ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25062—2010

信息安全技术　鉴别与授权　基于角色的访问控制模型与管理规范

Information security technology—Authentication and authorization—Role-based access control model and management specification

2010-09-02 发布　　2011-02-01 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、附录B和附录C为资料性附录。

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:中国科学院软件研究所,信息安全共性技术国家工程研究中心。

本标准主要起草人:冯登国、徐震、翟征德、张敏、张凡、黄亮、庄湧。

引　言

主流 IT 产品供应商开始在他们的数据库管理系统、安全管理系统、网络操作系统等产品中大量实现基于角色的访问控制功能，然而却没有对其特征集达成一致。缺乏广为接受的模型，导致了对基于角色的访问控制效用和含义理解的不规范性和不确定性。本标准参照 ANSI INCITS 359-2004，使用一个参考模型来定义基于角色的访问控制的特征，并描述这些特征的功能规范，通过以上方法来解决这些不规范与不确定的问题。

信息安全技术　鉴别与授权　基于角色的访问控制模型与管理规范

1　范围

本标准规定了基于角色的访问控制(RBAC)模型、RBAC 系统和管理功能规范。

本标准适用于信息系统中 RBAC 子系统的设计和实现，相关系统的测试和产品采购亦可参照使用。

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。

ISO/IEC 13568:2002　信息技术　Z 形式规范注释语法、形式系统和语义学

3　术语和定义

下列术语和定义适用于本标准。

3.1

组件　component

这里是指四个 RBAC 特征集之一：核心 RBAC、层次 RBAC、静态职责分离关系、动态职责分离关系。

3.2

对象　object

需要进行访问控制的系统资源，例如文件、打印机、终端、数据库记录等。

3.3

操作　operation

一个程序的可执行映像，当被调用时为用户执行某些功能。

3.4

权限　permission

对受 RBAC 保护的一个或多个对象执行某个操作的许可。

3.5

角色　role

组织语境中的一个工作职能，被授予角色的用户将具有相应的权威和责任。

3.6

用户　user

人、机器、网络、自主智能代理等，进行资源或服务访问的实施主体。

3.7

会话　session

从用户到其激活的角色集合的一个映射。

3.8

职责分离　separation of duty

限制用户获得存在利益冲突的权限集的约束，例如用户不能同时获得会计和审计的权限。