科学基金管理系统的用户权限管理模式研究

李 东[1],施懿闻[2],郝艳妮[3],毛基业[2]
(1. 国家自然科学基金委员会 信息中心,北京 100085;
2. 中国人民大学 商学院,北京 100872;
3. 爱瑞思软件(深圳)有限公司,广东 深圳 518057)

摘 要:针对科学基金管理系统权限管理的灵活需求,文中总结了当前主流的访问控制模型和行业最佳实践,并设计了"角色-项目"松耦合的权限管理模式。通过一个具体案例显示,通过合理的角色结构设计,结合基于工作流、角色等级的RBAC模型,该模式可以有效解决大型科学基金管理系统所面临的用户权限管理问题,如难以实现时间维度的控制、不能分级授权等问题,并能适应业务需求的发展和变化。此外,文中提出的信息系统权限管理模式的设计思路,弥补了目前权限管理领域缺乏的应用研究。

关键词:权限管理;访问控制;角色结构
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2012)02-0159-06

Research on Access Control to Grant Management Systems

LI Dong[1],SHI Yi-wen[2],HAO Yan-ni[3],MAO Ji-ye[2]
(1. Information Center,National Natural Science Foundation of China,Beijing 100085,China;
2. School of Business,Renmin University of China,Beijing 100872,China;
3. IRIS Systems (Shenzhen) Co.,Ltd,Shenzhen 518057,China)

Abstract:In response to the need for flexible access control to research grant management systems,it reviews the current access control models and best practices,and proposes a "role-project" loose coupling model for access control. Conducted a case study to show that,through proper role structure design and RBAC based on workflows and role hierarchy,the model can solve problems faced by a large research grant management system,e.g.,difficulties with time-based control and the inability to allow decentralized delegation of access privilege. It is also shown that the model can adapt to changes arising from rapid business development. Moreover,propose a generic approach to design solutions for access control to information systems,to make up for the lack of application-oriented research in this field.
Key words:management of access privilege;access control;role structure

1 概 述

各种企业和组织通常由于业务需要而保存大量重要数据。随着信息化的不断发展和深化,系统的数据安全也越来越受到各方的重视。在防止信息泄露和非法修改方面,目前有三种广泛应用的技术:授权、访问控制和审计[1]。其中前两者属于权限管理的范畴,是信息系统安全管理的重要手段,可通过和人事数据的结合,根据用户角色的属性,对角色进行横向分类等权限管理方法,实现较为灵活的管理模式[2]。

权限管理的关键在于访问控制策略,它决定了在设计权限管理体系时可以控制的权限维度,如时间、空间等。目前在访问控制领域已有较多的研究成果,其中基于角色的访问控制模型(RBAC)是目前最为流行的[3~7]。在此基础上有诸多的延伸,如基于工作流的RBAC模型、空间感知的RBAC模型等。这些模型为实际信息系统的权限管理模块提供了理论基础。

已有研究的重点主要集中在如何利用计算机技术实现访问控制模型。在权限管理的实际应用中,企业所面对的问题更多是如何根据自身的业务需求探索其信息系统的权限管理模式,如根据业务类型或组织机构的不同制定个性化的权限管理方案等。而根据企业业务特点和权限管理需求设计式,建立角色体系来合理应用访问控制模型及相关的案例研究尚少。希望通过案例研究,从权限管理领域的个体应用中总结出一般性的思路,为企业信息系统的权限管理模式提供借鉴和方法。

收稿日期:2011-06-30;**修回日期**:2011-10-09
基金项目:国家自然科学基金专项基金项目(M1021006)
作者简介:李 东(1970-),女,天津人,高级工程师,硕士,研究方向为计算机软件、数据挖掘技术与方法;毛基业,教授,博士生导师,研究方向为信息系统管理和电子商务。

某基金委的科学基金网络信息系统已运行十一年,随着基金项目数据量、业务工作量的快速增长,各级管理部门及管理人员对信息安全的要求不断提高,业务系统平台及技术在数据访问、信息安全管理、监督审计等方面需要进一步的改进。

文中以该科学基金管理单位为例,根据其工作的灵活性、保密性等特点,为其主要业务系统设计一种灵活的权限管理模式。文中也为如何依据企业的业务特点和权限管理需求,有效利用文献中已有的访问控制模型来设计信息系统的权限管理模式提供参考意见。

