ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25058—2010

信息安全技术
信息系统安全等级保护实施指南

Information security technology—
Implementation guide for classified protection of information system

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：毕马宁、马力、陈雪秀、李明、朱建平、任卫红、谢朝海、曲洁、袁静、李升、刘静、罗峥。

引　言

依据《中华人民共和国计算机信息系统安全保护条例》(国务院147号令)、《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)、《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),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;

——GB/T 22239—2008　信息安全技术　信息系统安全等级保护基本要求。

在对信息系统实施信息安全等级保护的过程中,除使用本标准外,在不同的阶段,还应参照其他有关信息安全等级保护的标准开展工作。

在信息系统定级阶段,应按照GB/T 22240—2008介绍的方法,确定信息系统安全保护等级。

在信息系统总体安全规划,安全设计与实施,安全运行与维护和信息系统终止等阶段,应按照GB 17859—1999、GB/T 22239—2008、GB/T 20269—2006、GB/T 20270—2006和GB/T 20271—2006等技术标准,设计、建设符合信息安全等级保护要求的信息系统,开展信息系统的运行维护管理工作。

GB 17859—1999、GB/T 22239—2008、GB/T 20269—2006、GB/T 20270—2006和GB/T 20271—2006等技术标准是信息系统安全等级保护的系列相关配套标准,其中GB 17859—1999是基础性标准,GB/T 20269—2006、GB/T 20270—2006和GB/T 20271—2006等是对GB 17859—1999的进一步细化和扩展,GB/T 22239—2008是以GB 17859—1999为基础,根据现有技术发展水平提出的对不同安全保护等级信息系统的最基本安全要求,是其他标准的一个底线子集。

对信息系统的安全等级保护应从GB/T 22239—2008出发,在保证信息系统满足基本安全要求的基础上,逐步提高对信息系统的保护水平,最终满足GB 17859—1999、GB/T 20269—2006、GB/T 20270—2006和GB/T 20271—2006等标准的要求。

除本标准和上述提到的标准外,在信息系统安全等级保护实施过程中,还可参照和使用GB/T 20272—2006和GB/T 20273—2006等其他等级保护相关技术标准。

信息安全技术
信息系统安全等级保护实施指南

1 范围

本标准规定了信息系统安全等级保护实施的过程，适用于指导信息系统安全等级保护的实施。

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/T 5271.8 信息技术 词汇 第8部分：安全

GB 17859—1999 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—1999 确立的以及下列术语和定义适用于本标准。

3.1

等级测评 classified security testing and evaluation

确定信息系统安全保护能力是否达到相应等级基本要求的过程。

4 等级保护实施概述

4.1 基本原则

信息系统安全等级保护的核心是对信息系统分等级、按标准进行建设、管理和监督。信息系统安全等级保护实施过程中应遵循以下基本原则：

a) 自主保护原则

信息系统运营、使用单位及其主管部门按照国家相关法规和标准，自主确定信息系统的安全保护等级，自行组织实施安全保护。

b) 重点保护原则

根据信息系统的重要程度、业务特点，通过划分不同安全保护等级的信息系统，实现不同强度的安全保护，集中资源优先保护涉及核心业务或关键信息资产的信息系统。

c) 同步建设原则

信息系统在新建、改建、扩建时应当同步规划和设计安全方案，投入一定比例的资金建设信息安全设施，保障信息安全与信息化建设相适应。

d) 动态调整原则

要跟踪信息系统的变化情况，调整安全保护措施。由于信息系统的应用类型、范围等条件的变化及其他原因，安全保护等级需要变更的，应当根据等级保护的管理规范和技术标准的要求，重新确定信息系统的安全保护等级，根据信息系统安全保护等级的调整情况，重新实施安全保护。

4.2 角色和职责

信息系统安全等级保护实施过程中涉及的各类角色和职责如下：