



# 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

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](http://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

如有印装差错 由本社发行中心调换  
版权专有 侵权必究  
举报电话:(010)68533533



GB/T 20273-2006

## 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。

## 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

# 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物。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。

## 3.1.7

**SSODB 安全功能 SSODB security function**

正确实施 SSODB 安全策略的全部硬件、固件、软件所提供的功能。每一个安全策略的实现,组成一个 SSODB 安全功能模块。一个 SSODB 的所有安全功能模块共同组成该 SSODB 的安全功能。

## 3.1.8

**SSF 控制范围 SSF scope of control**

SSODB 的操作所涉及的主体和客体的范围。

## 3.1.9

**数据完整性 data integrity**

数据完整性泛指数据库中数据的正确性和一致性,包括实体完整性、参照完整性和用户定义完整性。

## 3.1.10

**实体完整性 body integrity**

关系模型中的实体完整性是指关系表中字段级的完整性,即数据类型及取值的合理性。实体完整性规则要求,数据库中表示的任一实体是可区分的。对于关系模型,实体完整性表现为关系的主属性(基本键:主键/主码)不能是空值(NULL),也不能是重复值,即基本键的各个分量都不能为空。

## 3.1.11

**参照完整性 reference integrity**

关系模型中的参照完整性是指主码值和外码值表间的一致性。参照完整性规则要求,在任一时刻,如果关系 R1 的某些属性是关于关系 R2 的外键,则该外键的值必须是 R2 中某元组的主键值或为“空值”(空值意味着“不知道”的信息和“无意义”的信息)。参照完整性规则是“连接”关系运算正确执行的前提。

## 3.1.12

**用户定义完整性 user defined integrity**

关系模型中的用户定义完整性是指字段与表之间的断言关系(即业务规则)的正确性,也就是根据业务规则(比如价格的有效范围等)所确定的完整性约束。系统提供定义和检查用户定义完整性规则的机制,其目的是用统一的方式由系统处理,而不是由应用程序完成,这样不仅可以简化应用程序,还提高了完整性保证的可靠性。

## 3.2 缩略语

下列缩略语适用于本标准:

SFP	安全功能策略	security function policy
SSC	SSF 控制范围	SSF scope of control
SSF	SSODB 安全功能	SSODB security function
SSODB	数据库管理系统安全子系统	security subsystem of database management system
SSP	SSODB 安全策略	SSODB security policy

## 4 数据库管理系统安全功能基本要求

## 4.1 身份鉴别

## 4.1.1 用户标识

应对注册到数据库管理系统中的用户进行标识。用户标识信息是公开信息,一般以用户名和用户 ID 实现。为了管理方便,可将用户分组,也可使用别名。无论用户名、用户 ID、用户组还是用户别名,都要遵守标识的唯一性原则。用户标识分为:

- a) 基本标识:应在 SSF 实施所要求的动作之前,先对提出该动作要求的用户进行标识;



- b) 唯一性标识:应确保所标识用户在信息系统生存周期内的唯一性,并将用户标识与审计相关联;
- c) 标识信息管理:应对用户标识信息进行管理、维护,确保其不被非授权地访问、修改或删除。

#### 4.1.2 用户鉴别

应对登录到数据库管理系统的用户进行身份真实性鉴别。通过对用户所提供的“鉴别信息”的验证,证明该用户确有所声称的某种身份,这些“鉴别信息”必须是保密的,不易伪造的。用户鉴别分为:

- a) 基本鉴别:应在 SSF 实施所要求地动作之前,先对提出该动作要求的用户成功地进行鉴别。
- b) 不可伪造鉴别:应检测并防止使用伪造或复制的鉴别数据。一方面,要求 SSF 应检测或防止由任何别的用户伪造的鉴别数据,另一方面,要求 SSF 应检测或防止当前用户从任何其他用户处复制的鉴别数据的使用。
- c) 一次性使用鉴别:应能提供一次性使用鉴别数据操作的鉴别机制,即 SSF 应防止与已标识过的鉴别机制有关的鉴别数据的重用。
- d) 多机制鉴别:应能提供不同的鉴别机制,用于鉴别特定事件的用户身份,并且 SSF 应根据所描述的多种鉴别机制如何提供鉴别的规则,来鉴别任何用户所声称的身份。
- e) 重新鉴别:应有能力规定需要重新鉴别用户的事件,即 SSF 应在需要重鉴别的条件表所指示的条件下,重新鉴别用户。例如,用户终端操作超时被断开后,重新连接时需要进行重鉴别。

