计算机科学2002Vol. 29№. 3

角色层次关系的分析与研究

Analysis and Research on Role Hierarchies

张绍莲　欧阳毅　杜　鹏　谢俊元

（南京大学软件新技术国家重点实验室　南京大学计算机科学与技术系　南京210093）

Abstract　Constructing a role hierarchy is the key process of implementing RBAC models. In this paper, we first analyze the concept of role hierarchy from the view of application field, and then introduce four typical kinds of role hierarchy: permission-usage, role-activation, manage-relation, constraint-inheritance. Last we propose a common RBAC model synthesizing the four role hierarchies, which simulates the situations in the application field and embodies the management relationship in the real world and so simplifies management of authorizations.

Keywords　Role-Based Access Control, Role Hierarchy

1　引言

随着计算机技术及应用的发展，计算机信息系统越来越复杂，资源访问权限的管理也变得越来越困难，以角色为中介的访问控制（Role-Based Access Control，RBAC）[1,2]技术的出现大大缓解了资源管理的问题。RBAC的基本思想是通过角色实现用户与权限之间的逻辑隔离，用户不直接与权限发生关联，而角色与权限相关联，用户根据其工作职能与一定角色相关联。

如果把角色理解为现实社会中工作职位在信息管理领域中的一个抽象，那么RBAC的权限管理方式非常类似于应用领域中的管理模式。当RBAC用于信息系统的权限管理时，这种以角色为中介的管理模式容易被普通用户理解和接受。事实上，能够提供这种自然化、人性化的权限管理方式是RBAC技术近年来日益受到重视的最主要的原因。显然，现实生活中的工作职位不是孤立的，它们之间存在一定的联系，比如权限包含、上级管理下级等，在角色之间引入一定的层次关系来模拟现实社会中工作职位间的关系是RBAC技术优越性的一个主要体现，目前几乎所有的描述RBAC技术的理论模型都把构造合适的角色层次关系作为重点解决问题，比如RBAC96模型[3]提出了角色与角色之间的继承关系，ARBAC97模型[4]提出了角色（即管理角色）和角色（即普通角色）之间的管理授权关系，Nyanchama的角色层次图模型[5]更强调构造合适的角色层次关系。研究角色之间的层次关系对于RBAC技术在信息系统中的广泛应用具有极其重要的推动作用。

本文主要从模拟现实社会的组织机构出发重点研究角色之间的层次关系，首先概述构造合适的角色层次关系的作用，分析了非常流行的角色层次关系——权限继承关系，提出了角色继承层次关系、管理层次关系、约束继承层次关系，并分析它们的含义和主要应用范围，本文最后利用这几种角色层次关系模拟了现实社会的组织结构内部之间的联系，给出了比较通用的角色层次关系框架模型。

2　角色层次关系的意义

角色层次关系是RBAC技术用于大型信息系统中重点需要考虑的问题，引起了众多学者的重视，构造合理的角色层次关系对于解决权限管理的实际问题具有非常重要的意义，这主要表现在以下三个方面：

（1）角色之间的层次关系是对应用领域中工作职位间关系的一个非常形象的模拟[6]。尽量模拟应用领域的组织结构和其中的权限管理一直是RBAC技术追求的目标，构造角色层次关系是其中的一个主要体现。

（2）构造合适的角色层次关系在很大程度上方便了系统的权限管理。例如：某子部门新增加一项具体业务，这在应用RBAC技术的信息系统中相当于为对应该子部门的那组角色添加相应的权限，如果把这组角色按照权限继承组织成一定角色层次关系，只需要管理者给该组内最低级角色赋予相应的权限，其它角色通过继承层次关系自动获得相应的权限，如果以后某个时候这部门不再需要这些权限，只需取消该组内最低级角色的相应权限即可。角色层次关系使得相应的权限变更非常容易管理，如果不把角色组织成层次关系，需要逐个管理每个角色的权限变更。

（3）能够满足某些特殊安全管理的需要，比如满足层次化管理的需要或者满足最小特权原则。如果应用领域的组织结构复杂，其对应的RBAC系统中的角色数量很多，管理员自己难以对所有角色进行直接管理，那么就需要在角色之间构造合适的管理层次关系，实现对某些角色的间接管理。此外，在角色之间构造合适的角色继承关系，方便实现权限管理中的最小特权原则，提高系统的安全性。

3　角色概念的延伸与常见的角色层次关系

3.1　角色概念的延伸

角色是实现权限与用户逻辑隔离的语义结构，作为一种抽象结构，角色的含义与它的应用领域密切相关。在办公系统中，可以理解为工作职位的抽象，在操作系统的安全管理中，角色可以看作是一组管理职能的抽象。

