文章编号：1002-0411(2009)-03-0276-05

业务过程管理中基于组织和角色语义的访问控制

王伟然，张　洵，范玉顺

（清华大学自动化系，北京　100084）

摘　要：针对现有业务过程访问控制方法不能充分满足业务过程管理（BPM）实际需求的问题，首先分析了基于角色的访问控制（RBAC）和基于任务的访问控制（TBAC）等方法的不足；然后提出了一种基于组织结构和角色语义的访问控制（OR-SBAC）模型和方法，并采用形式化方法描述了 OR-SBAC 模型及其部件；最后给出了 OR-SBAC 的应用案例. OR-SBAC 进一步划分了角色和受控主体，使用企业的组织结构进行用户与角色间的关联，在角色授权过程中通过角色适配器，基于一阶谓词逻辑进行角色语义推理，并考虑了时间和空间上下文等问题. OR-SBAC 方法的描述能力强，权限分配效率高，能够满足业务过程管理中访问控制的复杂性、多样性和灵活性等方面的需求.

关键词：业务过程管理（BPM）；访问控制；组织结构；角色；语义

中图分类号：TP309.2, TP391　　**文献标识码**：A

Organization and Role Semantic Based Access Control of Business Process Management

WANG Wei-ran, ZHANG Xun, FAN Yu-shun

(*Department of Automation, Tsinghua University, Beijing* 100084, *China*)

Abstract: Current access control methods of business process can not meet the practical requirements of business process management (BPM). In order to solve this problem, disadvantages of the access control methods including role-based access control (RBAC) and task-based access control (TBAC) are analyzed. Then, an organization and role semantic based access control (OR-SBAC) model and method are proposed, its model along with the formal description of its components is presented, and an application example is given. The OR-SBAC method provides further classification of the roles and the controlled subjects, utilizes organizational structure to describe the relationship between user and role, fulfills authorization through role adapter by illation based on role semantics, and considers contexts of time and space. The strong description ability and high authorization efficiency of the OR-SBAC method meets the requirements of complexity, variety and flexibility in BPM.

Keywords: business process management (BPM); access control; organizational structure; role; semantics

1　引言（Introduction）

业务过程管理（BPM）的管理对象多种多样，运行过程比较复杂. 访问控制是 BPM 中的一个重要问题，影响着信息系统的安全和业务过程运行的有效性[1].

传统的自主访问控制（discretionary access control，DAC）和强制访问控制（mandatory access control，MAC）等访问控制方法存在安全性不高、完整性不足和使用过程复杂等问题[2]. RBAC 是目前的主流方法，现有的 BPM 访问控制大都基于 RBAC 方法[3~5]. RBAC 在用户和访问许可之间引入了角色（role）的概念，提供了较好的灵活性和扩展性. 目前对 RBAC 的扩展主要集中在两方面——建立和丰富用户或访问许可权的结构以及对 RBAC 进行约束[6,7]. 但是 RBAC 没有对任务（task）和角色加以区分. 作为一种被动的、提前授权的技术，RBAC 难以满足 BPM 动态运行过程中访问控制的实际需要[8,9].

TBAC 可以用于工作流运行中的动态授权[10]，但是并非所有访问操作都与业务过程实例中的任务相关，而且该方法在应用中过于复杂. Oh 和 Park 在 RBAC 的基础上，把任务引入到角色与访问许可之间，将 RBAC 与 TBAC 相结合，提出了基于任务和角色的访问控制方法（task-role-based access control，T-RBAC）[6]. 但 T-RBAC 仍无法解决不同实例存在不同权限的问题. 其他的访问控制方法，如基于属性

基金项目：国家 863 计划资助项目 (2006AA04Z166)；国家自然科学基金资助项目 (60674080)
收稿日期：2008-12-01

的访问控制（ABAC）[11,12]、业务集成中基于策略的访问控制[13]、基于受控实体的访问控制（EBAC）[9]等，由于对用户的描述能力不足，并且在应用中操作复杂，难以满足业务过程管理的需求.

