ICS 35.020
L 09

中华人民共和国国家标准

GB 17859—1999

计算机信息系统
安全保护等级划分准则

Classified criteria for security protection of computer information system

1999-09-13 发布　　2001-01-01 实施

国家质量技术监督局　发布

前　　言

本标准主要有三个目的：一，为计算机信息系统安全法规的制定和执法部门的监督检查提供依据；二，为安全产品的研制提供技术支持；三，为安全系统的建设和管理提供技术指导。

本标准的制定参考了美国的可信计算机系统评估准则(DoD 5200.28-STD)和可信计算机网络系统说明(NCSC-TG-005)。

在本标准文本中，黑体字表示较低等级中没有出现或增强的性能要求。

本标准是计算机信息系统安全保护等级系列标准的第一部分。计算机信息系统安全保护等级系列标准包括以下部分：

计算机信息系统安全等级划分准则；

计算机信息系统安全等级划分准则应用指南；

计算机信息系统安全等级评估准则；

……

本标准的实施应遵循配套国家标准的具体规定。

本标准由中华人民共和国公安部提出并归口。

本标准起草单位：清华大学、北京大学、中国科学院。

本标准主要起草人：胡道元、王立福、卿斯汉、景乾元、那日松、李志鹏、蔡庆明、朱卫国、陈钟。

本标准于2001年1月1日起实施。

本标准委托中华人民共和国公安部负责解释。

中华人民共和国国家标准

计算机信息系统
安全保护等级划分准则

GB 17859—1999

Classified criteria for security protection of computer information system

1 范围

本标准规定了计算机信息系统安全保护能力的五个等级，即：

第一级：用户自主保护级；

第二级：系统审计保护级；

第三级：安全标记保护级；

第四级：结构化保护级；

第五级：访问验证保护级。

本标准适用于计算机信息系统安全保护技术能力等级的划分。计算机信息系统安全保护能力随着安全保护等级的增高，逐渐增强。

2 引用标准

下列标准所包含的条文，通过在本标准中引用而构成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 5271 数据处理词汇

3 定义

除本章定义外，其他未列出的定义见 GB/T 5271。

3.1 计算机信息系统 computer information system

计算机信息系统是由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

3.2 计算机信息系统可信计算基 trusted computing base of computer information system

计算机系统内保护装置的总体，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保护环境并提供一个可信计算系统所要求的附加用户服务。

3.3 客体 object

信息的载体。

3.4 主体 subject

引起信息在客体之间流动的人、进程或设备等。

3.5 敏感标记 sensitivity label

表示客体安全级别并描述客体数据敏感性的一组信息，可信计算基中把敏感标记作为强制访问控制决策的依据。

国家质量技术监督局 1999-09-13 批准　　2001-01-01 实施