2 文献回顾

本节主要回顾权限管理中访问控制领域的前沿文献,以及西门子公司和欧洲某银行在用户角色的横向及纵向结构方面进行的研究,在应用层面对权限管理的前沿文献进行较为全面的梳理,并从两方面为之后的案例研究进行理论支持。第一,访问控制模型作为权限管理的基础,明确了在进行权限管理模式设计时可以实现的控制维度(如时间、角色层级等)。第二,角色结构的研究为权限管理中角色层的设计提供了一定的支持。

2.1 访问控制模型

基于角色的访问控制(RBAC)是目前最主流的,得到了国内外研究者的认可[3~7]。基于不同的组织业务和环境需求,在 RBAC 的基础上不断进行扩展,主要在权限管理中添加了时间维度、空间维度和支持角色委托的限制。下面将分别进行描述。

文献主要权限管理模型见表 1。

表 1 文献主要权限管理模型

模型	主要内容
基于角色的访问控制	分配给每个用户一个合适的角色,并且每一个角色都有对应的权限
基于工作流的动态访问控制	通过添加任务维度,将访问控制的二维矩阵(Z: S×O->P)扩展为三维
空间感知的 RBAC 模型	将用户的访问位置作为确定权限规则的决定因素之一
基于角色的委托模型	主体将系统中的权限委托给其他主体,以便以前者的名义进行工作

2.1.1 基于角色的访问控制

该模型的基本思路是在用户和权限之间引入角色的概念。Ferraiolo 和 Kuhn(1992)首次提出 RBAC,并且给出了如角色激活、层次角色和限制等[5]。由于 RBAC 模型可以有效地减少相应的管理成本,有关的研究和应用得到了迅速发展。Ferraiolo 等(1995)和 Sandhu 等(1996)都提出了有关 RBAC 模型的早期形式化定义[6,7],其中 Sandhu 等(1996)给出了比较完整的框架——RBAC96。

RBAC96 是个模型族,其中包括 RBAC0 ~ RBAC3 四个概念性模型。首先,RBAC0 是基本模型,定义了支持 RBAC 概念的系统最低需求。其次,RBAC1 和 RBAC2 都包含了 RBAC0,且各自增加了独立的特点,称为高级模型。RBAC1 增加了角色分级的概念,一个角色可以从另一个角色继承权限。RBAC2 增加了一些限制,强调在 RBAC 的不同组件中在配置方面的一些限制,例如互斥角色的限制。最后,RBAC3 称为统一模型,其包含了 RBAC1 和 RBAC2。以下将详细讨论分层角色的方案。

权限角色的层级,可以自然地反映组织层级中的授权和职责。按照惯例,功能更强大(高级)的角色在图表顶部显示,功能较弱(初级)的角色在底部。如医师是相对高级的保健提供者,所以,它不但可以继承保健提供者这个角色的所有权限,还可以拥有自己额外的权限。而且继承是具有传递性的,初级保健医师这一更高级角色继承了医师和保健提供者两个角色的权限。除了继承医师的权限,初级保健医师和专科医师也有直接分配给他们的不同权限。在多重继承中,项目主管同时从测试工程师和程序员的角色继承权限。

从数学的角度,这些层级应该是偏序的。偏序是一种自反、传递和反对称的关系。继承是自反的,因为一个角色继承自己的权限;传递性是此情境的一个必然要求,而反对称性可以避免由于角色相互继承而带来的冗余[8]。

层级的角色结构中,角色可以有重叠功能,即用户可以属于不同的角色但分配了部分相同的权限。针对这个特点,对于一些组织,其拥有大量的用户需要分配一些常规的权限。这样,需要大量重复的权限分配的工作,从而使权限管理变得异常繁琐。设计层级结构的角色,可以更好地支持组织的内部结构,也可以提高系统效率。这种结构可以与核心的 RBAC 很好地结合,同时也在现有的 RBAC 中得到广泛的实际应用[9]。

简而言之,RBAC 就是将权限赋给角色,角色分配给用户[3,4]。用户和访问权限没有直接的关系,但通过角色共同决定了权限管理的规则。该模型的优点是提高了权限管理的灵活性,且拓展性高,易于维护。

