ICS 35.020
L 09

中华人民共和国国家标准

GB/T 20008—2005

信息安全技术
操作系统安全评估准则

Information security technology—
Operating systems security evaluation criteria

2005-11-11 发布　　2006-05-01 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

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
操作系统安全评估准则
GB/T 20008—2005
*
中 国 标 准 出 版 社 出 版 发 行
北京西城区复兴门外三里河北街 16 号
邮政编码:100045
http://www.spc.net.cn
电话:63787337、63787447
2006 年 5 月第一版　2006 年 5 月电子版制作
*
书号:155066·1-27492

目　　次

前　言

GB 17859—1999《计算机信息系统安全保护等级划分准则》是我国计算机信息系统安全等级管理的重要标准，已于1999年9月13日发布。为促进安全等级管理工作的正常有序开展，特制定一系列相关的标准。本标准是系列标准之一。

本标准文本中，黑体字表示较低等级中没有出现或增强的评估内容。

本标准的附录A中说明操作系统面临的主要威胁和对策。

本标准的附录A是资料性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：北京大学软件工程国家工程中心，公安部公共信息网络安全监察局。

本标准主要起草人：王立福，赵学志，刘学洋，葛佳。

引　言

操作系统是管理硬件资源、控制程序运行、改善人机界面和为应用软件提供支持的一种系统软件。它是最靠近硬件的一层软件，将物理机器（裸机）扩展成可靠性高、使用方便、功能齐全的理想机器。操作系统设计的好坏直接影响计算机系统的性能，操作系统还应考虑系统的各个方面，任何遗漏或考虑不周都会影响计算机的工作。

用户使用计算机实际上是通过操作系统进行的，操作系统提供给用户的使用手段（或称界面）主要有三种：终端命令、系统调用和作业控制语言。

信息安全技术
操作系统安全评估准则

1 范围

本标准从信息技术方面规定了按照GB 17859—1999的五个安全保护等级对操作系统安全保护等级划分所需要的评估内容。

本标准适用于计算机通用操作系统的安全保护等级的评估，对于通用操作系统安全功能的研制、开发和测试亦可参照使用。

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

GB/T 18336.1—2001 信息技术 安全技术 信息技术安全性评估准则 第1部分：简介和一般模型(idt ISO/IEC 15408-1：1999)

3 术语和定义

GB 17859—1999和GB/T 18336.1—2001确立的术语和定义适用于本标准。

4 安全环境

4.1 物理方面

对操作系统资源的处理限定在一些可控制的访问设备内，防止未授权的物理访问。所有与实施操作系统安全策略相关的硬件和软件，应受到保护以免于未授权的物理修改。

4.2 人员方面

有一个或多个能胜任的授权用户来管理操作系统及所包含的信息。管理员遵从管理员指南实施管理，可能有偶然的失误，但不是恶意或敌对的。授权用户支配必要的授权来访问由操作系统管理的最少量的信息。

4.3 连通性方面

若操作系统包含多个工作站点，则各网络信息服务域中的所有工作站点都由一个中心工作站点管理。网络信息服务域可以由多个管理域组成，管理员管理本地资源和用户账号，在整个信息服务域中对资源进行无缝操作应是可能的。所有网络设备都能正确地没有改动地传送数据。

5 评估内容

5.1 用户自主保护级

5.1.1 自主访问控制

操作系统安全功能应实施安全机制，控制用户对客体的访问，其方法可以是：

——基于用户的权能表，为用户规定是否可以对客体进行访问；

——基于客体的访问控制表。