### 4.2 自主访问控制

#### 4.2.1 访问操作

应由数据库子语言定义,并与数据一起存放在数据字典中。对任何 SQL 对象进行操作应有明确的权限许可,并且权限随着操作和对象的变化而变化,安全系统应有能力判断这种权限许可。操作与对象紧密相联,即把“操作+对象”作为一个授权。表 1 是 GRANT(授权)语句对象类型与相关操作的举例。

表 1 GRANT 语句的对象类型与相关操作

对 象	操 作
基本表	SELECT、INSERT、UPDATE、DELETE、TRIGGER、REFERENCES
视图	SELECT、INSERT、UPDATE、DELETE、REFERENCES
列	SELECT、INSERT、UPDATE、REFERENCES
域	USAGE
字符集	USAGE
排序	USAGE
转换	USAGE
SQL 调用	EXECUTE
UDT	UNDER

表中,除 USAGE 和 UNDER 外,其余操作均符合 SQL 语句中使用的动词。

#### 4.2.2 访问规则

应以访问控制表或访问矩阵的形式表示,并通过执行相应的访问控制程序实现。每当执行 SQL 语句、有访问要求出现时,通过调用相应的访问控制程序,实现对访问要求的控制。

#### 4.2.3 授权传播限制

应限制具有某一权限的用户将该权限传给其他用户。当一个用户被授予某权限,同时拥有将该权限授予其他用户的权力时,该用户才拥有对该授权的传播权。为了增强数据库系统的安全性,需要对授权传播进行某些限制。

### 4.3 标记

#### 4.3.1 主体标记

SSF 应为主体指定敏感标记,这些敏感标记是等级分类和非等级类别的组合,是实施强制访问控制的依据。

#### 4.3.2 客体标记

SSF 应为客体指定敏感标记,这些敏感标记是等级分类和非等级类别的组合,是实施强制访问控制的依据。

### 4.4 强制访问控制

#### 4.4.1 访问控制安全策略

应采用确定的安全策略模型实现强制访问控制。当前常用的安全策略模型是多级安全模型。该模型将 SSODB 安全控制范围内的所有主、客体成分通过标记设置敏感标记。并按简单保密性原则确定的规则——从下读、向上写,根据访问者主体和被访问者客体的敏感标记,实现主、客体之间每次访问的强制性控制。根据数据库管理系统的运行环境的不同,强制访问控制分为:

- a) 在单一计算机系统中或网络环境的多机系统上运行的单一数据库管理系统,访问控制所需的敏感标记存储在统一的数据库字典中,使用单一的访问规则实现;
- b) 在网络环境的多机系统上运行的分布式数据库系统,全局应用的强制访问控制应在全局 DBMS 层实现,局域应用的强制访问控制应在局部 DBMS 层实现。其所采用的访问规则是一致的。

#### 4.4.2 访问控制粒度及特点

应根据数据库特点和不同安全保护等级的不同要求,实现不同粒度的访问控制。这些特点主要是:

- a) 数据以特定结构格式存放,客体的粒度可以是:关系数据库的表、视图、元组(记录)、列(字段)、元素(每个元组的字段)、日志、片段、分区、快照、约束和规则、DBMS 核心代码、用户应用程序、存储过程、触发器、各种访问接口等;
- b) 数据库系统有完整定义的访问操作,如表 1 所示;
- c) 数据库是数据与逻辑的统一,数据库中不仅存放了数据,还存放了大量的用于管理和使用这些数据的程序,这些程序和数据同样需要进行保护,以防止未经授权的使用、篡改、增加或破坏;
- d) 数据库中的三级结构(物理结构、逻辑结构、概念模型结构)和两种数据独立性(物理独立性、逻辑独立性)大大减轻数据库应用程序的维护工作量,但是由于不同的逻辑结构可能对应于相同的物理结构,给访问控制带来新的问题,应对访问规则进行一致性检查;
- e) 分布式数据库管理系统中,全局应用的访问控制应在全局 DBMS 层实现,局部应用的访问控制应在局部 DBMS 层实现,并根据需要各自选择不同的访问控制策略。