为此，在 RBAC 和 TBAC 的基础上，提出一种支持业务过程管理的基于组织和角色语义的访问控制方法（organization and role semantic based access control，OR-SBAC）. OR-SBAC 使用组织结构，进一步划分角色和受控主体，引入角色适配器的概念，通过角色语义的推理实现访问授权. 全文首先分析了 BPM 中访问控制的主要问题，然后讨论了 OR-SBAC 的模型组成和访问控制方法，并进行了形式化描述，最后给出了一个应用案例.

2　BPM 访问控制的主要问题（Main issues in access control of BPM）

业务过程管理系统中管理对象的规模、系统复杂性和业务过程运行的多样性，使得 BPM 中的访问控制需要满足一些特定要求. 主要包括以下 3 个方面的问题：

(1) 受控主体的复杂性. 受控主体是指用户在逻辑层面上的访问对象，例如业务活动、资源元素等. 从流程的角度，可将 BPM 中的受控主体分为 3 类：独立于过程的受控主体，例如不直接出现在过程中的组织、资源、文档等；基于过程模型的受控主体，主要是过程静态模型中的元素；基于过程实例的受控主体，主要是过程运行中的元素. 不同类别受控主体的访问操作也不尽相同. 同时，访问授权与受控主体的状态有关，例如编制状态下的过程模型仅能够被具备建模权限的用户访问，发布后才能够被具备查看和监控权限的用户访问.

(2) 角色的复杂性. BPM 中的基本角色可分为 3 类：组织角色、流程角色和系统角色. 组织角色（例如“部门经理”）是存在于组织结构或角色结构中的静态的角色，独立于过程实例. 流程角色（例如“流程发起者”）是依存于过程实例的角色，仅在该实例的生命周期内有意义，不同过程实例内相同的流程角色常常指代不同的用户. 组织角色和流程角色的结合（例如，指定“流程发起者所在部门的经理”为任务执行者）使得 BPM 中的实际角色描述更加复杂. 系统角色是系统管理操作所需要具备的角色.

(3) 时间和空间上下文相关性. 现代企业的组织形式中，部门、人员和区域的调整更加灵活，在访问控制中必须考虑到时间和空间因素，例如人员调整或分布式企业的组织结构等. 在这方面，已有文献[14,15]引入组织结构和空间上下文等要素以降低复杂性，但使用范围过窄，不能直接用于 BPM 中的访问控制.

此外，还要考虑用户自主授权等其他需求. 因此 BPM 的访问控制较为复杂，这也是目前的方法没有很好地覆盖业务过程管理需求的主要原因.

3　OR-SBAC 模型组成及访问控制方法（Components and access control method of OR-SBAC model）

3.1　OR-SBAC 的访问控制机制

OR-SBAC 方法是针对上述问题提出的，模型如图 1 所示.

角色分为系统角色、组织角色和流程角色 3 类. 其中系统角色与用户直接关联，组织角色和流程角色通过企业模型中的组织结构与用户建立关联. 受控主体包括 3 类：独立于过程的受控主体、基于过程模型的受控主体和基于过程实例的受控主体. 其中对前两类受控主体主要采取被动的访问控制，对最后一类主要采取主动的访问控制，后两类受控主

