市级电费核算系统的访问控制*

沈宇红[1], 黄 [illegible]
(1. 广州供电分公司, 广东 广州 510620;
2. 中山大学电子通信工程系, 广东 广州 510275)

摘 要: 基于角色的访问控制 (RBAC) 是近几年访问控制领域的热点。然而组织关系密切、例如大型企业的信息管理, 还存在组织之间联系不紧密的问题。根据大型企业组织应用特点, 在电费核算系统上设计一种以组织为核心, 基于角色的组织层次式的访问控制, 客体、功能、角色等与组织挂钩, 在宏观上是给组织授予权限, 在每个组织上又具体划分成有继承关系的角色功能集, 由直接上级管理者对下级组织的授权和用户管理。这种管理方式是大型企业的信息访问控制的一种有效新方式。

关键词: 访问控制; 角色; 组织
中图分类号: TP393.01 文献标识码: A 文章编号: 0529-6579 (2005) S1-0178-03

访问控制是当前信息安全领域研究的热点问题之一。目前访问控制类型主要有 3 种: 自主访问控制 (DAC, Discretionary Access Control), 强制访问控制 (MAC, Mandatory Access Control) 和基于角色的访问控制 (RBAC, Role Based Access Control)。另外尚有一些新兴的如给予组织的、任务的、对象的访问控制。DAC 十分灵活, 但安全性不强, 授权管理复杂。MAC 是一种比较严格的访问控制方法, 但灵活性差。

基于角色的访问控制 RBAC 将权限赋给角色, 角色分配给用户。这种访问控制方式使用户通过角色享有权限, 而不直接与权限相关联。其不足在于与组织联系较弱。而基于组织的访问控制作为新兴的访问控制, 其管理仍处于待完善阶段[1—4]。

市级电费核算系统作为一个分布的企业网络, 人员众多, 管理复杂, 拥有独立管理而又互相合作的子组织单位。根据其特点, 本文提出一种以组织为核心的, 基于角色的组织层次式的新访问控制方式。

1 电费核算系统的应用分析

电费核算系统是一个多级、分布式的复杂系统, 它是在核算中心的统一领导下, 各子组织单位在独立管理自己的业务资源的同时进行相互的合作, 为全市用户提供一个无感觉分单位的统一服务窗口。组织结如图 1 所示。

应用者的访问管理有以下特点:

(1) 用同一数据库, 同一软件系统;

(2) 核算中心可以管理所有的配营部资源;

(3) 除了某些共享服务, 如电费查询与收取外, 一般情况下, 各个配营部只能管理自己所属的客户资源;

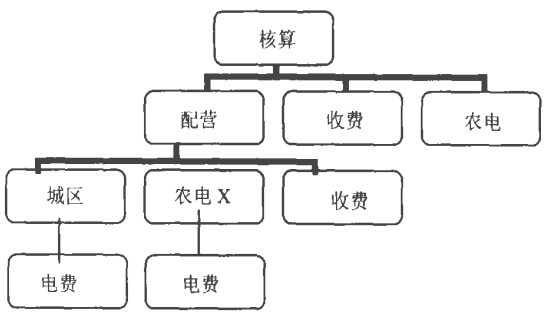

图 1 核算电费组织架构图
Fig. 1 The boom of electrical fee MIS

(4) 配营部中的资源一般可分为城区及农电两种; 但也有配营部将之合并的情况。

①同一配营部中, 城区与农电只能管理自己所属的客户资源;

②城区的管理相对比较规范, 班组设置大体一致, 但是班组内的访问权限 (角色) 分配会有很大的差异;

③农电的管理则五花八门, 有的因管理的范围比较广, 增设收费点来分管, 有的则将抄表班与核收班合二为一。

由此可见, 组织与资源客体是紧密相关的。由

* 收稿日期: 2005—02—02
作者简介: 沈宇红 (1975 年生), 女, 工程师; E-mail: yandan1978@163.com

于不同子组织资源客体的差异，需实行各自独特的管理方式，传统的统一管理模式的访问控制方法难以管理及应用。因此，研究一种新的访问控制方式，将访问权限批量授予子组织，让子组织自己独立去细化分配管理，市级最高管理者只需实行粗放式管理直属子组织，是现代化管理的迫切需要。为此本文提出一种以组织为核心的，基于角色的组织层次式访问控制方式。该方式显著提高了管理的灵活性，安全性和效率。

2　核算系统的访问控制设计

在访问控制设计中，系统的实体如用户、客体、操作、角色等都需要有组织的属性。管理分层次和部门，每一个组织单元仅有一个管理角色授予一个管理员，负责安排本单元的角色设置、权限角色分配以及用户角色分配，负责直接的下级的可用功能分配和用户分配。

采用 ARBAC02 的用户库和权限库概念。不同之处在于 ARBAC02 须预先定义，而 RBOHAC 则根据组织结构来定义，由对应等级的管理员设置好组织结构（子组织）和用户库（用户－组织指派）、权限库（权限－组织指派）。由于组织结构与现实的组织结构非常接近，用户被指派到唯一的一个组织中，组织中的角色权限需要从本组织所拥有的权限中取得，不同组织间的角色关联不大，这样可以简化管理。