### 4.5 数据流控制

在以数据流方式实现数据流动的数据库管理系统中,应采用数据流控制机制实现对数据流动的控制,以防止具有高等级安全的数据信息向低等级的区域流动。

### 4.6 安全审计

数据库管理系统的安全审计应:

- a) 建立独立的安全审计系统;
- b) 定义与数据库安全相关的审计事件;
- c) 设置专门的安全审计员;
- d) 设置专门用于存储数据库系统审计数据的安全审计库;
- e) 提供适用于数据库系统的安全审计设置、分析和查阅的工具。

### 4.7 用户数据完整性

#### 4.7.1 实体完整性和参照完整性

- a) 数据库管理系统应确保数据库中的用户数据具有实体完整性和参照完整性。关系之间的参照

完整性规则是“连接”关系运算正确执行的前提。

- b) 用户定义基本表时,应说明主键、外键,被引用表、列和引用行为。当数据录入、更新、删除时,应由数据库管理系统根据说明自动维护实体完整性和参照完整性。

#### 4.7.2 用户定义完整性

- a) 数据库管理系统应提供支持用户定义完整性的功能。系统应提供定义和检查用户定义完整性规则的机制,其目的是用统一的方式由系统处理,而不是由应用程序完成,从而不仅可以简化应用程序,还提高了完整性保证的可靠性。
- b) 数据库管理系统应支持为约束或断言命名(或提供默认名称),定义检查时间、延迟模式或设置默认检查时间和延迟模式,支持约束和断言的撤消。

#### 4.7.3 数据操作的完整性

数据操作的完整性约束为:

- a) 用户定义基本表时应定义主键和外键;
- b) 对于候选键,应由用户指明其唯一性;
- c) 对于外键,用户应指明被引用关系和引用行为;
- d) 应由数据库管理系统检查对主键、外键、候选键数据操作是否符合完整性要求,不允许提交任何违反完整性的事务;
- e) 删除或更新某元组时,数据库管理系统应检查该元组是否含有外键,若有,应根据用户预定义的引用行为进行删除。

### 4.8 用户数据保密性

#### 4.8.1 存储数据保密性

数据库管理系统应确保数据库中存储的用户数据的保密性。

#### 4.8.2 传输数据保密性

数据库管理系统应确保数据库中传输的用户数据的保密性。

#### 4.8.3 客体重用

数据库管理系统大量使用的动态资源,多由操作系统分配。实现客体安全重用的操作系统和数据库管理系统应满足以下要求:

- a) 数据库管理系统提出资源分配要求,如创建新库、数据库设备初始化等,所得到的资源不应包含该客体以前的任何信息内容;
- b) 数据库管理系统提出资源索回要求,应确保这些资源中的全部信息被清除;
- c) 数据库管理系统要求创建新的数据库用户进程,应确保分配给每个进程的资源不包含残留信息;
- d) 数据库管理系统应确保已经被删除或被释放的信息不再是可用的。

#### 4.9 可信路径

在数据库用户进行注册或进行其他安全性操作时,应提供 SSODB 与用户之间的可信通信通路,实现用户与 SSF 间的安全数据交换。

#### 4.10 推理控制

应采用推理控制的方法防止数据库中的用户数据被非授权地获取。运用推理方法获取权限以外的数据库信息,是一种较为隐蔽的信息攻击方法。在具有较高安全级别要求的数据库系统中,应考虑对这种攻击的防御。

### 5 数据库管理系统安全技术分等级要求

#### 5.1 第一级:用户自主保护级

##### 5.1.1 安全功能

### 5.1.1.1 身份鉴别

身份鉴别包括对用户的身份进行标识和鉴别。可根据 4.1 的描述,按 GB/T 20271—2006 中 6.1.3.1 的要求,从以下方面设计和实现数据库管理系统的身份鉴别功能:

- a) 对进入数据库管理系统的用户进行身份标识,根据 4.1.1 的描述,按以下要求设计:
  - 凡需进入数据库管理系统的用户,应先进行标识(建立账号);
  - 数据库管理系统用户标识一般使用用户名和用户标识符(UID)。
- b) 对登录到数据库管理系统的用户身份的真实性进行鉴别,根据 4.1.2 的描述,按以下要求设计:
  - 采用口令进行鉴别,并在每次用户登录系统时进行鉴别;
  - 口令应是不可见的,并在存储时有安全保护;
  - 通过对不成功的鉴别尝试的值(包括尝试次数和时间的阈值)进行预先定义,并明确规定达到该值时应采取的措施来实现鉴别失败的处理。
- c) 对注册到数据库管理系统的用户,应按以下要求设计和实现用户—主体绑定功能:
  - 将用户进程与所有者用户相关联,使用户进程的行为可以追溯到进程的所有者用户;
  - 将系统进程动态地与当前服务要求者用户相关联,使系统进程的行为可以追溯到当前服务的要求者用户。

### 5.1.1.2 自主访问控制

可根据 4.2 中访问操作、访问规则和授权传播的描述,按 GB/T 20271—2006 中 6.1.3.2 的要求,设计和实现数据库管理系统的自主访问控制功能,允许命名用户以用户和/或用户组的身份规定并控制对客体的访问,并阻止非授权用户对客体的访问。

### 5.1.1.3 用户数据完整性

可根据 4.7 的描述,按 GB/T 20271—2006 中 6.1.3.3 的要求,从以下方面设计和实现数据库管理系统的用户数据完整性功能:

- a) 对数据库管理系统内部传输的用户数据,如进程间的通信,应提供保证数据完整性的功能;
- b) 对数据库管理系统中处理的用户数据,可根据 4.7.1、4.7.2、4.7.3 的描述,按 GB/T 20271—2006 中 6.1.3.3 的要求实现实体完整性、参照完整性和用户定义完整性,按回退的要求设计相应的 SSODB 安全功能模块,进行异常情况的事务回退,以确保数据的完整性。

## 5.1.2 SSODB 自身安全保护

### 5.1.2.1 SSF 物理安全保护

按 GB/T 20271—2006 中 6.1.4.1 的要求,实现 SSF 的物理安全保护,通过对物理安全的检查,发现以物理方式的攻击对 SSF 造成的威胁和破坏。

### 5.1.2.2 SSF 运行安全保护

按 GB/T 20271—2006 中 6.1.4.2 的要求,从以下方面 SSF 的运行安全保护:

- a) 系统在设计时不应留有“后门”。即不应以维护、支持或操作需要为借口,设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口。
- b) 安全结构应是一个独立的、严格定义的系统软件的一个子集,并应防止外部干扰和破坏,如修改其代码或数据结构。
- c) 应提供设置和升级配置参数的安装机制。在初始化和对与安全有关的数据结构进行保护之前,应对用户和管理员的安全策略属性进行定义。
- d) 在 SSODB 失败或中断后,应确保其以最小的损害得到恢复,并按照失败保护中所描述的内容,实现对 SSF 出现失败时的处理。

### 5.1.2.3 SSF 数据安全保护

按 GB/T 20271—2006 中 6.1.4.3 的要求,对在 SSODB 内传输的 SSF 数据,实现 SSODB 内 SSF

数据传输的基本保护。

#### 5.1.2.4 资源利用

按 GB/T 20271—2006 中 6.1.4.4 的要求,从以下方面实现 SSODB 的资源利用:

- a) 通过一定措施确保当系统出现某些确定的故障时,SSF 也能维持正常运行;
- b) 采取适当的策略,按有限服务优先级提供主体使用 SSC 内某个资源子集的优先级,进行 SSODB 资源的管理和分配;
- c) 按资源分配中最大限额的要求,进行 SSODB 资源的管理和分配,确保用户和主体不会独占某种受控资源。

#### 5.1.2.5 SSODB 访问控制

按 GB/T 20271—2006 中 6.1.4.5 的要求,从以下方面实现 SSODB 的访问控制:

- a) 按会话建立机制,对会话建立的管理进行设计;
- b) 按多重并发会话限定中基本限定的要求,进行会话管理的设计。在基于基本标识的基础上,SSF 应限制系统的并发会话的最大数量,并应利用默认值作为会话次数的限定数;
- c) 按可选属性范围限定的要求,选择某种会话安全属性的所有失败的尝试,对用来建立会话的安全属性的范围进行限制。

### 5.1.3 SSODB 设计和实现

#### 5.1.3.1 配置管理

按 GB/T 20271—2006 中 6.1.5.1 的要求,实现 SSODB 基本的配置管理能力,即要求开发者所使用的版本号与所表示的 SSODB 样本完全对应。

#### 5.1.3.2 分发和操作

按 GB/T 20271—2006 中 6.1.5.2 的要求,从以下方面实现数据库管理系统的 SSODB 分发和操作:

- a) 应以文档形式提供对 SSODB 安全地进行分发的过程,并对安装、生成和启动的过程进行说明,并最终生成安全的配置。文档中所描述的内容应包括:
  - 提供分发的过程;
  - 安全启动和操作的过程。
- b) 对系统的未授权修改的风险,应在交付时控制到最低限度。包装及安全分送和安装过程中的安全性由末端用户确认,所有安全机制都应以功能状态交付。
- c) 所有软件应提供安全安装默认值,使安全机制有效地发挥安全作用。
- d) 随同系统交付的全部默认用户标识码,应在交付时处于非激活状态,并在使用前由管理员激活。
- e) 用户文档应同交付的软件一起包装,并应有一套规程确保当前送给用户的软件是严格按照最新的版本制作的。

#### 5.1.3.3 开发

按 GB/T 20271—2006 中 6.1.5.3 的要求,从以下方面进行 SSODB 的开发:

- a) 按非形式化功能说明、描述性高层设计、SSF 子集实现、SSF 内部结构模块化、描述性低层设计和非形式化对应性说明的要求,进行 SSODB 的设计;
- b) 系统的设计和开发应保护数据的完整性,例如,检查数据更新的规则,多重输入的正确处理,返回状态的检查,中间结果的检查,合理值输入检查,事务处理更新的正确性检查等;
- c) 在内部代码检查时,应解决潜在的安全缺陷,关闭或取消所有的后门;
- d) 交付的软件和文档,应进行关于安全缺陷的定期的和书面的检查,并将检查结果告知用户;
- e) 由系统控制的敏感数据,如口令、密钥等,不应在未受保护的程序或文档中以明文形式存储;
- f) 应以书面形式提供给用户关于软件所有权法律保护的指南。

#### 5.1.3.4 文档要求

按 GB/T 20271—2006 中 6.1.5.4 的要求,从以下方面编制 SSODB 的文档:

- a) 用户文档应提供关于不同用户的可见的安全机制以及如何利用它们的信息,并说明它们的用途和提供有关它们使用的指南;
- b) 安全管理员文档应提供有关如何设置、维护和分析系统安全的详细指导,以及与安全有关的管理员功能的详细描述,包括增加和删除一个用户、改变主、客体的安全属性等;
- c) 文档中不应提供任何一旦泄露将会危及系统安全的信息。有关安全的指令和文档应划分等级分别提供给用户、数据库系统管理员和系统安全员。这些文档应为独立的文档,或作为独立的章节插入到管理员指南和用户指南中。

#### 5.1.3.5 生存周期支持

按 GB/T 20271—2006 中 6.1.5.5 的要求,从以下方面实现 SSODB 的生存周期支持:

- a) 按开发者定义生存周期模型进行 SSODB 开发;
- b) 文档应详细阐述安全启动和操作的过程,详细说明安全功能在启动、正常操作维护时是否能被撤消或修改,说明在故障或系统出错时如何恢复系统至安全状态。

#### 5.1.3.6 测试

按 GB/T 20271—2006 中 6.1.5.6 的要求,从以下方面对 SSODB 进行测试:

- a) 通过一般功能测试和相符独立性测试,确认 SSODB 的功能与所要求功能的一致性;
- b) 所有系统的安全特性,应被全面测试;
- c) 所有发现的漏洞应被改正、消除或使其无效,并在消除漏洞后重新测试,以证实它们已被消除,且没有引出新的漏洞;
- d) 应提供测试文档,详细描述测试计划、测试过程、测试结果。

