ICS 35.040
L 80

中华人民共和国国家标准

GB/T 22239—2008

信息安全技术
信息系统安全等级保护基本要求

Information security technology—
Baseline for classified protection of information system security

2008-06-19 发布　　2008-11-01 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和附录B是规范性附录。

本标准由公安部和全国信息安全标准化技术委员会提出。

本标准由全国信息安全标准化技术委员会归口。

本标准起草单位：公安部信息安全等级保护评估中心。

本标准主要起草人：马力、任卫红、李明、袁静、谢朝海、曲洁、李升、陈雪秀、朱建平、黄洪、刘静、罗峥、毕马宁。

引　言

依据国家信息安全等级保护管理规定制定本标准。

本标准是信息安全等级保护相关系列标准之一。

与本标准相关的系列标准包括：

——GB/T 22240—2008《信息安全技术　信息系统安全等级保护定级指南》；

——国家标准《信息安全技术　信息系统安全等级保护实施指南》。

本标准与 GB 17859—1999、GB/T 20269—2006、GB/T 20270—2006、GB/T 20271—2006 等标准共同构成了信息系统安全等级保护的相关配套标准。其中 GB 17859—1999 是基础性标准，本标准、GB/T 20269—2006、GB/T 20270—2006、GB/T 20271—2006 等是在 GB 17859—1999 基础上的进一步细化和扩展。

本标准在 GB 17859—1999、GB/T 20269—2006、GB/T 20270—2006、GB/T 20271—2006 等技术类标准的基础上，根据现有技术的发展水平，提出和规定了不同安全保护等级信息系统的最低保护要求，即基本安全要求，基本安全要求包括基本技术要求和基本管理要求，本标准适用于指导不同安全保护等级信息系统的安全建设和监督管理。

在本标准文本中，黑体字表示较低等级中没有出现或增强的要求。

信息安全技术
信息系统安全等级保护基本要求

1 范围

本标准规定了不同安全保护等级信息系统的基本保护要求，包括基本技术要求和基本管理要求，适用于指导分等级的信息系统的安全建设和监督管理。

2 规范性引用文件

下列文件中的条款通过在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使用这些文件的最新版本。凡是不注明日期的引用文件，其最新版本适用于本标准。

GB/T 5271.8 信息技术 词汇 第8部分：安全(GB/T 5271.8—2001，idt ISO/IEC 2382-8：1998)

GB 17859 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

3 术语和定义

GB/T 5271.8 和 GB 17859 确立的以及下列术语和定义适用于本标准。

3.1

安全保护能力 security protection ability

系统能够抵御威胁、发现安全事件以及在系统遭到损害后能够恢复先前状态等的程度。

4 信息系统安全等级保护概述

4.1 信息系统安全保护等级

信息系统根据其在国家安全、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，由低到高划分为五级，五级定义见GB/T 22240—2008。

4.2 不同等级的安全保护能力

不同等级的信息系统应具备的基本安全保护能力如下：

第一级安全保护能力：应能够防护系统免受来自个人的、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，在系统遭到损害后，能够恢复部分功能。

第二级安全保护能力：应能够防护系统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安全事件，在系统遭到损害后，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系统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，能够发现安全漏洞和安全事件，在系统遭到损害后，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系统免受来自国家级别的、敌对组织的、拥有