RBAC 模型已非常成熟,目前已广泛应用于各类企业、政府,及高校的信息系统,是最基础也是最普遍的一种权限管理模型。但是 RBAC 模型没有提供操作顺序的控制机制,难以应用于有严格操作顺序的系统。这会产生如下缺点:主体在执行任务以前就拥有权限,或在完成任务后继续拥有权限,会导致主体拥有额外的权限,不符合最小授权原则,使系统安全面临风险。

2.1.2　基于工作流的动态访问控制

由于RBAC的授权是静态的,给其应用带来了一定的局限性,解决这一问题的主要方法就是采用动态授权的基于工作流的访问控制模型。该模型在决定访问权限时,不仅要考虑主体与客体,还需要考虑到主体和主体当前执行的任务及任务的状态。通常情况下,任务的状态包括:静止态、活动态、挂起态、终止态和夭折态。只有某任务在活动状态下,才可以拥有相应的权限[10]。

该模型的难点在于如何保证一些权限的基本限制,如应自动将角色权限归为当前任务的最小权限,并保证动态的责任分离,即一个任务与主体的任何一个当前活动任务都不互斥时,这个任务才能授权给该主体。Joshi等(2005)对这类有时间特性的RBAC模型的用户层级和权限分离限制进行了研究[11]。

由于该模型依赖特定工作流,一旦工作流有所变动,所带来的权限更改会十分巨大。此外,即使在工作流系统中,并不是所有用户都有执行任务的权限。单纯采用工作流访问控制模型会提高系统开发和维护的复杂度,以及系统运行的效率。所以,可以针对任务的类型将任务划分为工作流任务及非工作流任务,可将非工作流任务的访问权限进行静态绑定,避免不必要的更改[12]。

基于工作流的动态访问控制模型在各类信息系统中,尤其是办公自动化(OA)、电子商务和电子政务等领域得到了广泛关注。如在OA系统的核心——公文流转,解决了在工作流进程中主客体属性的适时变更及访问过程的连续性控制问题。

2.1.3　空间感知的RBAC模型

随着互联网的广泛应用,信息系统与互联网的结合越来越紧密,使用户可以利用更多的设备,在更广泛的时空获取系统资源,但随之带来的也是更多的安全隐患。所以,地点也成为了影响访问控制决策的重要因素[13,14]。例如,用户在非办公地点访问系统,则需要更高级别的权限,即地点决定了用户实际采用的权限规则。Damiani等(2007)提出了结合空间感知的RBAC模型(GEO-RBAC)[13]。该模型中的地点仍是一个逻辑概念,而并不是物理坐标。一旦用户处于移动的状态,所处的地点发生改变,权限规则应做如何的调整。

该模型的应用存在两个难点:第一,如何确定用户所在的地点,以及确定用户所在地点技术(如GPS)的可用性及有效性。第二,如何制定用户在不同地点所采用的权限规则。该模型在国内研究有限,当前主要集中在理论阶段,尚未有相关的实施和部署方案,今后的研究需要注重将模型和实际实施结合在一起。

2.1.4　基于角色的委托模型

委托是一种重要的安全策略,其主要思想是系统中的主体将权限委托给其他主体,以便以前者的名义进行工作。在组织中,三种情况可能发生委托[15]:

职能备份:某人出差或长期休假,因而需要将其工作权利委托给他人,以保证其工作可以继续。

工作协同:组织间或组织内需要协同工作时,可能需要以委托的方式给用户授予一定的权限。

权限下放:当某一组织建立或者重组后,权限可以通过委托的方式从高级角色向低级角色扩散。

Barka和Sandhu(2000)最早讨论了基于RBAC的委托策略,并提出了基于角色的委托模型:RBDM0[15]。但该模型不支持角色层次、部分委托和多步委托。在此基础上,Zhang等(2001)提出了RDM2000模型,解决了角色层次和多步委托的问题,但与RBDM0类似,委托也是粗粒度的,即只支持角色级别的委托[16]。PBDM模型解决了部分权限委托的问题。其中部分委托是通过委托人创建临时角色并分配相应的委托权限来实现的[17]。这种方法需要创建大量临时性角色,从而导致权限管理十分复杂。

