协同工作系统中用户角色的设计与实施*

李亚子[1]　孙海霞[1]　蒋　君[2]　钱　庆[1]
[1](中国医学科学院医学信息研究所　北京 100020)
[2](北京万方数据股份有限公司　北京 100038)

【摘要】在研究基于用户和资源矩阵控制资源访问管理模式,以及用户角色在协同系统构建框架中作用的基础上,界定角色、权限、任务等概念,设计协同系统中角色管理模块,并阐述角色管理控制资源操作的逻辑过程,据此开发用户角色管理原型系统,根据项目需要设计 4 类角色,并应用于科技知识组织体系构建系统中。
【关键词】协同工作系统　角色管理　知识组织体系
【分类号】G350

Design and Implementation of Role Management in Collaborative System

Li Yazi[1]　Sun Haixia[1]　Jiang Jun[2]　Qian Qing[1]
[1](Institute of Medical Information, Chinese Academy of Medical Sciences, Beijing 100020, China)
[2](Wanfang Data Co., Ltd., Beijing 100038, China)

【Abstract】This paper researches resources management model of access control based on resource – user metric, and functions of user management in collaborative systems, then defines some concepts, such as role, right, task, and designs modules of role management subsystem, and also details logic process of above role management controlling to access resources. Finally, it develops prototype system of role management, according to needs of the projects, assigns 4 types of roles, and applies the roles to the system of constructing science knowledge organization system.
【Keywords】Collaborative system　Role management　Knowledge organization system

1　引　言

以计算机为基础的协作系统将个人和团队快速地关联组织起来,形成虚拟合作环境以实现特定目标。角色管理是协同工作系统的重要组成部分,是实施大规模协同作业的前提条件[1]。笔者所参与“十二五”科技支撑计划课题“科技知识组织体系的协同工作系统和辅助工具开发”的研究,该课题旨在建设知识组织体系分布式协同加工系统,整合理、工、农、医专业知识力量,构建适合现代知识服务环境的超级科技组织体系,系统加工的内容包括词条、概念、范畴表以及本体等。本文设计的用户角色管理是该系统的重要组成部分,角色管理的资源包括素材、概念、范畴以及本体等主要内容,同时也包括用户、角色、日志、版本等特定资源。在分布式虚拟环境中,通过角色管理确保知识组织体系能够被正确地加工、组织及发布,并对外服务。角色管理帮助系统(或者管理员,简称系统)在分布式应用环境中管理授权,设定用户通过指定应用程序访问的系统资源,以及访问的途径和方式。

收稿日期:2013 – 01 – 14
收修改稿日期:2013 – 02 – 14
* 本文系国家“十二五”科技支撑计划基金项目“科技知识组织体系的协同工作系统和辅助工具开发”(项目编号:2011BAH10B02)和中国医学科学院医学信息研究所基本科研业务费专项课题“国家级新型农村合作医疗信息系统建设关键问题研究”(项目编号:11R0101)的研究成果之一。

2 相关研究

研究者从理论上探讨了协作系统角色管理和资源访问控制管理的模式，如 Tolone 等[2] 通过构建用户和资源操作矩阵实现用户对资源访问的控制，资源访问控制矩阵模型如图 1 所示：

	File1	File2	File3	File4
John	创建者（可读、可写）		创建者（可读、可写）	
Alice	可读		可读	可读
Bob	可读、可写	可读		创建者（可读、可写）

图 1 资源访问控制矩阵模型[2]

矩阵的横向是系统中的资源（以文件形式表示），纵向是系统用户，横向和纵向的交叉处表示用户对资源拥有的操作权限。该方法直观明了，易于设计和实现。Li 等[3] 对资源进一步抽象，以对象形式控制用户对对象的操作权限，其他研究者从构建协同系统整体框架方面开展用户角色和权限管理的理论探讨[4]。角色管理是内容管理的基础模块，如 Drupal 等，在资源的操作权限控制方面，主要以模块为单元进行分配，在资源层面直接设置权限能力不足[5]。另外，具有较大影响力的本体或其他知识组织构建系统均涉及到分布式环境下用户及其权限管理问题，如 Web Protégé[6]、WebOnto[7]、Ontolingua[8] 等。Web Protégé 支持多用户并发创建和编辑本体，但是对用户的配置只能在服务器端执行，且必须重启服务器执行新的角色权限[9]；WebOnto 是较早实现分布式管理本体的工具，但仅局限于元项目控制粒度，即在项目一级控制用户的操作权限，管理的粒度较粗[10]。

本文在分析已有分布式协作系统中用户角色管理理论和实践的基础上，总结角色管理相关概念，借鉴资源控制矩阵方法设计角色及权限管理功能模块，阐述角色在执行任务中判断操作权限的逻辑流程，最后将其应用于实际的项目中。

3 角色设置方法

3.1 角 色

角色是相关权限命令的集合，使用角色的主要目的是简化权限管理，角色主要由权限和用户构成。这里涉及到几个定义：对象、操作、权限和任务[11]，它们之间的关系如图 2 所示：

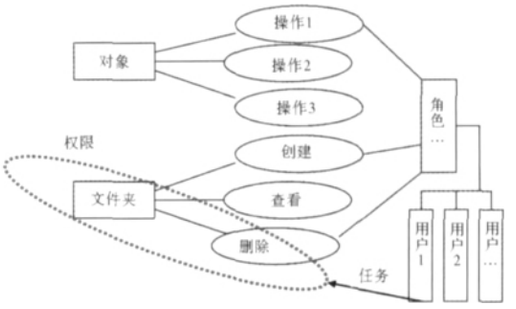

图 2 用户、对象、操作及任务示意图

（1）对象（Object），是被用户或者系统操作的资源，本文所述系统涉及到素材、概念、范畴、以及本体等对象。

（2）操作（Performance），指对象能够接受的外部操作，例如对象是文件夹，那么相关的操作有创建、删除、查看和更新文件夹等。这里有这样一个假设（虽是假设但也是共识），即一旦对象创建完成，那么其具备的操作类型也是明确的，否则操作和之后的权限管理将处于无序状态。

（3）权限（Right），指对一个对象施行的操作，例如文件夹的创建者对文件夹有修改与删除的权限，而其他用户只有查看的权限。图 2 中椭圆形的虚线框表示的权限为对文件夹进行删除。

（4）任务（Task），是系统或者用户对对象施加的操作，即完成一项或者几项动作，在具备安全管理能力的系统中，需要判断任务的有效性，例如一个任务是删除文件夹，那么首先判断发起这个动作的用户是否有此权限。

用户是任务的发起者，是权限的约束主体，而对象是约束的客体，操作是约束的范围。

角色和用户的关系是角色包含用户，即分配用户到相应的角色中（为用户赋予某个或者某几个角色）。在角色管理中，通过角色定义对象的操作授予用户权限。

3.2 角色的作用

角色是一组特权，对某些对象具有一系列操作的权限，角色可以分配给用户或者其他角色，即角色嵌套角色，是否需要嵌套取决于系统对安全管理的复杂程度。角色的优点可以总结为如下几点：

（1）特权不是每次直接授予一个用户；而是先创

建角色，向该角色授予一些特权，再将该角色授予多个用户或者其他角色。

(2) 在增加或者删除一个角色的某种特权时，被授予该角色的所有用户和角色都会自动获得新加的特权或自动失去这种特权。

(3) 可以将多个角色授予一个用户或角色。

(4) 可以为角色设置单独密码。

(5) 可以基于角色设置其他功能。

角色管理有助于对授予多个用户的多种权限进行相应的管理。

3.3　角色的设置

一般系统在设定角色时有两个默认角色：超级管理员以及公共用户，本文在以上两个角色的基础上设计了单位管理员、个人用户等角色。

(1) 超级管理员具有最高权限，即能够对所有对象进行所有类型的操作，一般在系统建成后，由系统分配超级管理员。

(2) 单位管理员是每个单位的总负责人，负责签收超级管理员为本单位设定的任务和权限，并管理本单位的用户和资源等内容。

(3) 个人用户，个人用户隶属于单位，由单位管理员创建，并被授予权限和任务，是实际任务的执行者。

(4) 公共用户，对系统中的对象仅具有查看的权限。一般默认设置公共用户是最低权限，创建一个用户时默认赋予该用户为公共用户的角色。

4　角色管理功能设计

4.1　角色管理功能模块

角色管理模块应该具有创建、删除、修改和查看角色的功能，能够激活和禁止角色及其权限，为角色增加用户，为角色创建权限。用户角色管理功能模块如图 3 所示：

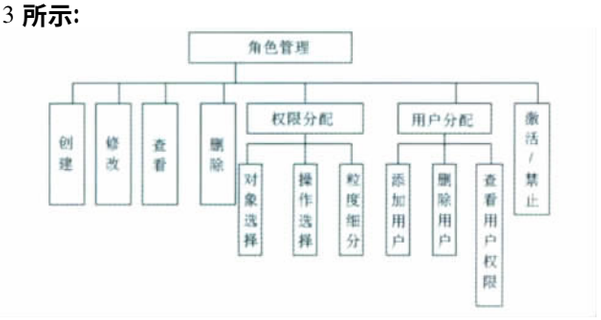

图 3　用户角色管理功能模块图

(1) 创建：定义角色的基本属性，例如角色名称等。

(2) 修改：对角色基本属性进行修改。

(3) 查看：查看角色列表，浏览角色包含的用户以及角色所具有的权限。

(4) 删除：删除建立的角色，同时角色中包含的用户所具有相应的权限也被撤销。

(5) 权限分配：定义角色能够操纵的对象，以及对这些对象能够施加的操作。

(6) 用户分配：为角色添加用户。

(7) 激活/禁止：根据实际需要激活/禁止角色。

4.2　角色作用的逻辑流程

角色发挥作用在于控制用户对对象的操作，即判断用户是否有权限完成任务，宏观层面上任务是指分配给单位或者个人用户的工作，微观层面上任务是可对一系列对象实施若干操作的集合。登录用户通过角色控制其是否有权限完成任务的逻辑过程，如图 4 所示：

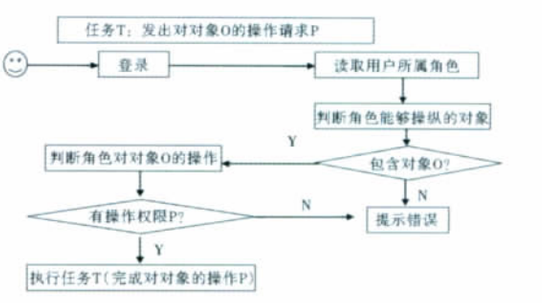

图 4　角色管理通过权限控制用户完成任务 T 的逻辑过程

用户登录以后，将要执行任务 T(Task)，即发起对某个对象 O(Object) 的访问请求或者其他操作请求 P(Performance)。判断登录用户是否有执行一项任务的权限，首先需要判断该用户所属的角色(可以是多个角色) R(Roles)，判断 R 是否有对对象 O 的操作权限：如果没有，提示错误；如果有，则判断对 O 的操作类型是否包含 P，如果没有包含 P 则提示错误，如果包含对 O 的操作类型 P，则执行该任务 T。

5　系统实现

5.1　科技知识组织体系构建系统中角色划分

科技知识组织体系加工的主要内容包括理、工、

农、医4个领域的素材、概念、范畴以及本体4个纵向层次，每个层次包含不同类型的内容，其他内容包括：日志及版本信息等。科技知识组织体系构建系统将用户角色划分为4大类。

(1) 超级用户

在系统构建的过程中设置超级用户。超级用户拥有对所有对象的操作权、最终的审核权，其最主要的功能是管理单位用户角色，科技知识组织体系构建系统中设置一个超级用户，为理、工、农、医4家单位设定相应的角色，分配需要加工的内容，并赋予操作权限。

(2) 单位用户

单位用户由超级管理员分配，分别指中国科学院文献情报中心、中国科学技术信息研究所、中国农业科学院农业信息研究所以及中国医学科学院医学信息研究所。单位用户对外负责签收超级用户分配的任务，对内负责管理本单位用户，并分配任务，同时负责本单位加工知识组织体系内容的初步审查。

(3) 个人用户

个人用户由单位用户创建，个人用户可来自于单位内部，也可来自于单位外部，是知识组织体系创建、编辑等任务的实际执行者。个人用户角色又可分为更细一级的角色，例如在单位中设置知识组织体系创建角色、审核角色等。

(4) 公共用户

公共用户具有最低级别的权限，仅可以检索与查看知识组织体系中的内容。

5.2 科技知识组织体系构建系统中角色分配实施

在角色管理模块的功能描述中重点展示单位用户给个人用户分配权限的过程，例如中国医学科学院医学信息研究所(简称医科院信息所)单位用户为本单位工作人员(个人用户)分配任务，即将指定的操作权限赋予系统中需要管理的内容(对象)。图5是医科院信息所设定本单位用户角色，选择该决策可操作的对象(资源)，以及施加在备选对象上的操作类型。

点击“高级”可以对对象的粒度进行细分。例如在素材层(灰色底纹表示选中素材层，如果不在高级中进行操作说明对对象的所有内容都具有权限)。图6为医科院信息所单位用户为下属个人用户设置可操作的对象，是对对象的进一步细分。

在概念层次点击“高级”，可按照领域来分配可操作的对象，范畴层可按照节点分配操作对象，本体层可按照本体类型等进行角色设定。图7为角色选定个人用户。

角色管理

角色名称：医科院信息所单位用户

权限分配						用户分配	
	对象	查看	创建	更新	删除	统计	操作…	操作n
□	用户	□	□	□	□	□	□	□
√	素材	√	□	√	□	□	□	□
□	概念	□	□	□	□	□	□	□
√	范畴	√	√	□	□	□	□	□
□	本体	□	□	□	□	□	□	□
□	日志	□	□	□	□	□	□	□
□	版本	□	□	□	□	□	□	□
□	…	…	…	…	…	…	…	…
高级…								

图5 医科院信息所为本单位用户角色分配权限

角色管理

角色名称：医科院信息所单位用户

操作对象：素材

选择	素材名称	素材描述
√	MeSH Concept	……
□	SNOMED-CT	……
√	LONIC	……
□	……	……

图6 为隶属于本单位的用户角色设定操作对象

角色管理

角色名称：医科院信息所单位用户

权限分配				用户分配
	用户名	真实姓名	单位	描述
□	Lyz	XXXX1	单位1	XXXX1是系统部的……
√	Sunhx	XXXX2	单位1	XXXX2是资源部的……
□	Xiangj	XXXX3	单位1	XXXX1负责……
□	……	……	……	……
查看…				

图7 为角色添加个人用户

为角色选定用户，使其具备执行具体任务的权限。点击“查看”可以看到该用户具有的所有权限(操作的对象以及对对象拥有的操作类型)。通过勾选完成增加或删除。

6 结 语

本文的角色管理功能模块初步实现了对理、工、农、医4个单位及个人用户操作权限进行管理，为分布式协同加工超级科技词表内容奠定了基础，为充分利用领域专家的专业知识提供了技术手段。角色管理仅是协同加工系统的基础部分，而对资源操作的并发控制以及依赖关系的管理等将是未来研究的重点内容。

参考文献:

[1] Zhu H. Conflict Resolution with Roles in a Collaborative System [J]. *International Journal of Intelligent Control and Systems*, 2005, 10(1): 11 – 20.