针对现实社会的组织结构，我们不难看出每个组织内的

张绍莲　硕士，主要研究方向：计算机网络及安全。欧阳毅　硕士，主要研究方向：计算机网络及安全。杜　鹏　硕士，主要研究方向：分布式系统及高性能计算。谢俊元　博导，主要研究方向：网络安全，人工智能。

工作职位常常会对应两种不同的职能：处理具体业务的职位和管理职位，前者如一般程序员，它的责任（或者说权利）是按指定设计编写程序代码，后者如项目经理，它的主要任务不再是处理具体的业务（如编写程序代码），而是协调项目组内部的其他成员共同完成一项任务，如指定谁负责项目设计，谁负责编写哪部分代码等。显然，这两类工作职位具有截然不同的职能和责任，要深入探讨角色之间的层次关系以便非常形象地模拟现实社会中工作职位间的关系，就必须通过不同类型的角色区分这两类不同的工作职位。

根据现实社会中两种不同的工作职位，角色可以简单地分为常规角色和管理角色，分别与它们相对应。在计算机信息系统领域，以角色的操作是否影响信息系统中其它实体的授权关系作为区分这两类角色的依据。常规角色根据给定的权限完成一定的信息处理，但是它所执行的操作不会改变其它实体的授权关系，比如操作系统的某角色只能执行普通文件读写权限，而这些操作不影响其实体（用户或角色）是否拥有某种权限。相反，管理角色带有一定的管理职能，它执行的操作有可能引起其它实体（角色或用户）拥有的权限，如操作系统中的用户管理员。

虽然，在很多 RBAC 模型（ARBAC97模型除外）中还没有明确提出管理角色的概念，但是随着 RBAC 在大型系统中的深入应用，管理角色的概念将会得到普遍的应用，区分常规角色和管理角色有助于 RBAC 技术的深入研究。

3.2 主要的角色层次关系

权限继承关系在很多 RBAC 模型中得到应用，通过上述管理角色和常规角色的区分，可见在角色与角色之间构造合适的管理关系也是对现实组织结构的一种很好的模拟。此外，本文还提出了角色继承、约束继承两种角色层次关系。下面关于角色层次关系的讨论主要涉及到这四种角色层次关系。

4 四种角色层次关系

4.1 权限继承关系

权限继承关系的含义是：若角色 R1权限继承角色 R2，那么 R1自动拥有 R2的所有权限。权限继承关系在一定程度上反映了一个组织内部的权利和责任关系，方便了系统的权限管理。权限继承关系是目前最受人关注的角色层次关系，几乎所有的 RBAC 模型都涉及到它，此外一些学者还对权限继承的应用问题做了深入的研究，RBAC96模型通过提出私有角色的概念来描述不愿对外公开（即被其他角色继承）的权限，并通过角色分离的方法来实现。文[3]利用类继承的思想提出了私有权限的概念，一个角色拥有的权限分为私有权限和公共权限，高级角色只能继承低级角色的公共权限，私有权限的提出解决了权限部分继承的问题。

构造合适的权限继承角色层次关系是权限继承关系方便系统权限管理的基础，不难想象，权限继承体现了一种自底向上的权限积聚的思想，要构造合适的角色层次关系常常需要管理者非常清楚所管角色的各种细节。

权限继承关系在常规角色中得到了广泛的应用，但在管理角色之间很难得到很好的应用，因为如果把管理角色看作是组织机构内部管理职位的抽象，那么权限继承管理就是越层管理的体现，越层管理在很多领域都不提倡。比如校长能够管理系主任职位的设立与人员任免，系主任能够管理教研室主任职位的设立与人员任免，但是要校长继承系主任的权限直接管理系下面教研室主任的人员显然不合乎现实生活中的实际情况，也容易带来管理混乱、责任不明确等问题。

4.2 角色继承关系

角色继承关系是指：如果角色 R1（高级角色）角色继承 R2（低级角色），那么拥有角色 R1的用户 U 自动隐含拥有角色 R2，即使没有把 R2分配给用户 U。

角色继承关系是一种非常有用的角色层次关系，虽然它不对应现实社会中权利和责任关系，但是它体现信息系统安全中最重要的管理原则，即最小特权原则。一个拥有高级角色的用户可以根据自己的实际需要，尽可能地以拥有权限最少的某低级角色登陆进系统，这样登陆的目的是：一方面能够减少因用户执行的误操作而对系统安全带来的危害；另一方面在出现安全意外时（比如登陆后被非法用户用特洛伊木马控制），也能最大限度地减少安全损失。在 RBAC 的系统中支持角色继承与操作系统提倡管理员是同样的道理，除非需要尽量用一般用户的账号登陆系统。