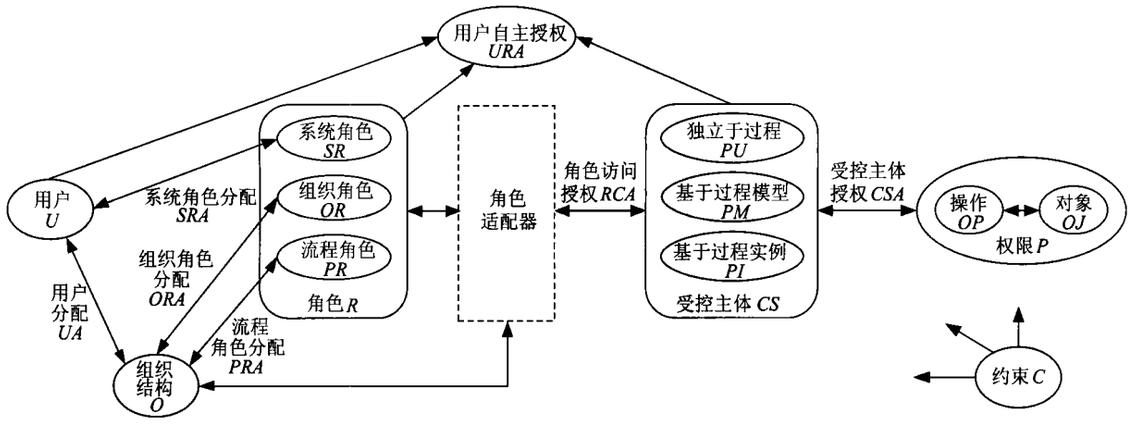

图 1　OR-SBAC 访问控制模型

Fig.1　OR-SBAC access control model

体的访问控制还与本身的属性有关. 在角色和受控主体间引入“角色适配器”，如图 2 所示，通过基于角色语义的推理将用户的角色和受控主体的角色描述进行匹配，从而进行角色访问授权.

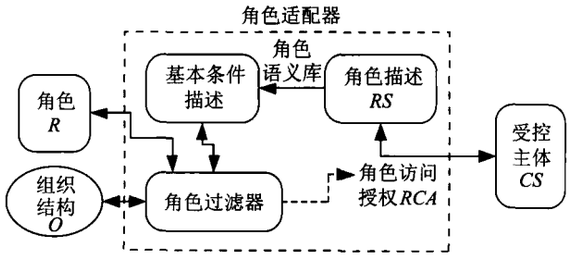

图 2 角色适配器用于角色访问授权

Fig.2 Role adapter used in role access authorization

在这一机制中，组织结构的使用能够在简化授权操作的同时，以更强的表达能力适应组织动态性的要求；角色语义的引入使访问控制满足 BPM 的动态性要求，并简化授权过程，提高授权效率.

3.2 OR-SBAC 的模型部件

OR-SBAC 模型由如下部件组成：

(1) 用户集 U，组织结构 O，角色集 R，角色描述集 RS，受控主体集 CS，权限集 P，操作集 OP，对象集 OJ，约束集 C，受控主体访问集 AC. 其中：

① 组织结构 O 为四元组 (D,E,R_D,R_{DE})，$D=\{d_{ij}\}$ 表示组织（例如部门或项目组）的集合，其中 d_{ij} 表示第 i 层的第 j 个组织；$E=\{e_l\}$ 表示人员的集合，其中 e_l 表示第 l 个人员；$R_D=\{(d_{ij},d_{(i+1)k},t_b,t_e)\}$ 表示组织间层次关系，含义为 $d_{(i+1)k}$ 是 d_{ij} 的下层组织，起止时间为 t_b 到 t_e；$R_{DE}=\{(d_{ij},e_l,t_b,t_e)\}$ 表示人员和组织的从属关系，含义为人员 e_l 属于组织 d_{ij}，起止时间为 t_b 到 t_e.

② 角色集 $R=SR\cup OR\cup PR$，其中 SR、OR 和 PR 分别表示系统角色、组织角色和流程角色的集合.

③ 受控主体集 $CS=PU\cup PM\cup PI$，其中 PU、PM 和 PI 分别表示独立于过程、基于过程模型和基于过程实例的受控主体集合，其中 $PM=\{pm_i\}$，$PI=\{pi_i\}$；$sta(pm_i)$ 和 $sta(pi_i)$ 分别表示这两类受控主体的状态，其状态空间分别为 $STAM$ 和 $STAI$.

(2) 用户分配 $UA\subseteq U\times E$，将用户与组织结构中的人员相对应.

(3) 系统角色分配 $SRA\subseteq U\times SR$，将系统角色直接分配给用户.

组织角色分配 $ORA=\{(or_k,o_i,t_b,t_e,ihr)\}$，其中 $or_k\in OR$ 为组织角色，$o_i\in D\cup E$ 为组织或人员，该分配表示组织角色 or_k 属于组织 o_i，t_b 和 t_e 为该分配的起止时间，ihr 表示该分配是否允许其他用户通过用户自主授权的方式继承权限.

