ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20272—2019
代替 GB/T 20272—2006

信息安全技术　操作系统安全技术要求

**Information security technology—
Security technical requirements for operating system**

2019-08-30 发布　　2020-03-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 20272—2006《信息安全技术　操作系统安全技术要求》，与 GB/T 20272—2006 相比，除编辑性修改外主要技术变化如下：

——删除了“操作系统安全技术”“SSOOS 安全策略”“安全功能策略”“安全要素”“SSOOS 安全功能”“SSF 控制范围”的术语和定义（见 2006 年版的 3.1.2、3.1.4、3.1.5、3.1.6、3.1.7、3.1.8）；

——删除了“SFP 安全功能策略”“SSC SSF 控制范围”“SSP SSOOS 安全策略”的缩略语（见 2006 年版的 3.2）；

——增加了“UID 用户标识符”的缩略语（见第 4 章）；

——增加了“网络安全保护”安全功能要求（见 6.1.1.4、6.2.1.6、6.3.1.7、6.4.1.9、6.5.1.9）；

——增加了“数据加密”安全功能要求（见 6.2.1.5.1、6.3.1.6.2、6.4.1.6.2、6.5.1.6.2）；

——增加了“可信信道”安全功能要求（见 6.4.1.8、6.5.1.8）；

——在“安全功能”中，将“标记”“强制访问控制”合并为“标记和强制访问控制”（见 6.3.1.3、6.4.1.3、6.5.1.3）；

——删除了“数据流控制”安全功能要求（见 2006 年版的 4.3.1.5、4.4.1.5、4.5.1.5）；

——增加了 “可信度量”自身安全要求（见 6.2.2.4、6.3.2.4、6.4.2.4、6.5.2.4）；

——增加了 “可信恢复”自身安全要求（见 6.4.2.5、6.5.2.5）；

——增加了“安全策略配置”自身安全要求（见 6.1.2.4、6.2.2.5、6.3.2.5、6.4.2.6、6.5.2.6）；

——删除了 “SSF 物理安全保护”（见 2006 年版的 4.1.2.1、4.2.2.1、4.3.2.1、4.4.2.1、4.5.2.1）；

——将“SSOOS 访问控制”修改为“用户登录访问控制”（见 6.1.2.3、6.2.2.3、6.3.2.3、6.4.2.3、6.5.2.3）；

——将“SSF 数据安全保护”中的相关内容，整合到“数据完整性”“数据保密性”“可信路径”等安全功能中（见 6.1.1.3、6.2.1.4、6.2.1.5、6.3.1.5、6.3.1.6、6.4.1.5、6.4.1.6、6.4.1.7、6.5.1.5、6.5.1.6、6.5.1.7）；

——将“SSOOS 设计和实现”修改为“安全保障要求”，并根据 GB/T 18336.3—2015 的要求，进行了相应的修改（见 6.1.3、6.2.3、6.3.3、6.4.3、6.5.3，2006 年版的 4.1.3、4.2.3、4.3.3、4.4.3、4.5.3）；

——删除了“SSOOS 安全管理”要求（见 2006 年版的 4.1.4、4.2.4、4.3.4、4.4.4、4.5.4）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

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。

本标准起草单位：公安部第三研究所、北京江南天安科技有限公司、中科方德软件有限公司、中标软件有限公司、天津麒麟信息技术有限公司、普华基础软件股份有限公司、北京凝思软件股份有限公司。

本标准主要起草人：邱梓华、宋好好、陈妍、胡亚兰、顾健、陈冠直、徐宁、魏立峰、吴永成、朱健伟、王成靖、吉增瑞、丁丽萍、董军平、龚文、郎金刚、谭一鸣、胡丹妮、杨诏钧、戴华东、王玉成、孟健、宫敏、彭志航。

本标准所代替标准的历次版本发布情况为：

——GB/T 20272—2006。

信息安全技术　操作系统安全技术要求

1　范围

本标准规定了五个安全等级操作系统的安全技术要求。

本标准适用于操作系统安全性的研发、测试、维护和评价。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB 17859—1999　计算机信息系统　安全保护等级划分准则

GB/T 18336.3—2015　信息技术　安全技术 信息技术安全评估准则　第3部分：安全保障组件

GB/T 20271—2006　信息安全技术　信息系统通用安全技术要求

GB/T 29240—2012　信息安全技术　终端计算机通用安全技术要求与测试评价方法

3　术语和定义

GB 17859—1999、GB/T 18336.3—2015、GB/T 20271—2006 和 GB/T 29240—2012 界定的以及下列术语和定义适用于本文件。

3.1

操作系统安全　security of operating system

操作系统自身以及其所存储、传输和处理的信息的保密性、完整性和可用性。

3.2

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。

4　缩略语

下列缩略语适用于本文件。

SSF：SSOOS 安全功能(SSOOS Security Function)

SSOOS：操作系统安全子系统(Security Subsystem of Operating System)

UID：用户标识符(User Identifier)

5　产品描述

资源管理(包括设备硬件资源和数据资源)是操作系统最为基本的功能，操作系统中对资源的安全保护由 SSOOS 来实现。

SSOOS 是操作系统中所有安全保护装置的组合体。SSOOS 一般包含多个 SSF，每个安全功能模块是一个或多个安全功能策略的具体实现。SSOOS 中的所有安全功能策略构成了一个安全域，以保护