ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20272—2006

信息安全技术
操作系统安全技术要求

Information security technology—
Security techniques requirement for operating system

2006-05-31 发布　　2006-12-01 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：北京思源新创信息安全资讯有限公司，江南计算技术研究所技术服务中心。

本标准主要起草人：吉增瑞、汪晓茵、王志强、陈冠直、景乾元、宋健平。

引　言

本标准用以指导设计者如何设计和实现具有所需要的安全保护等级的操作系统，主要说明为实现GB 17859—1999中每一个安全保护等级的要求，操作系统应采取的安全技术措施，以及各安全技术要求在不同安全保护等级中具体实现上的差异。

计算机操作系统是信息系统的重要组成部分。计算机操作系统的主要功能是进行计算机资源管理和提供用户使用计算机的界面。操作系统所管理的资源包括各种用户资源和计算机的系统资源。用户资源可以归结为以文件形式表示的数据信息资源。系统资源包括系统程序和系统数据以及为管理计算机硬件资源而设置的各种表格，其在操作系统中也都是以文件的形式表现，分别称为可执行文件、数据文件、配置文件等。可见，对操作系统中资源的保护，实际上是对操作系统中文件的保护。由于操作系统在计算机系统中有着十分重要的地位和作用，所以对计算机系统的攻击和威胁（包括人为的和自然的），操作系统往往成为主要的目标。也正因为如此，操作系统的安全就变得十分重要。操作系统安全既要考虑操作系统的安全运行，也要考虑对操作系统中资源的保护（主要是以文件形式表示的数据信息资源的保护）。由于攻击和威胁既可能是针对系统运行的，也可能是针对信息的保密性、完整性和可用性的，所以对操作系统的安全保护的功能要求，需要从操作系统的安全运行和操作系统数据的安全保护两方面综合进行考虑。根据GB 17859—1999所列安全要素及GB/T 20271—2006关于信息系统安全功能要素的描述，本标准从身份鉴别、自主访问控制、标记和强制访问控制、数据流控制、审计、数据完整性、数据保密性、可信路径等方面对操作系统的安全功能要求进行更加具体的描述。为了确保安全功能要素达到所确定的安全性要求，需要通过一定的安全保证机制来实现，根据GB/T 20271—2006关于信息系统安全保证要素的描述，本标准从操作系统安全子系统（SSOOS）自身安全保护、操作系统安全子系统（SSOOS）的设计和实现以及操作系统安全子系统（SSOOS）的安全管理等方面，对操作系统的安全保证要求进行更加具体的描述。操作系统的安全还需要有相应的安全硬件系统（即物理安全）方面的支持，以及安全管理方面的支持，这已超出本标准的范围。

综合以上说明，本标准以GB 17859—1999五个安全保护等级的划分为基础，对操作系统的每一个安全保护等级的安全功能技术要求和安全保证技术要求做详细的描述。为清晰表示每一个安全等级比较低一级安全等级的安全技术要求的增加和增强，在第4章的描述中，每一级新增部分用“宋体加粗字”表示。

信息安全技术　操作系统安全技术要求

1　范围

本标准依据 GB 17859—1999 的五个安全保护等级的划分，根据操作系统在信息系统中的作用，规定了各个安全等级的操作系统所需要的安全技术要求。

本标准适用于按等级化要求进行的操作系统安全的设计和实现，对按等级化要求进行的操作系统安全的测试和管理可参照使用。

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 20271—2006　信息安全技术　信息系统通用安全技术要求

3　术语、定义和缩略语

3.1　术语和定义

GB 17859—1999 和 GB/T 20271—2006 确立的以及下列术语和定义适用于本标准。

3.1.1

操作系统安全　security of operating system

操作系统所存储、传输和处理的信息的保密性、完整性和可用性的表征。

3.1.2

操作系统安全技术　security technology of operating system

实现各种类型的操作系统安全需要的所有安全技术。

3.1.3

操作系统安全子系统　security subsystem of operating system

操作系统中安全保护装置的总称，包括硬件、固件、软件和负责执行安全策略的组合体。它建立了一个基本的操作系统安全保护环境，并提供安全操作系统要求的附加用户服务。

注：按照 GB 17859—1999 对 TCB（可信计算基）的定义，SSOOS（操作系统安全子系统）就是操作系统的 TCB。

3.1.4

SSOOS 安全策略　SSOOS security policy

对 SSOOS 中的资源进行管理、保护和分配的一组规则。一个 SSOOS 中可以有一个或多个安全策略。

3.1.5

安全功能策略　security function policy

为实现 SSOOS 安全要素要求的功能所采用的安全策略。

3.1.6

安全要素　security element

本标准中各安全保护等级的安全技术要求所包含的安全内容的组成成分。