流程角色分配 $PRA=\{(pr_i,pi_j,e_k,t_b,t_e,ihr)\}$，其中 pr_i 为流程实例，pi_j 为流程角色，e_k 为人员，t_b 和 t_e 为该分配的起止时间，ihr 表示该分配是否允许其他用户通过用户自主授权的方式继承权限.

(4) 角色访问授权 $RCA=\{(rs_i,cs_j,AC_k,STA_p)\}$. 其中 rs_i 为角色描述，cs_j 为受控主体，AC_k 为允许授权的访问集合，STA_p 是受控主体状态空间的子集，在受控主体基于过程模型或过程实例时有意义，为允许授权时的状态集合.

(5) 受控主体授权 $OSA\subseteq CS\times P$，表示受控主体和权限之间的分配.

(6) 用户自主授权 $URA\subseteq U\times U\times(R\cup CS)$. 用户可以自主地将角色或受控主体的访问权限让渡给其他用户，或从被让渡用户回收.

3.3 OR-SBAC 的角色访问授权方法

OR-SBAC 的角色访问授权基于角色语义进行，如图 2 所示，根据受控主体关联的角色描述，通过角色语义库，将约束和隐含条件（例如时间和空间上下文等）显式化，得到基本条件描述表达式. 角色过滤器通过查询相应的角色、组织和自主授权记录，按照这一表达式进行推理，给出角色访问授权的结果.

角色语义的表达和推理以基于一阶谓词逻辑的形式进行. 全总个体域为 $U\cup O\cup R\cup CS\cup T$（其中 T 为时间的集合），个体变元以带下标的小写字母表示，授权操作的对象用户标记为 u_x；谓词以大写字母表示，一目谓词表示个体具备的角色或属性，二目谓词和多目谓词表示两个或多个个体之间的关系；连接符与量词使用一阶谓词逻辑中的标准形式，包括 $\wedge$（与）、$\vee$（或）、$\neg$（非）、$\exists$（存在量词）、$\forall$（全称量词）等.

OR-SBAC 的访问授权包含如下的隐含原则：

隐含原则 1：如果受控主体 $cs\notin PI$，则 cs 的角色描述中不应包含与流程角色有关的条件.

隐含原则 2：用户在自主授权中，让渡的角色必须是该用户所具备的，让渡的受控主体访问权限必须是该用户能够得到访问授权的，并允许用户通过自主授权的方式继承.

角色适配器中，谓词的定义及其与角色描述的关联保存在角色语义库中，表达式的判断是在角色过滤器中依据谓词的定义进行的. 角色过滤器按照用户授权内容的不同，通过如下两个方面完成用户自主授权的推理：角色授权方面，将自主授权得到

的角色归并到用户角色后再进行推理；受控主体授权方面，查询用户是否通过自主授权得到了受控主体权限，并且该自主授权符合隐含原则 2.

4　应用案例（Application case）

由清华大学自动化系网络化制造课题组设计和开发的 BPM 系统采用了 OR-SBAC 方法进行访问控制. 该 BPM 系统以集成化企业建模为理论基础，包括建模工具、浏览工具、文档管理工具、用户管理工具及模型合并工具等模块，对企业模型的过程、组织、资源、功能、信息、产品和文档等多个视图进行建模和查看，并对业务过程实例的运行进行可视化的管理. 该系统的访问操作对象包括 3 类：基于过程模型的受控主体、基于过程实例的受控主体以及独立于过程的受控主体. 模型和实例的数据、权限集、用户集、角色集、角色描述集、角色语义库等信息都保存在 SQL Server 关系数据库中.

在访问过程中，通过查找组织结构、过程实例定义和系统权限分配，获取用户的相应角色；通过 OR-SBAC 方法中基于语义的推理过程，将所获取的角色与受控主体的角色描述进行匹配，以实现授权. 下面以某部门经理的访问控制过程为例进行说明：

首先，系统读取组织结构，建立该部门经理对应的用户，并将该用户与组织结构中的人员和角色相关联. 在过程模型中定义活动的角色描述，例如将“公务报销”流程的“部门审批”活动的角色描述定义为“本部门经理”，约束规则描述为“由费用发生时的部门经理审批”. 根据角色语义库的定义和约束规则（角色语义库中包括系统开发时定义的标准语义定义，也包括企业应用时自主添加的语义定义），可得到基本条件描述的表达式如下：

$$(\exists d_0)((Mgr(u_x,d_0,t_0))\wedge(\exists u_i)(Bl(u_i,d_0,t_0)\wedge PIr(u_i,pr_0)))$$

