ICS 35.020
L 09

中华人民共和国国家标准

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—
Data base management systems security evaluation criteria

2005-11-11 发布　　2006-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB 17859—1999《计算机信息系统安全保护等级划分准则》是我国计算机信息系统安全等级管理的重要标准，已于1999年9月13日发布。为促进安全等级管理工作的正常有序开展，特制定一系列相关的标准。本标准是系列标准之一。

本标准文本中，黑体字表示较低等级中没有出现或增强的评估内容。

本标准的附录A中说明数据库管理系统面临的主要威胁和对策。

本标准的附录A是资料性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：北京大学软件工程国家工程中心、东软股份有限公司、公安部公共信息网络安全监察局。

本标准主要起草人：王立福，赵学志，程万军，刘学洋，葛佳。

引　言

数据库管理系统是为数据库的建立、使用和维护而配置的软件。它建立在操作系统的基础上，对数据库进行统一的管理和控制。用户使用的各种数据库命令以及应用程序的执行，都要通过数据库管理系统。数据库管理系统还提供对数据库的维护支持，按照系统管理人员的规定要求，保证数据库的安全性。

数据库管理系统可以帮助不同用户共享一个公共数据集合的软件系统并维护各数据项之间语义上的关联。

数据库管理系统负责在用户应用中存储、格式化、维护和管理用户数据。数据库管理系统通过其内在的功能，以适当的结构来存储数据并通过维护机制来维护这些数据的逻辑关系和完整性，为应用提供一致、完整、安全、可靠的服务。

信息安全技术
数据库管理系统安全评估准则

1 范围

本标准从信息技术方面规定了按照GB 17859—1999的五个安全保护等级对数据库管理系统安全保护等级划分所需要的评估内容。

本标准适用于数据库管理系统的安全保护等级的评估,对于数据库管理系统安全功能的研制、开发和测试亦可参照使用。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 18336.1—2001 信息技术 安全技术 信息技术安全性评估准则 第1部分:简介和一般模型(idt ISO/IEC 15408-1:1999)

3 术语和定义

GB 17859—1999和GB/T 18336.1—2001确立的术语和定义适用于本标准。

4 安全环境

4.1 物理方面

数据库管理系统所处的物理环境是安全的。对数据库管理系统资源的处理限定在一些可控制的访问设备内,防止未授权的物理访问。所有有关安全策略实施的系统硬件和软件受到保护以免于未授权的物理修改。

4.2 人员方面

有一个或多个能胜任的授权用户来管理数据库管理系统和它所包含信息的安全。管理员应经过一定培训,以便能正确有效地建立和维护安全策略。被授权的管理员能严格遵从系统管理员文档的要求进行操作,不会蓄意破坏数据库管理系统,不会蓄意违反操作规程。授权用户具备必要的授权来访问由数据库管理系统管理的最少量的信息。

4.3 连通性方面

数据库管理系统在系统管理员的配置下正常运行,用户可以通过网络远程访问和使用数据库管理系统。授权用户可以获得他们希望得到的适当服务。

5 评估内容

5.1 用户自主保护级

5.1.1 自主访问控制

数据库管理系统安全功能定义和控制系统中命名用户对命名客体的访问。自主访问控制的实施机制允许用户指定和控制客体的共享,并具备限制访问权限扩散的控制能力。自主访问控制机制根据用