组织之间具有权限继承关系，但不是所有权限均可继承。有鉴于此，本文借鉴对象管理方法，引入了权限属性概念，将权限区分为私有权限、公有权限和特征权限。其中私有权限不能被继承；公有权限永远被继承；特征权限的继承类别可以分成一般继承、私有化继承、公有化继承和无特征继承，对应着继承为特征权限、私有权限、公有权限和不继承权限。因而既可以处理复杂的组织层次关系。又可以实现组织权限由上而下的继承分配。

在设置权限属性的同时，为简化权限的配置，对操作类型定义了包含关系：修改包含了读，读包含了无权限。从而权限的分配可以只给最大的操作就可以了，大大地减少了权限的分配。

要在同一运行环境下，客体对不同的组织有不同的访问限制，引入了视图作为客体的抽象，在本模型中是作为一种选择条件，这样就能做到共用一套系统，但又满足独立或合作地管理自己资源的要求。对每个组织设置其唯一的访问方向：双亲、孩子、本身，从而达到客体与组织的紧密关联。如图 2 所示。

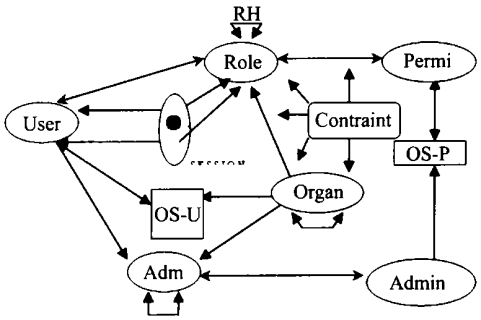

图 2　AC 模型

Fig. 2　The model of AC

3　访问控制的实现

客体分为数据库资源以及应用系统资源，对于数据库资源是禁止客户直接使用的，因此可以控制授权 SQLPLUS 客户端产品连接来实现阻止，应用系统的使用是访问控制的关键。

在数据库只能感建立以下数据库表实体：用户信息表、组织信息表、功能表、视图信息表、语境限制表、操作关系表、用户－组织信息表、权限－组织信息表、角色－组织信息表、权限－角色信息表、用户－角色信息表。下面介绍相关表的主要信息。

(1) 用户信息表
(用户编号,
用户姓名,
用户口令,
任职岗位,
primary key (用户编号))

(2) 组织信息表
(组织 ID ,
组织名,
双亲组织 ID,
访问资源方向,
primary key (组织 ID))

(3) 视图信息表
(视图 ID,
功能 ID (not null unique),
组织资源限制,
语境限制 ID 号,
primary key (视图 ID))

(4) 用户－组织信息表
(用户 ID,
组织 ID,
primary key (用户 ID, 组织 ID)))

(5) 权限—组织信息表
(组织 ID,
视图 ID,
操作 ID,
权限属性,
权限继承方式,
primary key (组织 ID, 视图 ID))
(6) 角色—组织信息表
(组织 ID,
角色 ID,
角色名,
primary key (组织 ID, 角色 ID))
(7) 权限—角色信息表
(组织 ID ,
角色 ID,
视图 ID,
操作 ID,
primary key(组织 ID, 角色 ID, 视图 ID))
(8) 用户—角色信息表
(用户 ID,
组织 ID ,
角色 ID,
primary key(组织 ID, 角色 ID, 组织 ID))

准确、合理地设置组织角色和授予相应的功能权限, 是一个信息系统安全使用的基本保障条件。

4 结 语

本文提出的基于角色的组织层次式访问控制更能与现实的大型企业运作管理一致; 企业是分层次, 分部门的; 各个部门在统一的管理, 相互合作而又相对彼此自主; 上级主管应该是宏观管理并直接面对各下级单位。

参考文献:

[1] Anas Abou El Kalam, Rania El Baida, Philippe Balbiani. Organization based access control[DB/OL]. http://www.ensi-bourges.fr/perso/abouelkalam/document, 2005.
[2] Frederic Cuppens, Alexandre Miege. Administration model for Or-BAC[DB/OL]. htpp://www-simis.inria.fr/~Bougaim, 2005.
[3] 张晓辉, 王培康. 大型信息系统用户权限管理[J]. 计算机应用, 2000(11): 35—36.
[4] 周俊. 大型信息系统用户权限管理的探讨与实现[J]. 计算机应用研究, 2004(12): 143—16.

The Access Control for Electrical Fee MIS in Municipal Enterprise

SHEN Yu-hong[1], *HUANG Cai*[2]
(1. Guangzhou Power Supply Branch, GPG, Guangdong, Guangzhou 510620, China
2. Department of Electrinics Engineering, Sun Yat—sen University, Guangzhou 510275, China)

Abstract: Role-based access control (RBAC) is a hot topic in the research field of access control recently. But there are some shortcoming. In this paper, the rose base organization-hiberarchy access control is designed for electrical fee MIS. In this model, each entity has organizational property. On the macro view, it gives legal power to organization. And each organization has the inherit role. This kind of management method is a kind of valid way for the access control of the large business enterprise.

Key words: Access Control; Role; Organization