#### 5.1.4 SSODB 安全管理

按 GB/T 20271—2006 中 6.1.6 的要求,实现 SSODB 的安全管理,对 SSODB 的访问控制、鉴别控制、审计等相关的功能,以及与一般的安装、配置等有关的功能,制定相应的操作、运行规程和行为规范制度。

### 5.2 第二级:系统审计保护级

#### 5.2.1 安全功能

##### 5.2.1.1 身份鉴别

身份鉴别包括对用户的身份进行标识和鉴别。根据 4.1 的描述,按 GB/T 20271—2006 中 6.2.3.1 的要求,从以下方面设计和实现数据库管理系统的身份鉴别功能:

- a) 应对进入数据库管理系统的用户进行身份标识,根据 4.1.1 的描述,按以下要求设计:
  - 凡需进入数据库管理系统的用户,应先进行标识(建立账号);
  - 数据库管理系统用户标识一般使用用户名和用户标识符(UID),并在数据库管理系统的整个生存周期实现用户的唯一性标识,以及用户名或别名、UID 等之间的一致性。
- b) 应对登录到数据库管理系统的用户身份的真实性进行鉴别,根据 4.1.2 的描述,按以下要求设计:
  - 采用强化管理的口令鉴别/基于令牌的动态口令鉴别等机制进行身份鉴别,并在每次用户登录系统时进行鉴别;
  - 鉴别信息应是不可见的,并在存储和传输时有安全保护;
  - 通过对不成功的鉴别尝试的值(包括尝试次数和时间的阈值)进行预先定义,并明确规定达到该值时应采取的措施来实现鉴别失败的处理。
- c) 对注册到数据库管理系统的用户,应按以下要求设计和实现用户-主体绑定功能:
  - 将用户进程与所有者用户相关联,使用户进程的行为可以追溯到进程的所有者用户;



——将系统进程动态地与当前服务要求者用户相关联,使系统进程的行为可以追溯到当前服务的要求者用户。

#### 5.2.1.2 自主访问控制

根据 4.2 中访问操作、访问规则和授权传播的描述,按照 GB/T 20271—2006 中 6.2.3.2 的要求,从以下方面设计和实现数据库管理系统的自主访问控制功能:

- a) 允许命名用户以用户的身份规定并控制对客体的访问,并阻止非授权用户对客体的访问;
- b) 用目录表访问控制、存取控制表访问控制、能力表访问控制等访问控制表访问控制确定主体对客体的访问权限;
- c) 自主访问控制主体的粒度应是用户级,客体的粒度应是表级和/或记录、字段级;
- d) 自主访问控制应与身份鉴别和审计相结合,通过确认用户身份的真实性和记录用户的各种成功的或不成功的访问,使用户对自己的行为承担明确的责任。

#### 5.2.1.3 安全审计

根据 4.6 的描述,按 GB/T 20271—2006 中 6.2.2.3 的要求,设计安全审计功能。本安全保护等级要求:

- a) 安全审计功能的设计应与用户标识与鉴别、自主访问控制等安全功能的设计紧密结合;
- b) 提供审计日志,潜在侵害分析,基本审计查阅和有限审计查阅,安全审计事件选择,以及受保护的审计踪迹存储等功能;
- c) 能够生成、维护及保护审计过程,使其免遭修改、非法访问及破坏,特别要保护审计数据,要严格限制未经授权的用户访问;
- d) 能够创建并维护一个对受保护客体访问的审计踪迹,保护审计记录不被未授权的访问、修改和破坏。

#### 5.2.1.4 用户数据完整性

根据 4.7 的描述,按 GB/T 20271—2006 中 6.2.3.3 的要求,从以下方面设计和实现数据库管理系统的用户数据完整性功能:

- a) 在对数据进行访问操作时,检查以库结构形式存储在数据库中的用户数据是否出现完整性错误;
- b) 对数据库管理系统内部传输的用户数据,如进程间的通信,应提供保证数据完整性的功能;
- c) 对数据库管理系统中处理的用户数据,根据 4.7.1、4.7.2、4.7.3 的描述,按照 GB/T 20271—2006 中 6.2.3.5 的要求实现实体完整性、参照完整性和用户定义完整性,按回退的要求设计相应的 SSODB 安全功能模块,进行异常情况的事务回退,以确保数据的完整性。

