ICS 35.040
L 80

中华人民共和国国家标准

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 techniques requirement for database management system

2006-05-31 发布　　2006-12-01 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

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：北京思源新创信息安全资讯有限公司，江南计算技术研究所技术服务中心。

本标准主要起草人：吉增瑞、王志强、陈冠直、陆 晔、孙 炜、景乾元、宋健平。

引　言

本标准用以指导设计者如何设计和实现具有所需要的安全保护等级的数据库管理系统，主要说明为实现 GB 17859—1999 中每一个保护等级的安全要求，数据库管理系统应采取的安全技术措施，以及各安全技术要求在不同安全保护等级中具体实现上的差异。

数据库管理系统是信息系统的重要组成部分，特别是对于存储和管理数据资源的数据服务器是必不可少的。数据库管理系统的主要功能是对数据信息进行结构化组织与管理，并提供方便的检索和使用。当前，常见的数据库结构为关系模式，多以表结构形式表示。数据库管理系统安全就是要对数据库中存储的数据信息进行安全保护，使其免遭由于人为的和自然的原因所带来的泄露、破坏和不可用的情况。大多数的数据库管理系统是以操作系统文件作为建库的基础。所以操作系统安全、特别是文件系统的安全便成为数据库管理系统安全的基础。当然，安全的硬件环境（即物理安全）也是必不可少的。这些显然不在数据库管理系统安全之列。数据库管理系统的安全既要考虑数据库管理系统的安全运行保护，也要考虑对数据库管理系统中所存储、传输和处理的数据信息的保护（包括以库结构形式存储的用户数据信息和以其他形式存储的由数据库管理系统使用的数据信息）。由于攻击和威胁既可能是针对数据库管理系统运行的，也可能是针对数据库管理系统中所存储、传输和处理的数据信息的保密性、完整性和可用性的，所以对数据库管理系统的安全保护的功能要求，需要从系统安全运行和信息安全保护两方面综合进行考虑。根据 GB 17859—1999 所列安全要素及 GB/T 20271—2006 关于信息系统安全功能要素的描述，本标准从身份鉴别、自主访问控制、标记和强制访问控制、数据流控制、安全审计、数据完整性、数据保密性、可信路径、推理控制等方面对数据库管理系统的安全功能要求进行更加具体的描述。通过推理从数据库中的已知数据获取未知数据是对数据库的保密性进行攻击的一种特有方法。推理控制是对这种推理方法的对抗。本标准对较高安全等级的数据库管理系统提出了推理控制的要求，将其作为一个安全要素。为了确保安全功能要素达到所确定的安全性要求，需要通过一定的安全保证机制来实现，根据 GB/T 20271—2006 关于信息系统安全保证要素的描述，本标准从数据库管理系统的 SSODB 自身安全保护、数据库管理系统 SSODB 的设计和实现以及数据库管理系统 SSODB 的安全管理等方面，对数据库管理系统的安全保证要求进行更加具体的描述。

本标准按照 GB 17859—1999 的五个安全等级的划分，对每一个安全等级的安全功能技术要求和安全保证技术要求做详细的描述。在第 4 章对数据库管理系统安全功能基本要求进行简要说明的基础上，第 5 章分别从安全功能技术要求和安全保证技术要求两方面，对数据库管理系统安全技术的分等级要求进行了详细说明。为清晰表示每一个安全等级比较低一级安全等级的安全技术要求的增加和增强，在第 5 章的描述中，每一级的新增部分用“宋体加粗字”表示。

信息安全技术　数据库管理系统安全技术要求

1　范围

本标准依据 GB 17859—1999 的五个安全保护等级的划分，根据数据库管理系统在信息系统中的作用，规定了各个安全等级的数据库管理系统所需要的安全技术要求。

本标准适用于按等级化要求进行的安全数据库管理系统的设计和实现，对按等级化要求进行的数据库管理系统安全的测试和管理可参照使用。

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 20271—2006　信息安全技术　信息系统通用安全技术要求

3　术语、定义和缩略语

3.1　术语和定义

GB 17859—1999 和 GB/T 20271—2006 确立的以及下列术语和定义适用于本标准。

3.1.1

数据库管理系统安全　security of database management system

数据库管理系统所存储、传输和处理的信息的保密性、完整性和可用性的表征。

3.1.2

数据库管理系统安全技术　security technology of database management system

实现各种类型的数据库管理系统安全需要的所有安全技术。

3.1.3

数据库管理系统安全子系统　security subsystem of database management system

数据库管理中安全保护装置的总称，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数据库管理系统安全保护环境，并提供安全数据库管理系统所要求的附加用户服务。

注：按照 GB 17859—1999 对 TCB（可信计算基）的定义，SSODB（数据库管理系统安全子系统）就是数据库管理系统的 TCB。

3.1.4

SSODB 安全策略　SSODB security policy

对 SSODB 中的资源进行管理、保护和分配的一组规则。一个 SSODB 中可以有一个或多个安全策略。

3.1.5

安全功能策略　security function policy

为实现 SSODB 安全要素要求的功能所采用的安全策略。

3.1.6

安全要素　security element

本标准中各安全保护等级的安全技术要求所包含的安全内容的组成成分。