其中 d_0 为组织变元，u_x、u_s 和 u_i 为用户变元，t_0 为时间变元，pr_0 为过程实例（受控主体）变元，$Mgr(u_s,d_0,t_0)$ 表示用户 u_s 对应的人员在 t_0 时刻具备 d_0 部门经理的角色（组织角色），$Bl(u_i,d_0,t_0)$ 表示用户 u_i 在 t_0 时刻属于组织 d_0，$PIr(u_i,pr_0)$ 表示用户 u_i 具备过程实例 pr_0 的发起者角色（流程角色）.

同时，具备系统管理权限的用户使用用户管理工具，对角色和角色描述分配企业模型中各个视图的权限，将权限分配到各视图中的节点，并对不同节点分配不同等级的权限.

当该部门经理登录到系统的相应模块和视图时，首先获取该用户所具备的所有角色，根据这些角色通过角色适配器进行角色访问授权，将该用户具备的角色和企业的组织结构代入到基本条件表达式的运算中，根据验证结果进行授权，不同类型的对象在各视图中分别列出. 基于过程模型的受控主体方面，例如，在过程视图和文档视图中，将各角色被授权的节点及其授权的权限级别进行归并，展示用户得到授权的模型元素，并以不同图标表示得到的不同授权级别，见图 3、4. 基于过程实例的受控主体方面，例如，当该用户所主管的部门中有“公务报销”的过程实例运行到了“部门审批”活动时，通过了该表达式的验证，获得访问授权，此时该活动被展现在“查看当前任务”的视图中，如图 5 所示. 系统管理的对象则在系统管理和用户管理等视图中，根据用户的系统角色得到授权进行展示.

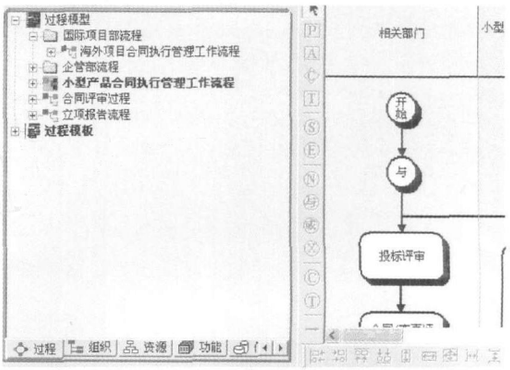

图 3　OR-SBAC 访问控制应用结果示例（过程视图）

Fig.3　An application example of OR-SBAC access control (process view)

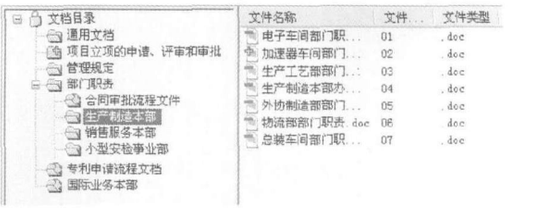

图 4　OR-SBAC 访问控制应用结果示例（文档视图）

Fig.4　An application example of OR-SBAC access control (document view)

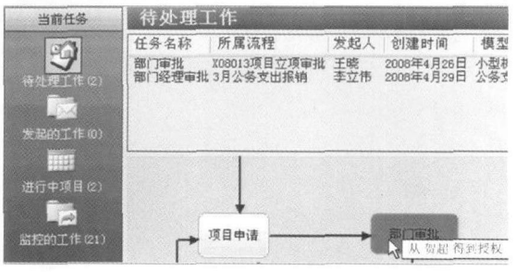

图 5　OR-SBAC 访问控制应用结果示例（查看当前任务视图）

Fig.5　An application example of OR-SBAC access control (view of current tasks)

在上述过程中，针对受控主体的状态，根据约束规则进行访问控制. 例如仅当活动实例处于“运行”状态时才对“执行”操作进行授权，而在其他状态时则屏蔽该操作授权. 同时，对系统中各用户的访问状态进行记录，对并发访问进行控制，避免操作冲突.