Crampton和Khambhammettu(2007)提出,权限委托有两种形式:授予和转让[18]。其中,授予模式是指,在委托成功后委托人和受托人均有所委托的权限;而转让模式是指,在委托成功后,访问的权利就转移至受托人,而委托人将不再拥有该权限。之前的研究多围绕授予模式委托展开,而对于某些业务包含敏感权限,不希望将此权限提供给较多的用户,通常会对拥有权限的用户数加以限制,转让模式的委托会更适合此类业务。但转让模式的委托机制会由于其非单调性,实现起来比授予模式复杂的多。

国内研究者在基础委托模型的基础上,提出角色委托具有临时性、受限传播性、常规角色关联性、部分性等特点[19~22],把限制引入角色委托模型将成为研究的热点。中国科学院软件研究所信息安全国家重点实验室目前在此类模型方面研究水平较为领先,并采用形式化语言建立了模型,为具体的实施打下了基础。目前国内应用此类模型的例子尚少。

2.2　角色结构

角色结构的设计与权限管理有着紧密的联系,但是对角色的定义仍存在一些问题。比如,有些角色明显缺乏粒度,如何将角色与组织结构紧密地结合在一起。这些问题可以通过不同的角色结构的设计进行解决。

关于角色的横向结构,可以有不同的分类进行组织。以西门子公司的某系统为例[2],其根据角色不同维度的特点,将角色分为职能角色、组织角色、基本角

色、层级角色和特殊角色五类。这种分类方式降低了角色管理的复杂性，可以使业务环境的变化降低到一个角色分类。“基本角色”、“层级角色”和“组织角色”这些分类都可以快速的定义。主要关心的是“特殊角色”这个分类，因为它通常是临时定义的。对于“职能角色”这个分类必须事先对需求和角色调查过程进行调研。角色调查的目标在于减少角色的数量，以及加强角色在组织重构时的健壮性。

关于角色的纵向结构，以下以一个欧洲银行的基于角色的访问控制系统为例[23]进一步说明。该银行的系统角色定义由行政职位（如：职员、部门经理、区域经理等）和岗位职能（如：财务分析、软件工程师等）两者共同决定。另外，用户所属的部门也是一些应用系统访问控制规范的一部分。这种角色定义原则支持角色层级和访问权限继承。

例如，组织中存在如下行政职位：

区域经理 > 部门经理 > 职员

但在没有结合岗位职责的情况下，这种层级并没有什么意义。比如“财务分析/部门经理”（角色 B）这一角色会比“财务分析/职员”（角色 A）有更多的权利，但“软件工程师/部门经理”和“财务分析/职员”因为岗位职责不同，并没有类似的层级关系。

本节通过对权限管理前沿文献的梳理，总结了目前主流的访问控制模型，以及在实际应用中角色结构设计的一般思路。但目前关于如何将这些模型有效的结合并落实在信息系统权限管理中的研究尚少。很多组织仍旧面临权限管理不能适应其业务需求，如不能根据业务类型灵活配置不同的工作流和时间约束，或在不同的组织机构中进行个性化的权限管理。以上问题是目前的研究所难以解决的。所以，针对以上问题，文中通过对理论模型的梳理、实践经验的总结，将以某基金委的业务系统为例，在现有访问控制研究的基础上，展开对权限管理体系及管理模式的研究探索，对其他企业信息系统所面临类似的问题给予解决思路。

3 应用实例

以某科学基金委的业务系统——项目信息管理系统为例，从分析科学基金管理系统的权限管理需求出发，通过总结和分析，设计一套满足其需求的权限管理体系，并解释信息系统权限管理模式设计的思路。

首先，通过总结和该基金委工作人员的访谈得到其目前面临的问题，抽取出当前在权限管理方面的需求和挑战。然后，结合前沿文献中的访问控制模型和角色结构，通过不同的权限管理维度，将其有效地结合，形成满足该基金委需求的角色体系。并且实现了“用户-项目”松耦合的权限管理模式，通过权限管理中稳定的维度间的灵活映射关系，来满足其个性化的权限管理需求。最后，将方案的设计思路进行总结，为面临类似问题的企业给予更具普适性的结论。