角色继承关系在常规角色之间能得到很好的应用，构造良好的角色继承关系能够真正提高系统对误操作和意外事件的抵抗力。与权限继承相类似，角色继承关系在用于管理角色之间时同样体现越层管理的思想，可能会带来也容易带来管理混乱、责任不明确等问题。

尽管构造权限继承关系与角色继承关系的目的不同，二者的表现形式也有所区别，但是它们具有相同的实质：拥有高级角色的用户具有更多的权限，通过权限继承获得的权限和通过角色继承获得的权限在使用时没有区别。由于二者具有相同的实质，可以统一构造相应的角色层次关系，根据应用需求的不同来决定解释成权限继承关系或角色继承关系。

4.3 管理层次关系

如果把角色看作现实组织中工作职位的抽象，在角色之间构造管理关系是对组织管理结构的一种非常自然的模拟，现实生活中的有些职位不仅仅处理具体业务还对其它职位的业务处理实施一定的管理，角色间管理层次关系恰巧反映了职位之间的这种关系。

角色管理层次关系的含义：若一个角色（高级角色）R1与另一个角色（低级角色）R2存在管理层次关系，那么角色 R1可以为 R2添加新的权限，或删除已有的权限，也可以把角色 R1分配给特定的用户，甚至可以删除角色 R1。

管理层次关系体现了自顶向下、逐级管理的思想，利用管理层次关系可以很好地解决角色管理问题。在应用实际系统中，当角色的数量不多时，管理员可以有效地对角色的生成、权限配置、用户指派进行集中式控制。但是在涉及到众多角色的大系统中，如何定义和管理这些成百上千的角色及它们之间的关系（即本文的 RBAC 实例框架）本身就很复杂，难以再由管理员进行集中管理和控制。显然在角色之间定义管理层次关系可以实现实例框架的分布式管理，管理员只需管理最高层的一些管理角色，其它常规角色和低级管理角色通过这些高级管理角色直接或间接地进行管理。

此外，通过管理层次关系还体现了权限传递的思想，通过这种关系可以实现复杂的 RBAC 实例框架自顶向下、逐步细化的过程。首先最高级管理者（即管理员）试图直接创建整个 RBAC 实例框架，当发现某部分实例框架过于复杂或不便于直接创建（对应于下一级子部门等）时，就创建相应的低一级管理角色，并赋予它们相应的管理权限，由它们承担相应部分实例框架的细化创建，上一级的管理职位只是从宏观上协调下一级的管理工作，而不能直接参与下一级的管理。下一级的

管理角色同样也可以创建更低级的管理角色(这些创建出来的管理角色对上一级的管理角色透明,即不可见)以实现对某部分实例框架更加具体的管理,直到该部分实例框架创建工作都得到具体的落实。整个 RBAC 实例框架的形成过程,相当于一棵倒立树的向下生长过程,如图1。

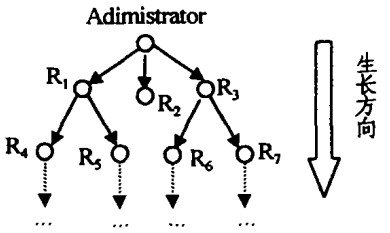

图1 管理层次关系与实例框架的创建

管理关系可以用在管理角色和管理角色之间,也可以用在管理角色与常规角色之间,在常规角色内部很少用到。当用于管理角色之间时,管理层次关系比权限继承关系更能反映组织内部的权利和责任关系,通过管理关系组织起来的角色层次关系更加形象地描述了管理职位之间的关系。

4.4 约束继承关系

约束继承关系是指:低级角色在行使自己的权限时必须满足对它的管理角色的约束,也就是说低级角色继承高级角色的约束条件。当用于管理角色之间时,约束继承关系具有非常重要的实际意义,它非常形象地体现了安全管理策略的继承性。从现实的组织结构中不难发现这种继承性,在一个复杂的组织中,比如一所大学,它的各级子部门都有自己的规章制度(对应信息系统中的安全策略),而且这些规章制度不是孤立的,它们的作用范围存在一定的联系:系级管理角色在行使自己的管理权限时,不仅要遵守系内的一些管理规定,还要遵守学校一级所制定的各种规章制度,教研室内部的管理角色要继承学校、系两级制定的规章制度。如果在安全策略和管理角色之间建立一个映射关系,那么这种安全策略在管理角色之间的约束继承层次关系完全模拟了现实社会中规章制度作用范围之间的关系。