5 结束语（Conclusion）

与现有方法相比较，一方面，OR-SBAC 可以覆盖各主要业务过程访问控制方法的表达要素和描述能力. 例如，使用组织的层次结构和角色定义可以方便地表达层次 RBAC 方法中的角色层次关系；另一方面，由于对角色和受控主体进行了进一步分类，使用企业的组织结构进行用户与角色间的关联，并在角色授权过程中基于一阶谓词逻辑进行角色语义推理，OR-SBAC 具有更丰富的表达能力并且具备较高的授权效率，解决了现有方法对 BPM 支持的不足，能够更有效地对 BPM 运行过程中的各类参与者、管理对象和操作进行控制. OR-SBAC 方法能主动适应组织结构的动态变化并提高权限分配的效率，有效地支持业务过程的动态运行，从而满足业务过程管理（BPM）在访问控制复杂性、多样性和灵活性等方面的需求.

参考文献（References）

[1] 谭伟，范玉顺. 业务过程管理框架与关键技术研究 [J]. 计算机集成制造系统，2004，10(7)：737～743.

[2] 赵亮，茅兵，谢立. 访问控制研究综述 [J]. 计算机工程，2004，30(2)：1～2,189.

[3] 裘炅，谭建荣，张树有，等. 应用角色访问控制的工作流动态授权模型 [J]. 计算机辅助设计与图形学学报，2004，16(7)：992～998.

[4] 邢光林，洪帆. 基于角色和任务的工作流授权模型及约束描述 [J]. 计算机研究与发展，2005，42(11)：1946～1953.

[5] 杨书新，王坚. 工作流系统流程监控权限控制研究 [J]. 计算机集成制造系统，2007，13(11)：2224～2228.

[6] Bertino E. RBAC models – Concepts and trends[J]. Computers & Security, 2003, 22(6): 511～514.

[7] Li Q, Zhang X W, Xu M W, *et al*. Towards group-based RBAC model for secure collaborations[J/OL]. http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V8G-4V75YM9-1&_user=6028809&_ coverDate=12%2F25%2F2008&_alid=846348517&_rdoc=1&_fmt=high&_orig=search&_cdi=5870&_sort=d&_docanchor=&view=c&_ct=4&_acct=C000069154&_version=1&_urlVersion=0&_userid=6028809&md5=7a26f1fe0157eae96a6a0ff0ebae830d, 2008-12-25/2008-12-27.

[8] Oh S, Park S. Task-role-based access control model[J]. Information Systems, 2003, 28(6): 533～562.

[9] 杨喜敏，谢长生. 基于受控实体的访问控制技术 [J]. 华中科技大学学报（自然科学版），2007，35(8)：56～59.

[10] 邓集波，洪帆. 基于任务的访问控制模型 [J]. 软件学报，2003，14(1)：76～82.

[11] Yuan E, Tong J. Attributed based access control (ABAC) for web services[A]. Proceedings of the IEEE International Conference on Web Services[C]. Los Alamitos, CA, USA: IEEE Computer Society, 2005. 561～569.

[12] Obiedkov S, Kourie D G, Eloff J H P. Building access control models with attribute exploration[J]. Computers & Security, 2009, 8(1-2): 2～7.

[13] Bhatti R, Gao D F, Li W S. Enabling policy-based access control in BI applications[J]. Data & Knowledge Engineering, 2008, 66(2): 199～222.

[14] 徐震，冯登国. 一种使用组织结构的访问控制方法 [J]. 计算机工程，2006，32(13)：20～22.

[15] 张宏，贺也平，石志国. 一个支持空间上下文的访问控制形式模型 [J]. 中国科学 E 辑：信息科学，2007，37(2)：254～271.

作者简介：

王伟然（1983－），男，博士生. 研究领域为企业建模，业务过程管理，业务性能管理.

张 洵（1973－），男，硕士，讲师. 研究领域为企业建模，企业集成，信息资源规划.

范玉顺（1962－），男，博士，教授，博士生导师. 研究领域为企业建模，工作流技术，网络化制造.