



# 中华人民共和国国家标准

GB/T 39680—2020

代替 GB/T 21028—2007, GB/T 25063—2010

---

## 信息安全技术 服务器安全技术要求和测评准则

Information security technology—  
Technique requirements and evaluation criteria for server security

2020-12-14 发布

2021-07-01 实施

---

国家市场监督管理总局  
国家标准化管理委员会 发布

## 目 次

前言 .....	III
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语、定义和缩略语 .....	1
4 概述 .....	2
5 安全技术要求 .....	2
5.1 安全功能要求 .....	2
5.1.1 设备标签 .....	2
5.1.2 硬件接口安全 .....	2
5.1.3 固件安全 .....	2
5.1.4 驱动程序安全 .....	3
5.1.5 可靠运行支持 .....	3
5.1.6 自身安全管理 .....	3
5.2 安全保障要求 .....	4
5.2.1 开发 .....	4
5.2.2 指导性文档 .....	4
5.2.3 生命周期支持 .....	5
5.2.4 测试 .....	5
5.2.5 脆弱性评定 .....	6
5.2.6 维护 .....	6
6 安全测评准则 .....	6
6.1 测试环境 .....	6
6.2 安全功能要求测评 .....	7
6.2.1 设备标签 .....	7
6.2.2 硬件接口安全 .....	7
6.2.3 固件安全 .....	8
6.2.4 驱动程序安全 .....	9
6.2.5 可靠运行支持 .....	9
6.2.6 自身安全管理 .....	10
6.3 安全保障要求测评 .....	12
6.3.1 开发 .....	12
6.3.2 指导性文档 .....	13
6.3.3 生命周期支持 .....	13

6.3.4 测试 .....	15
6.3.5 脆弱性评定 .....	17
6.3.6 维护 .....	17
附录 A (资料性附录) 服务器操作系统安全要求 .....	18
附录 B (资料性附录) 服务器安全技术要求分级表 .....	19
参考文献 .....	20

## 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 21028—2007《信息安全技术 服务器安全技术要求》和 GB/T 25063—2010《信息安全技术 服务器安全测评要求》，与 GB/T 21028—2007 和 GB/T 25063—2010 相比，主要技术变化如下：

- 整合了 GB/T 21028—2007 和 GB/T 25063—2010 两项标准内容，修改标准名称为《信息安全技术 服务器安全技术要求和测评准则》；
- 修改了服务器安全等级划分，由原来的五级调整为基本级和增强级（见第 5 章，GB/T 21028—2007 的第 5 章和 GB/T 25063—2010 的第 4 章～第 8 章）；
- 增加了安全功能要求中的固件安全技术要求和对应的测评准则（见 5.1.3 和 6.2.3）；
- 增加了安全功能要求中的自身安全管理安全技术要求和对应的测评准则（见 5.1.6 和 6.2.6）；
- 修改了操作系统安全技术要求（见附录 A，GB/T 21028—2007 的 5.1.1.2、5.2.1.2、5.3.1.2、5.4.1.2、5.5.1.2 和 GB/T 25063—2010 的 4.2、5.2、6.2、7.2）；
- 删除了数据库管理系统的具体安全要求和相应的测评要求（见 GB/T 21028—2007 的 5.1.1.3、5.2.1.3、5.3.1.3、5.4.1.3、5.5.1.3 和 GB/T 25063—2010 的 4.3、5.3、6.3、7.3）；
- 删除了应用系统的具体安全要求和相应的测评要求（见 GB/T 21028—2007 的 5.1.1.4、5.2.1.4、5.3.1.4、5.4.1.4、5.5.1.4 和 GB/T 25063—2010 的 4.4、5.4、6.4、7.4）。

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：浪潮电子信息产业股份有限公司、联想(北京)有限公司、华为技术有限公司、新华三技术有限公司、中国信息通信研究院、蓝盾信息安全技术股份有限公司、中国网络安全审查技术与认证中心、中国电力科学研究院、公安部第三研究所、中国信息安全测评中心、中国电子技术标准化研究院、国家计算机网络与信息安全管理中心、曙光信息产业(北京)有限公司、苏州浪潮智能科技有限公司。

本标准主要起草人：张东、刘刚、李汝鑫、庞婷、万晓兰、张治兵、刘强、申永波、宋桂香、王恩东、赵江、宋好好、孙彦、毛军捷、李凌、严敏辉、葛小宇、杜克宏、雷鸣、王晖、倪平、陆臻、邓雨、张宝峰、孙亚飞、孔玉婷、白欣璐、曹柱、查丽、张天涵。

本标准所代替标准的历次发布版本发布情况为：

- GB/T 21028—2007；
- GB/T 25063—2010。

# 信息安全技术

## 服务器安全技术要求和测评准则

### 1 范围

本标准规定了服务器的安全技术要求和测评准则。

本标准适用于服务器的研制、生产、维护和测评。

### 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/T 9813.3—2017 计算机通用规范 第3部分:服务器

GB/T 20272 信息安全技术 操作系统安全技术要求

GB/T 25069 信息安全技术 术语

### 3 术语、定义和缩略语

#### 3.1 术语和定义

GB/T 9813.3—2017、GB/T 20272 和 GB/T 25069 界定的以及下列术语和定义适用于本文件。

##### 3.1.1

###### **服务器 server**

网络环境下为客户端计算机提供特定应用服务的计算机系统。

注1:计算机系统指服务器硬件系统,主要包含独立计算单元、存储单元、网络传输单元、监控管理单元、供电单元及驱动程序等。

注2:改写 GB/T 9813.3—2017,定义 3.1。

##### 3.1.2

###### **服务器引导固件 server boot firmware**

负责服务器芯片组的初始化和配置,收集、汇总硬件资源信息并引导进入操作系统的程序。

##### 3.1.3

###### **带外管理模块 out-of-band management module**

通过专用物理通道对服务器进行控制管理和维护的独立管理单元。

注:例如 x86 平台的基板管理控制器等。

##### 3.1.4

###### **带外管理模块固件 out-of-band management module firmware**

存在于带外管理模块中,用于实现其功能的程序。

##### 3.1.5

###### **驱动程序 driver program**

为操作系统或应用程序提供操作或控制服务器中特定设备的软件程序。