除了在管理角色间存在约束继承外,常规角色之间也可存在约束继承关系。如主任医生和普通医生都是常规角色,前者是后者的高级角色,如果规定主任医生在行使某项权限时存在一定的约束(比如每张处方的总药价不能超出某上限),那么普通医生肯定也要遵守这个约束,除非普通医生本来就不享有这个权限。

此外,约束继承和管理关系在用于管理角色之间时具有一定的一致性,如果管理角色 AR1与 AR2之间存在管理关系(AR1管理 AR2),那么在它们之间也可以构造约束继承关系,AR2一般来讲应该继承与 AR1相关的约束。所以在构造管理角色层次关系时二者可以合二为一,在应用这些层次关系执行管理时再分别解释这两种角色层次关系。

5 一个角色层次关系的综合应用模型

上面讨论的四种角色层次关系基本上反映了现实社会中组织结构内部工作职位之间的主要关系,利用它们可以为现实组织结构勾画形象的角色层次关系图,本节就提出了这样一个综合实现这四种关系的层次框架模型。

同应用领域的树形层次管理相类似,管理角色通过管理关系能够组织成树状层次结构,这个树状层次结构能够体现大多数组织结构的主体框架,如图2(左)。如果规定常规角色只能有一个直接管理角色对它实施管理(这种规定是合理的,因为我们这里讨论的是角色间关系而非用户关系,角色是我们自己定义的。现实中,如果一个用户在多个部门担任工作,则我们可以为该用户在每个部门的工作定义一个角色),那么常规角色所隶属的直接管理角色被划分为多个子集。由于基层管理角色比较熟悉其管辖区域内的组织结构,因此很容易通过自底向上的方式在这些常规角色间构造权限继承的角色层次关系,这些有权限继承关系的常规角色对应于最基本的业务处理子部门的组织结构,如图2(右)。显然在不属于同一个直接管理角色的常规角色之间构造继承关系是不必要的,从管理的角度看也不合理,这与应用领域中的情况大体一致。

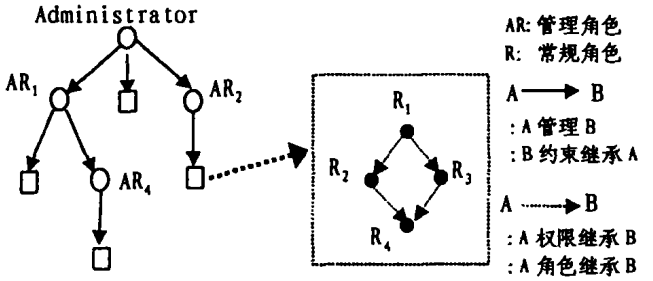

图2 一般组织结构对应的角色层次关系

在构造出上述两种角色层次关系之后,可以根据需要在上下级管理角色间构造约束继承层次关系,约束继承关系非常形象地展现了现实组织中上级部门管理策略(即管理规章制度等)对下级部门发挥作用的传递性。在常规角色之间引入角色继承关系可以很好体现最小特权管理原则,在不禁止越层管理的应用场合,也可以在管理角色之间引入权限继承关系和角色继承关系。

结束语 RBAC 模型是解决信息系统中复杂权限管理问题的一条非常有效的途径,而应用 RBAC 模型的关键在于构建符合安全策略、拟合实际情况的角色层次关系。本文根据现实生活中的组织管理机构,提出并分析了权限继承关系、角色继承关系、管理关系、约束继承关系四种角色间的层次关系。根据不同需要,可以灵活地选择实现这四种角色关系。由于这些关系都是从对现实社会的分析中抽取出来的,因此按照它们构建出来的 RBAC 系统就能够贴切、自然地模拟现实组织的运作方式,易于接受和理解。

参 考 文 献

1 Ferraiolo D F, Cuginiand J, Kuhn D R. Role Based Access Control: Features and Motivations. In: Proc. of the 11th Annual Conf. on Computer Security Applications. 1995

2 Sandhu R S, et al. Role-based Access Control: A Multi-Dimension View. In: Proc. of the 10th Annual Conf. on Computer Security Applications. 1994

3 Sandhu R S, et al. Role-Based Access Control Models. IEEE Computer, 1996, 29(2): 38～47

4 Sandhu R, et al. The ARBAC97 model for role-based administration of roles. ACM Transactions on Information and System Security, 1999, 2(1): 105～135

5 Nyanchama M, Osborn S. The role graph model and conflict of interest. ACM Transactions on Information and System Security, 1999, 2(1): 3～33

6 钟华,等. 扩充角色层次关系模型及其应用. 软件学报, 11(6): 779～784