全扩展要求针对个性化保护需求提出，需要根据安全保护等级和使用的特定技术或特定的应用场景选择性实现安全扩展要求。安全通用要求和安全扩展要求共同构成了对等级保护对象的安全要求。安全要求的选择见附录 A，整体安全保护能力的要求见附录 B 和附录 C。

本标准针对云计算、移动互联、物联网、工业控制系统提出了安全扩展要求。云计算应用场景参见附录 D，移动互联应用场景参见附录 E，物联网应用场景参见附录 F，工业控制系统应用场景参见附录 G，大数据应用场景参见附录 H。对于采用其他特殊技术或处于特殊应用场景的等级保护对象，应在安全风险评估的基础上，针对安全风险采取特殊的安全措施作为补充。

## 6 第一级安全要求

### 6.1 安全通用要求

#### 6.1.1 安全物理环境

##### 6.1.1.1 物理访问控制

机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。

#### 6.1.1.2 防盗窃和防破坏

应将设备或主要部件进行固定，并设置明显的不易除去的标识。

#### 6.1.1.3 防雷击

应将各类机柜、设施和设备等通过接地系统安全接地。

#### 6.1.1.4 防火

机房应设置灭火设备。

#### 6.1.1.5 防水和防潮

应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。

#### 6.1.1.6 温湿度控制

应设置必要的温湿度调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

#### 6.1.1.7 电力供应

应在机房供电线路上配置稳压器和过电压防护设备。

### 6.1.2 安全通信网络

#### 6.1.2.1 通信传输

应采用校验技术保证通信过程中数据的完整性。

#### 6.1.2.2 可信验证

可基于可信根对通信设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。

### 6.1.3 安全区域边界

#### 6.1.3.1 边界防护

应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。

#### 6.1.3.2 访问控制

本项要求包括：

a) 应在网络边界根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出。

#### 6.1.3.3 可信验证

可基于可信根对边界设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。