#### 5.2.1.5 用户数据保密性

根据 4.8.1、4.8.2 和 4.8.3 中 a) 的描述,按 GB/T 20271—2006 中 6.2.3.4 的要求,设计和实现数据库管理系统的用户数据保密性保护功能。

### 5.2.2 SSODB 自身安全保护

#### 5.2.2.1 SSF 物理安全保护

按 GB/T 20271—2006 中 6.2.4.1 的要求,实现 SSF 的物理安全保护,通过对物理攻击的检查,发现以物理方式的攻击对 SSF 造成的威胁和破坏。

#### 5.2.2.2 SSF 运行安全保护

按 GB/T 20271—2006 中 6.2.4.2 的要求,从以下方面实现 SSF 的运行安全保护:

- a) 系统在设计时不应留有“后门”。即不应以维护、支持或操作需要为借口,设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口;
- b) 安全结构应是一个独立的、严格定义的系统软件的一个子集,并应防止外部干扰和破坏,如修改其代码或数据结构;

- c) 应提供设置和升级配置参数的安装机制,在初始化和对与安全有关的数据结构进行保护之前,应对用户和管理员的安全策略属性进行定义;
- d) 当数据库管理系统安装完成后,在普通用户访问之前,系统应配置好初始用户和管理员职责、审计参数、系统审计跟踪设置以及对客体的合适的访问控制;
- e) 在 SSODB 失败或中断后,应保护其以最小的损害得到恢复,并按照失败保护中所描述的内容,实现对 SSF 出现失败时的处理。

#### 5.2.2.3 SSF 数据安全保护

按 GB/T 20271—2006 中 6.2.4.3 的要求,对在 SSODB 内传输的 SSF 数据进行以下安全保护:

- a) 实现 SSODB 内 SSF 数据传输的基本保护;
- b) SSODB 内 SSF 数据复制的一致性保护。

#### 5.2.2.4 资源利用

按 GB/T 20271—2006 中 6.2.4.4 的要求,从以下方面实现 SSODB 的资源利用:

- a) 通过一定措施确保当系统出现某些确定的故障时,SSF 也能维持正常运行;
- b) 采取适当的策略,按有限服务优先级提供主体使用 SSC 内某个资源子集的优先级,进行 SSODB 资源的管理和分配;
- c) 按资源分配中最大限额的要求,进行 SSODB 资源的管理和分配,确保用户和主体不会独占某种受控资源;
- d) 确保在被授权的主体发出请求时,资源能被访问和利用;
- e) 当系统资源的服务水平降低到预先规定的最小值时,应能检测和报警。

#### 5.2.2.5 SSODB 访问控制

按 GB/T 20271—2006 中 6.2.4.5 的要求,从以下方面实现 SSODB 的访问控制:

- a) 按会话建立机制的要求,对会话建立的管理进行设计。在建立 SSODB 会话之前,应鉴别用户的身份。登录机制不允许鉴别机制本身被旁路。
- b) 按多重并发会话限定中基本限定的要求,进行会话管理的设计。在基于基本标识的基础上,SSF 应限制系统的并发会话的最大数量,并应利用默认值作为会话次数的限定数。
- c) 按可选属性范围限定的要求,选择某种会话安全属性的所有失败的尝试,对用来建立会话的安全属性的范围进行限制。
- d) 成功登录系统后,SSODB 应记录并向用户显示以下数据:
  - 日期、时间、来源和上次成功登录系统的情况;
  - 上次成功访问系统以来身份鉴别失败的情况;
  - 应显示口令到期的天数;
  - 成功或不成功的事件次数的显示可以用整数计数、时间戳列表等表述方法。

### 5.2.3 SSODB 设计和实现

#### 5.2.3.1 配置管理

按 GB/T 20271—2006 中 6.2.5.1 的要求,从以下方面实现 SSODB 的配置管理:

