ICS 35.240.40
L 80

# 中华人民共和国国家标准

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

**Information security technology—
Technical requirements of security design for
information system classified protection**

2010-09-02 发布　　2011-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

# 目　　次

# 前　言

本标准的附录A、附录B是资料性附录。

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。

本标准主要起草单位:公安部第一研究所。

本标准主要起草人:厉剑、范红、胡志昂、吉增瑞、张洪斌、赵勇、金丽娜、韩煜、赵会敏、张红旗、杜学绘、宫敏、马永清、韩勇桥、王超、连一峰、张海霞、黄涛、徐国爱、金舒原、田志宏、姜伟、刘鑫、苏智睿、李理、刘卫国、李娜。

# 引　言

《中华人民共和国计算机信息系统安全保护条例》(国务院令第147号)明确规定我国“计算机信息系统实行安全等级保护”。依据国务院147号令要求制定发布的强制性国家标准GB 17859—1999《计算机信息系统　安全保护等级划分准则》为计算机信息系统安全保护等级的划分奠定了技术基础。《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号)明确指出实行信息安全等级保护“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统,抓紧建立信息安全等级保护制度”。《关于信息安全等级保护工作的实施意见》(公通字[2004]66号)和《信息安全等级保护管理办法》(公通字[2007]43号)确定了实施信息安全等级保护制度的原则、工作职责划分、实施要求和实施计划,明确了开展信息安全等级保护工作的基本内容、工作流程、工作方法等。

上述信息安全等级保护相关法规、政策文件、国家标准和公共安全行业标准的出台,为信息安全等级保护工作的开展提供了法律、政策、标准依据。

2007年7月全国开展重要信息系统等级保护定级工作,标志着信息安全等级保护工作在我国全面展开。在开展信息安全等级保护定级和备案工作基础上,各单位、各部门正在按照信息安全等级保护有关政策规定和技术标准规范,开展信息系统安全建设和加固工作,建立、健全信息安全管理制度,落实安全保护技术措施,全面贯彻落实信息安全等级保护制度。为了配合信息系统安全建设和加固工作,特制定本标准。

本标准规范了信息系统等级保护安全设计技术要求,包括第一级至第五级系统安全保护环境的安全计算环境、安全区域边界、安全通信网络和安全管理中心等方面的设计技术要求,以及定级系统互联的设计技术要求。涉及物理安全、安全管理、安全运维等方面的要求分别参见参考文献[9]、[2]、[7]、[10]等。进行安全技术设计时,要根据信息系统定级情况,确定相应安全策略,采取相应级别的安全保护措施。

在第5章至第9章中,每一级系统安全保护环境设计比较低一级系统安全保护环境设计所增加和增强的部分,用“**黑体**”表示。

# 信息安全技术
# 信息系统等级保护安全设计
# 技术要求

## 1 范围

本标准依据国家信息安全等级保护的要求，规定了信息系统等级保护安全设计技术要求。

本标准适用于指导信息系统运营使用单位、信息安全企业、信息安全服务机构开展信息系统等级保护安全技术方案的设计和实施，也可作为信息安全职能部门进行监督、检查和指导的依据。

## 2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 17859—1999 计算机信息系统 安全保护等级划分准则

## 3 术语和定义

GB 17859—1999 确立的以及下列术语和定义适用于本标准。

3.1

**定级系统 classified system**

按照参考文献[11]已确定安全保护等级的信息系统。定级系统分为第一级、第二级、第三级、第四级和第五级信息系统。

3.2

**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。

定级系统安全保护环境包括第一级系统安全保护环境、第二级系统安全保护环境、第三级系统安全保护环境、第四级系统安全保护环境、第五级系统安全保护环境以及定级系统的安全互联。

3.3

**安全计算环境 secure computing environment**

对定级系统的信息进行存储、处理及实施安全策略的相关部件。

安全计算环境按照保护能力划分为第一级安全计算环境、第二级安全计算环境、第三级安全计算环境、第四级安全计算环境和第五级安全计算环境。

3.4

**安全区域边界 secure area boundary**

对定级系统的安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件。

安全区域边界按照保护能力划分为第一级安全区域边界、第二级安全区域边界、第三级安全区域边界、第四级安全区域边界和第五级安全区域边界。