3.1 权限管理需求和挑战

需求分析是通过对某基金委工作人员的多次调研，通过对其描述的问题情境进行提炼，总结出其在权限管理方面存在两个主要需求。

（1）分级授权。

分级授权是该基金委的权限管理工作目前最重要的需求之一。根据各项目管理部门存在大量的“流动项目主任”和“兼聘用户”等非内部工作人员，并且每个学部对这两类工作人员的权限需求相对独立的业务特点，项目信息管理系统的权限全部由信息中心统一管理。这样会造成权力过于集中，增加了信息中心工作量，同时也带来一些管理问题。例如，各项目管理部门新进兼聘用户后，必须通过信息中心才可以为其开通或变更权限，频繁的权限调整难以高效实现。而且还会出现，在兼聘用户离职后，项目管理部门没有与信息中心及时沟通关闭相应权限，从而带来了信息泄露的隐患。相关监审部门也认为分级授权更为合理。

（2）时间维度的控制。

时间维度的控制有两方面含义。

第一，系统中各操作的有效时间。

根据每年该基金委内部的《项目管理主要工作进程安排》，各类项目的每一项操作都有时间的控制。目前只有依靠人工手动方式在规定时间开启/关闭相应的操作权限。会出现为了统计需要，在受理集中项目时，必须关闭非集中受理项目的申请权限，造成业务中断。

第二，针对“兼聘用户”此类临时角色，流动性较大，其赋予权限的有效期应到期收回，原系统不支持自动收回。

通过对以上需求的分析，总结出其权限管理工作具有以下特点：

1）组织结构稳定；

2）各类型的基金项目管理工作流程有很大不同，但某一类型的管理工作流程较为稳定；

3）人员与项目的映射较为灵活；

4）流动/兼聘人员较多，人员工作时间特点明显。

所以主要面临的挑战在于，在权限管理结构的设计时，需要满足该基金委相对稳定的组织结构与项目流程可以进行分别管理的特点，并通过较为灵活的映射关系满足其不断变化的需求。

3.2 科学基金管理系统的角色体系

权限管理的整体框架依旧采用基于角色的访问控制模型（RBAC）。RBAC 模型为一个三层结构，分别为

用户层、角色层和权限层,如图 1 所示。

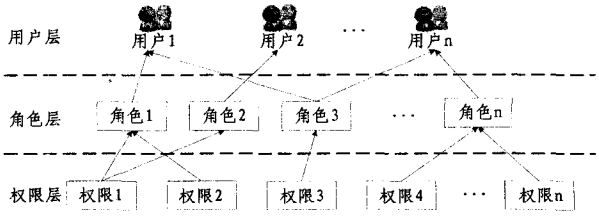

图 1　基于角色的访问控制模型的三层结构

权限层为原子级的权限,根据主体、客体和操作三个要素定义权限。

角色层是根据岗位职能、组织结构等特性,将各个权限分配至不同的角色。角色与权限是多对多的映射关系,即一个角色可以拥有多个权限,且每个权限可以赋给多个角色。角色层的设计是整个权限管理的关键。

用户层即系统的实际用户。用户与角色的映射也是多对多的,需要根据用户实际的工作需要,为其分配相应的角色。

所以,角色层的设计是整个权限管理的关键,因为这一层是连接原子级权限和实际用户的桥梁。在角色层的设计中,将根据该基金委在时间、角色层级等个性化需求的实际情况,将项目信息管理系统的用户权限由角色层级、组织机构、项目类型三个维度进行控制,建立一个立体的角色体系,如图 2 所示。