- a) 在配置管理能力方面应实现对版本号、配置项、授权控制等方面的管理要求。
- b) 配置管理范围方面,应将 SSODB 的实现表示、设计文档、测试文档、用户文档、管理员文档以及配置管理文档等置于配置管理之下。
- c) 在系统的整个生存期,即在它的开发、测试和维护期间,只有被授权的代码和代码修改才允许被加进已交付的源码的基本部分。所有改变应被记载和检查,以确保不危及系统的安全。通过技术、物理和保安规章三方面的结合,充分保护生成系统所用到的源码免遭未授权的修改和毁坏。在软件配置管理系统中,应包含以下方面的工具规程:
  - 从源码产生出系统新版本;



- 鉴定新生成的系统版本；
- 保护源码免遭未授权修改。

### 5.2.3.2 分发和操作

按 GB/T 20271—2006 中 6.2.5.2 的要求,从以下方面实现 SSODB 的分发和操作:

- a) 应以文档形式提供对 SSODB 安全地进行分发的过程,并对安装、生成和启动的过程进行说明,最终生成安全的配置。文档中所描述的内容应包括:
  - 提供分发的过程;
  - 安全启动和操作的过程;
  - 建立日志的过程。
- b) 对系统的未授权修改的风险,应在交付时控制到最低限度。包装及安全分送和安装过程中的安全性由末端用户确认,所有安全机制都应以功能状态交付。
- c) 所有软件应提供安全安装默认值,使安全机制有效地发挥安全功能。
- d) 随同系统交付的全部默认用户标识码,在交付时处于非激活状态,并在使用前由管理员激活。
- e) 用户文档应同交付的软件一起包装,并应有一套规程确保当前送给用户的软件是严格按照最新的版本制作的。

### 5.2.3.3 开发

按 GB/T 20271—2006 中 6.2.5.3 的要求,从以下方面进行 SSODB 的开发:

- a) 按非形式化安全策略模型、完全定义的外部接口、描述性高层设计、SSF 子集实现、SSF 内部结构层次化、描述性低层设计、非形式化对应性说明的要求,进行 SSODB 的设计;
- b) 系统的设计和开发应保护数据的完整性,例如,检查数据更新的规则,多重输入的正确处理,返回状态的检查,中间结果的检查,合理值输入检查,事务处理更新的正确性检查等;
- c) 在内部代码检查时,应解决潜在的安全缺陷,关闭或取消所有的后门;
- d) 交付的软件和文档,应进行关于安全缺陷的定期的和书面的检查,并将检查结果告知用户;
- e) 由系统控制的敏感数据,如口令、密钥等,不应在未受保护的程序或文档中以明文形式存储;
- f) 应以书面形式提供给用户关于软件所有权法律保护的指南。

### 5.2.3.4 文档要求

按 GB/T 20271—2006 中 6.2.5.4 的要求,从以下方面编制 SSODB 文档:

- a) 用户文档应提供关于不同用户的可见的安全机制以及如何利用它们的信息,并说明它们的用途和提供有关它们使用的指南。
- b) 安全管理员文档应提供有关如何设置、维护和分析系统安全的详细指导,包括当运行一个安全设备时,需要控制的有关功能和特权的警告,以及与安全有关的管理员功能的详细描述,包括增加和删除一个用户、改变主、客体的安全属性等。
- c) 文档中不应提供任何一旦泄露将会危及系统安全的信息。有关安全的指令和文档应划分等级分别提供给用户、数据库系统管理员和系统安全员。这些文档应为独立的文档,或作为独立的章节插入到管理员指南和用户指南中。文档也可为硬拷贝、电子文档或联机文档。如果是联机文档应控制对其的访问。
- d) 应提供关于所有审计工具的文档,包括为检查和保持审计文件所推荐的过程、针对每种审计事件的详细审计记录文件、为周期性备份和删除审计记录所推荐的过程等。
- e) 应提供如何进行系统自我评估的章节(带有网络管理、口令要求、拨号访问控制、意外事故计划的安全报告)和为灾害恢复计划所做的建议,以及描述普通入侵技术和其他威胁及查出及阻止的方法。

### 5.2.3.5 生存周期支持

按 GB/T 20271—2006 中 6.2.5.5 的要求,从以下方面实现 SSODB 的生存周期支持: