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

GB/T 20273—2006

中华人民共和国
国家标准
信息安全技术
数据库管理系统安全技术要求
GB/T 20273—2006
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.bzcbs.com
电话:68523946　68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 2.75　字数 74 千字
2006年10月第一版　2006年10月第一次印刷
*
书号:155066·1-28088　定价 19.00 元

GB/T 20273-2006

参 考 文 献

[1] 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)

[2] GB/T 18336.2—2001 信息技术 安全技术 信息技术安全性评估准则 第2部分:安全功能要求(idt ISO/IEC 15408-2:1999)

[3] GB/T 18336.3—2001 信息技术 安全技术 信息技术安全性评估准则 第3部分:安全保证要求(idt ISO/IEC 15408-3:1999)

目 次

前言 …… Ⅲ
引言 …… Ⅳ
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 …… 2
4 数据库管理系统安全功能基本要求 …… 2
4.1 身份鉴别 …… 2
4.1.1 用户标识 …… 2
4.1.2 用户鉴别 …… 3
4.2 自主访问控制 …… 3
4.2.1 访问操作 …… 3
4.2.2 访问规则 …… 3
4.2.3 授权传播限制 …… 3
4.3 标记 …… 4
4.3.1 主体标记 …… 4
4.3.2 客体标记 …… 4
4.4 强制访问控制 …… 4
4.4.1 访问控制安全策略 …… 4
4.4.2 访问控制粒度及特点 …… 4
4.5 数据流控制 …… 4
4.6 安全审计 …… 4
4.7 用户数据完整性 …… 4
4.7.1 实体完整性和参照完整性 …… 4
4.7.2 用户定义完整性 …… 5
4.7.3 数据操作的完整性 …… 5
4.8 用户数据保密性 …… 5
4.8.1 存储数据保密性 …… 5
4.8.2 传输数据保密性 …… 5
4.8.3 客体重用 …… 5
4.9 可信路径 …… 5
4.10 推理控制 …… 5
5 数据库管理系统安全技术分等级要求 …… 5
5.1 第一级:用户自主保护级 …… 5
5.1.1 安全功能 …… 5
5.1.2 SSODB自身安全保护 …… 6
5.1.3 SSODB设计和实现 …… 7

5.1.4 SSODB 安全管理 …… 8
5.2 第二级:系统审计保护级 …… 8
5.2.1 安全功能 …… 8
5.2.2 SSODB 自身安全保护 …… 9
5.2.3 SSODB 设计和实现 …… 10
5.2.4 SSODB 安全管理 …… 12
5.3 第三级:安全标记保护级 …… 12
5.3.1 安全功能 …… 12
5.3.2 SSODB 自身安全保护 …… 14
5.3.3 SSODB 设计和实现 …… 15
5.3.4 SSODB 安全管理 …… 18
5.4 第四级:结构化保护级 …… 18
5.4.1 安全功能 …… 18
5.4.2 SSODB 自身安全保护 …… 20
5.4.3 SSODB 设计和实现 …… 21
5.4.4 SSODB 安全管理要求 …… 24
5.5 第五级:访问验证保护级 …… 24
5.5.1 安全功能 …… 24
5.5.2 SSODB 自身安全保护 …… 26
5.5.3 SSODB 设计和实现 …… 28
5.5.4 SSODB 安全管理 …… 31
附录 A(资料性附录) 标准概念说明 …… 32
A.1 组成与相互关系 …… 32
A.2 数据库管理系统安全的特殊要求 …… 32
A.3 数据库管理系统的用户管理 …… 33
A.4 数据库管理系统的安全性 …… 33
A.5 数据库管理系统安全保护等级的划分 …… 33
A.6 关于数据库管理系统中的主体与客体 …… 33
A.7 关于 SSODB、SSF、SSP、SFP 及其相互关系 …… 33
A.8 关于推理控制 …… 34
A.9 关于密码技术和数据库加密 …… 35
参考文献 …… 36

检测所有的推理问题是很难的。比较可行的办法是:

——对数据重新分级;

——对约束重新分级。

A.9 关于密码技术和数据库加密

密码技术已成为当今信息系统安全保护的关键技术,在较高安全保护等级中所采用的安全策略,必须以密码技术作为构成信息安全保护的重要机制,或将密码技术与系统安全技术相结合,组成统一的安全机制。数据库管理系统中密码技术的主要应用领域包括关键信息的存储加密保护和传输加密保护,以及以 PKI 为基础的 CA 认证系统实现对用户身份和设备的真实性的鉴别。各个安全保护等级密码技术的具体配置由国家密码主管部门决定。