[2] Tolone W, Ahn G J, Pai T, et al. Access Control in Collaborative Systems [J]. *ACM Computing Surveys*, 2005, 37(1): 29 – 41.

[3] Li D, Muntz R. Role – based Conflict Resolution Method for a Collaborative System [C/OL]. In: *Proceedings of the* 1998 *ACM Conference on Computer Supported Cooperative Work*(*CSCW'*98). New York, NY, USA: ACM, 1998: 179 – 188. [2012 – 12 – 01]. http://dl.acm.org/citation.cfm?id=289492.

[4] 李亚子,钱庆,郭文丽,等. 大规模本体协同构建框架研究与设计 [J]. *图书情报工作*, 2011, 55(12): 96 – 100. (Li Yazi, Qian Qing, Guo Wenli, et al. Research and Design of Collaborative Construction Framework for Large Scale Ontology [J]. *Library and Information Service*, 2011, 55(12): 96 – 100.)

[5] Administration Guider of Drupal [OL]. [2012 – 12 – 16]. http://drupal.org/documentation/administer.

[6] Web Protégé [OL]. [2012 – 12 – 16]. http://protege.stanford.edu/.

[7] WebOnto User Guider [OL]. [2012 – 11 – 16]. http://new.euromise.org/mgt/webonto/main.html.

[8] 田晓迪. Ontolingua Server: 全球第一个本体服务器 [J]. *现代图书情报技术*, 2006(2): 21 – 25. (Tian Xiaodi. Ontolingua Server: The First Ontology Server in the World [J]. *New Technology of Library and Information Service*, 2006(2): 21 – 25.)

[9] Web Protégé Wiki [OL]. [2012 – 12 – 16]. http://protegewiki.stanford.edu/wiki/Protege_Client_Server_Tutorial_Configuration#The_Metaproject.

[10] Domingue J. WebOnto User Guide (1.0) [OL]. [2012 – 12 – 16]. http://new.euromise.org/mgt/webonto/main.html.

[11] 普里斯. Oracle Database 10g SQL 开发指南 [M]. 冯锐,由渊霞译. 北京: 清华大学出版社, 2005: 400 – 500. (Price J. Oracle Database 10g SQL Developer Guider [M]. Translated by Feng Rui, You Yuanxia. Beijing: Tsinghua University of Press, 2005: 400 – 500.

(作者 E – mail: qian.q@imicams.ac.cn)

OpenAIRE 发布第二版 OpenAIRE 指南

OpenAIRE 指南 2.0 促使 OpenAIRE 可以达到机构知识库和知识库服务聚合器(Aggregator)的兼容。实施该指南,知识库管理者使作者可以更容易地将他们的出版物存入符合欧盟委员会开放获取要求的知识库中。对知识库平台开发者来说,该指南为在未来的平台中为欧盟委员会所资助的作者增加支持性功能提供了指导。

与以前的指南版本相比,2.0 版本有两个主要变化:

(1) 促进聚合器与 OpenAIRE 的兼容,使它们的元数据可以在 OpenAIRE 基础设施上显示。

(2) 扩展命名空间以支持对项目的标识。扩展的命名空间将提供表达项目信息的通用方式,它不仅仅可用于欧盟委员会或第七框架计划项目,还可用于国家或国际的任何其他资助者和项目。虽然指南建议使用扩展命名空间,但已经与 OpenAIRE 兼容的知识库和期刊可以使用指南的强制规定部分(与 OpenAIRE 指南 1.1 相同)来保持兼容性,而不需要进行额外的工作。

对于第二点,在指南的未来版本中将寻求表达项目信息的更可持续的解决方案,这可能包括引进资助机构和资助计划词汇表、以关联数据的形式以及与 CERIF 标准兼容的方式展示信息。

(编译自: http://www.openaire.eu/en/home/9-news-events/427-openaire-releases-version-20-of-the-openaire-guidelines)

(本刊讯)