ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20009—2019
代替 GB/T 20009—2005

信息安全技术
数据库管理系统安全评估准则

Information security technology—
Security evaluation criteria for database management 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 20009—2005《信息安全技术　数据库管理系统安全评估准则》。与GB/T 20009—2005相比，除编辑性修改外主要技术变化如下：

——修改了第3章术语和定义及缩略语(见3.1和3.2，2005年版第3章)；

——修改了第4章“安全环境”，标题修改为评估总则，描述了数据库管理系统总体要求、评估要求、评估环境和评估流程(见第4章，2005年版第4章)；

——修改了第5章评估内容，按照GB/T 30270—2013定义了GB/T 20273—2019中的安全功能组件和安全保障组件评估内容(见第5章，2005年版第5章)；

——删除了附录A“数据库管理系统面临的威胁和对策”(见2005年版附录A)；

——按照评估保障级概念列出了EAL2、EAL3和EAL4组件列表及评估准则。

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：中国信息安全测评中心、清华大学、北京江南天安科技有限公司、公安部第三研究所、北京大学、武汉达梦数据库有限公司、天津南大通用数据技术股份有限公司。

本标准主要起草人：张宝峰、毕海英、叶晓俊、王峰、王建民、陈冠直、陆臻、沈亮、顾健、宋好好、赵玉洁、吉增瑞、刘昱函、刘学洋、胡文蕙、付铨、方红霞、冯源、李德军。

本标准所代替标准的历次版本发布情况为：

——GB/T 20009—2005。

信息安全技术
数据库管理系统安全评估准则

1 范围

本标准依据 GB/T 20273—2019 规定了数据库管理系统安全评估总则、评估内容和评估方法。

本标准适用于数据库管理系统的测试和评估，也可用于指导数据库管理系统的研发。

注：本标准规定的 EAL2 级、EAL3 级、EAL4 级的评估内容和评估方法既适用于基于 GB/T 18336—2015 所有部分的数据库管理系统安全性测评，同样适用于基于 GB 17859—1999 的数据库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的数据库管理系统安全性测评，相关对应关系参见附录 A 中 A.1。

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(包括所有的修改版)适用于本文件。

GB/T 18336.1～18336.3—2015 信息技术 安全技术 信息技术安全评估准则

GB/T 20273—2019 信息安全技术 数据库管理系统安全技术要求

GB/T 25069—2010 信息安全技术 术语

GB/T 30270—2013 信息技术 安全技术 信息技术安全性评估方法

3 术语和定义、缩略语

3.1 术语和定义

GB/T 25069—2010、GB/T 30270—2013 和 GB/T 20273—2019 界定的术语和定义适用于本文件。

3.2 缩略语

下列缩略语适用于本文件。

CC：通用准则(Common Criteria)

CEM：通用准则评估方法(Common Criteria Evaluation Methodology)

CM：配置管理(Configuration Management)

DBMS：数据库管理系统(DataBase Management System)

EAL：评估保障级(Evaluation Assurance Level)

ETR：评估技术报告(Evaluation Technical Report)

LBAC：基于标签的访问控制(Label Based Access Control)

OR：观察报告(Observation Report)

PP：保护轮廓(Protection Profile)

SFP：安全功能策略(Security Function Policy)

SQL：结构化查询语言(Structured Query Language)

ST：安全目标(Security Target)

TOE：评估对象(Target Of Evaluation)