



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 发布
中国国家标准化管理委员会

目 次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义、缩略语..... 1

 3.1 术语和定义 1

 3.2 缩略语 1

4 评估总则 2

 4.1 概述 2

 4.2 评估要求 2

 4.3 评估环境 2

 4.4 评估流程 3

5 评估内容 3

 5.1 安全功能评估 3

 5.2 安全保障评估 22

 5.3 评估方法 35

附录 A（资料性附录） 标准修订说明 40

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)

TSC:TSF 控制范围(TSF Scope of Control)
TSF:TOE 安全功能(TOE Security Functionality)
TSFI:TSF 接口(TSF Interface)
TSP:TOE 安全策略(TOE Security Policy)
TSS:TOE 概要规范(TOE Summary Specification)

4 评估总则

4.1 概述

本标准依据 GB/T 30270—2013 给出了 GB/T 20273—2019 定义的数据库管理系统(DBMS)评估对象(TOE)安全功能组件和安全保障组件的评估内容和评估方法。

4.2 评估要求

在对数据库管理系统进行安全评估时,首先依照 GB/T 30270—2013 的安全目标评估方法完成对 DBMS ST 的评估,在此基础上对 DBMS 的安全功能和安全保障进行评估:

- a) 安全功能评估目标是保证 GB/T 20273—2019 定义的安全功能组件设计与实现的完整性和正确性,一般通过对 DBMS 发起者提供的评估证据分析和 TOE 安全功能(TSF)独立性测试,确保 DBMS 安全功能满足其安全目标声称的功能要求。独立性测试应依据数据库产品厂商提供的一系列评估证据(如分析、设计与测试文档)和 TOE 安全策略(TSP),由评估者按照 ST 中的 TSS 对 DBMS 开发者提供的评估对象证据材料进行分析,并按照评估保障级的不同对 DBMS 安全功能组件进行抽样测试,或评估者自己设计相应的测试用例,独立地完成 DBMS 安全功能组件的功能测试,验证 TSF 的实现符合数据库管理系统概要规范。
- b) 安全保障评估目标是发现 DBMS 在设计与实现中的缺陷或脆弱性,以便在评估过程中要求开发者纠正评估对象相应的错误,从而减少 DBMS 在发布后运行过程中安全功能失效发生的可能性。因此安全性评估要求测试人员在模拟真实应用环境下,测试 DBMS 是否能抵御各种安全攻击,以确定该评估对象是否存在潜在的安全弱点或安全漏洞。穿透性测试技术是消除 DBMS 在设计或实现中的缺陷或脆弱性的有效方法。测试人员需依照数据库产品的通信协议、结构化查询语言、数据库开发接口、存储过程/函数等安全攻击面评估证据资料,通过模糊测试等穿透性测试技术对安全功能组件实现机制的可信性进行测试以确保安全功能组件的设计、实现和测试不存在未知的弱点/缺陷。

4.3 评估环境

在不同的网络环境和服务器环境支持下,通用数据库产品提供多种安全策略和安全控制机制的解决方案,以满足评估对象消费者的安全要求。数据库管理系统的测试环境分为 3 类:非集群数据库服务测试环境和集群数据库服务测试环境,集群测试环境又细分为共享存储的集群测试环境和非共享存储的集群测试环境。

应根据 GB/T 30270—2013 安全评估基本原则、过程和规程的体系选择某个测试环境,对数据库产品安全功能和安全保障进行评估。数据库管理系统安全组件的每个评估活动都包含两个通用的评估任务:

- a) 评估证据输入评估:评估发起者应向安全评估机构提供 DBMS 安全评估所有必需的评估材料:评估发起者应按照 GB/T 30270—2013 准备或开发 TOE 相关的评估证据,评估者应对这些输入要求进行评估。
- b) 评估结果输出评估:安全评估机构的输出任务评估的目的是评估输出的观察报告和评估技术

