ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20273—2019
代替 GB/T 20273—2006

信息安全技术
数据库管理系统安全技术要求

Information security technology—
Security technical requirements 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 …… Ⅲ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语、定义和缩略语 …… 1
3.1　术语和定义 …… 1
3.2　缩略语 …… 1
4　评估对象描述 …… 2
4.1　评估对象概述 …… 2
4.2　评估对象安全特性 …… 2
4.3　评估对象部署方式说明 …… 3
5　安全问题定义 …… 3
5.1　数据资产 …… 3
5.2　威胁 …… 4
5.3　组织安全策略 …… 6
5.4　假设 …… 7
6　安全目的 …… 8
6.1　TOE 安全目的 …… 8
6.2　环境安全目的 …… 11
7　安全要求 …… 13
7.1　扩展组件定义 …… 13
7.2　安全功能要求 …… 14
7.3　安全保障要求 …… 26
8　基本原理 …… 39
8.1　安全目的基本原理 …… 39
8.2　安全要求基本原理 …… 47
8.3　组件依赖关系 …… 54
附录 A（资料性附录）　关于标准修订和使用说明 …… 57
参考文献 …… 60

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 20273—2006《信息安全技术　数据库管理系统安全技术要求》，与 GB/T 20273—2006 相比主要技术变化如下：

——修改了“术语和定义”，增加了“缩略语”中的内容（见 3.1 和 3.2，2006 年版的 3.1）；

——增加了安全问题定义、安全目的、扩展组件定义、基本原理（见第 5 章、第 6 章、第 7 章、第 8 章）；

——修改了评估对象描述（见第 4 章，2006 年版的第 4 章）；

——删除了“安全审计”安全功能中提供“潜在侵害分析”“基于异常检测”和“简单攻击探测”的要求（见 2006 年版的第 5 章）；

——删除了“SSODB 自身安全保护”安全功能中提供“SSF 物理安全保护”的要求（见 2006 年版的第 5 章）；

——删除了“SSF 运行安全保护”安全功能中关于与“不可旁路性”“域分离”和“可信恢复”相关的要求（见 2006 年版的第 5 章）；

——删除了安全功能中提供“推理控制”的要求（见 2006 年版的第 5 章）；

——增加了附录 A 关于标准修订和使用说明。

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 20273—2006。

信息安全技术
数据库管理系统安全技术要求

1 范围

本标准规定了数据库管理系统评估对象描述，不同评估保障级的数据库管理系统安全问题定义、安全目的和安全要求，安全问题定义与安全目的、安全目的与安全要求之间的基本原理。

本标准适用于数据库管理系统的测试、评估和采购，也可用于指导数据库管理系统的研发。

注：本标准规定的 EAL2、EAL3、EAL4 级的安全要求既适用于基于 GB/T 18336.1—2015、GB/T 18336.2—2015 和 GB/T 18336.3—2015 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安全性测评，相关对应关系参见附录 A 的 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(包括所有的修改单)适用于本文件。

GB/T 18336.1—2015 信息技术 安全技术 信息技术安全评估准则 第 1 部分：简介和一般模型

GB/T 18336.2—2015 信息技术 安全技术 信息技术安全评估准则 第 2 部分：安全功能组件

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 25069—2010 信息安全技术 术语

GB/T 28821—2012 关系数据管理系统技术要求

3 术语、定义和缩略语

3.1 术语和定义

GB/T 25069—2010、GB/T 18336.1—2015 和 GB/T 28821—2012 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。

ACID：原子性、隔离性、一致性和持久性

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)

IT：信息技术(Information Technology)

JDBC：JAVA 数据库连接(Java DataBase Connectivity)

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

ODBC：开放数据库连接(Open DataBase Connectivity)

PP：保护轮廓(Protection Profile)