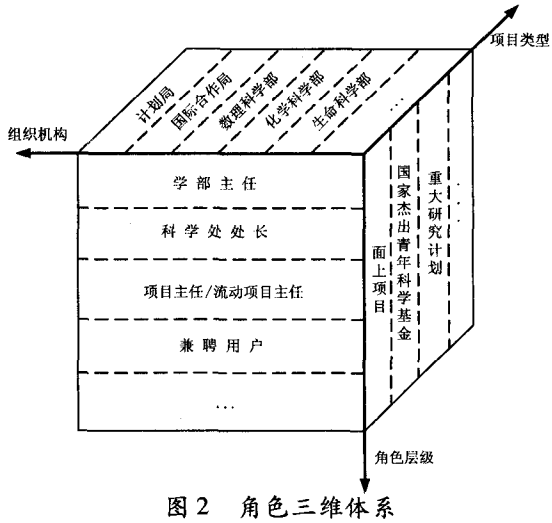

图 2　角色三维体系

主要访问控制点根据对该基金委权限管理需求的抽象得到,每一个控制点都将有一个或多个权限维度进行控制,如表 2 所示。

3.3　科学基金管理系统权限管理模式

根据该基金委较为稳定的用户结构和项目管理流程,以及映射灵活的权限管理特点,设计“用户-项目”松耦合的权限管理模式,让两个相对稳定的要素可以灵活地映射。并通过组织结构、角色层级和项目类型三个维度对用户的权限进行控制(如图 3 所示)。在角色层级和项目类型三个维度的管理中,分别采用了支持角色层级的 RBAC 和基于工作流的 RBAC,解决了分级授权以及工作流控制和时间控制等问题。

表 2　主要访问控制点

访问控制点	描述	控制维度
工作关键时点	根据该基金委管理工作计划,对各类项目时间关键点进行限制	组织结构项目类型
工作流控制	根据不同类型项目的业务流程,进行工作流的控制	项目类型
分级授权	根据该基金委工作需要,可以以管理部门为单位,赋予相对灵活的权限	角色层级

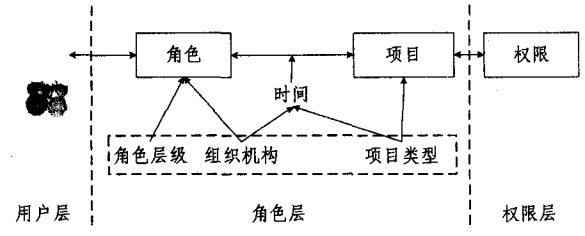

图 3　“角色-项目”的松耦合权限管理结构

“角色-项目”的松耦合的权限管理模式,主要由三个维度构成:组织机构维度、角色层级维度和项目类型维度。以上三个维度的权限管理分别遵循以下的原则。

第一,组织机构维度:

以其组织结构为横向划分依据。

各项目管理部门有相对独立的权限分配方法。

根据该基金委每年的管理工作进程,下一级部门可以根据上一级部门的工作安排,由领导在当前的时间约束内确定自己的工作进程。

第二,角色层级维度:

每个项目管理部门都有对应的纵向层级结构。

科学部的管理结构是:科学部主任—>科学处处长—>项目主任/流动项目主任—>学科赋权用户。

计划局的管理结构是:主管局长—>项目主管处处长—>处员。

国际合作局的管理结构是:主管局长—>地区处处长—>处员。

信息系统根据人事部门提供的工作人员名单,建立业务系统用户字典,根据管理工作的分工,统一授予系统角色,委外用户则由学部主任根据实际需要分配系统权限。

各项目管理部门中,上级角色可以查看其下级角色关键操作,授权人有权查看其赋予被授权人的操作。

第三,项目类型维度:

针对不同类型的基金项目(如面上项目、重点项目、国家杰出青年科学基金等),制定各自的工作流程模板。

由此,该基金委项目信息管理系统的权限管理工作可以通过以上三个维度展开。已按照问题情境设计了包含验证点的案例,来验证"用户-项目"松耦合权限管理模式的有效性。以该基金委比较关心的分级授权问题为例,通过设计以下案例,证明该角色体系可以通过某一组织的上级角色根据本组织的需求为下级角色赋权。并解释了如何通过"角色-项目"的松耦合权限管理模式开展分级授权的权限管理工作。

案例:数理科学部与生命科学部分别招聘了两名兼聘用户A和B,其权限分别由其所属部门的上级角色"科学处处长"设置。其权限如表3所示:

表3 权限设计

用户	角色层级	所属部门	权限
A	兼聘用户	数理科学部数理科学一处	负责数理科学一处中A0101项目的信息录入
B	兼聘用户	生命科学部生命科学四处	负责生命科学四处所有面上项目的信息录入

权限管理步骤:

第一,确定两名用户"角色层级"和"组织机构"的属性。

第二,根据以上两个属性确定AB两名用户在角色框架中的位置,并确定其上级角色。

第三,由上级角色根据本部门的规定,为A和B划分权限。可以根据项目申请代码和项目类型两个维度,限定其管理项目的范围。

最后,希望通过这个案例研究,抽象出设计信息系统权限管理模式的思路,从而弥补目前在信息系统权限管理研究中多理论模型研究,而缺少通过应用现有的技术手段来解决实际问题方面研究的现状。通过对某基金委的案例研究,提出在设计权限管理模式时,首先,需要对系统管理的业务逻辑有深入的理解,从而总结出需要信息系统从哪些方面对业务进行控制,如时间、用户等级、用户所属组织等。其次,根据每一类控制点寻找契合的访问控制模型,并明确相应的控制维度。再次,通过不同维度间的映射,形成权限管理体系。最后,需要通过实例的验证,考察该权限管理体系的有效性。

4 结束语

文中主要系统性梳理了权限管理中访问控制等领域的行业最佳实践、理论研究前沿和某科学基金委的实际需求,有效地利用了这三方面研究和调研成果。具体而言,首先系统地总结了当前主流的访问控制模型,以及角色结构设计的方法。其次,在案例研究中,通过搭建立体的角色结构,为该科学基金委的信息系统权限管理模式给予了合理的解决方案。通过合理的角色结构设计,结合基于工作流、角色等级的RBAC模型,"用户-项目"松耦合的权限管理模式已经可以解决目前该基金委信息系统中面临的业务挑战,如难以实现时间维度的控制、不能分级授权等问题。并且在一定程度上支持了业务变化的需求。

文中提出的信息系统在设计权限管理模式时的思路,弥补了目前权限管理领域缺乏的应用研究。通过对科学基金在信息系统权限管理面临问题的梳理,总结了当前科学基金信息系统权限管理中面临的挑战。为某科学基金委的项目管理系统的权限管理进行的方案再造与验证,解决了其当前面临的重要管理问题,并提炼了方案的设计思路,对相关科学基金机构的管理信息系统的权限管理方案和设计方法方面有一定的参考价值。

参考文献:

[1] Fernandez-Medina E, Trujillob J, Villarroelc R, et al. Access control and audit model for the multidimensional modeling of data warehouses[J]. Decision Support Systems, 2006, 42(3): 1270-1289.

[2] Roeckle H, Schimpf G, Wedinger R. Process-oriented approach for role-finding to implement role-based security administration in a large industrial organization[C]//Proceedings of the Fifth ACM Workshop on Role-based Access Control. Berlin, Germany: [s. n.], 2000: 103-110.

[3] 王延彬,许林英,杨海琛. OA系统中基于角色的用户权限管理[J]. 微处理机, 2008(4): 64-67.

[4] 陈继南,姜 莹,孔祥荣. 基于角色的Web信息系统权限管理方法[J]. 武汉理工大学学报(信息与管理工程版), 2008, 30(2): 265-268.

[5] Ferraiolo D, Kuhn R. Role-based access control[C]//Proceedings of the 15th National Computer Security Conference. [s. l.]: [s. n.], 1992: 554-563.

[6] Ferriaolo D, Cugini J, Kuhn R. Role-based access control (RBAC): features and motivations[C]//Proceedings of the 11th Annual Computer Security Application Conference. New Orleans: [s. n.], 1995: 241-248.

[7] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-based access control models[J]. IEEE Computer, 1996, 29(2): 38-47.

[8] Barka E, Sanduhu R. Role-based Delegation Model/ Hierarchical Roles (RBDM1)[C]//Proceedings of the 20th Annual Computer Security Applications Conference. Tucson, Arizona, USA: [s. n.], 2004: 396-404.

[9] Ferriaolo D F, Sandhu R, Gavrila S, et al. Proposed NIST Standard for Role-based Access Control[J]. ACM Transactions on Information and System Security, 2001, 4(3): 224-274.

(下转第167页)

的数据量是十几万条数据。

表 1　"索引优化"实例的查询数据表

查询条件	>20 岁	>30 岁	>40 岁	>50 岁
使用索引	17.2 毫秒	13.67 毫秒	9.62 毫秒	6.75 毫秒
未用索引	17.56 毫秒	14.45 毫秒	10.43 毫秒	7.61 毫秒

图 1 是经过各种优化手段后输入车牌号码、起始经过时间和结束经过时间后的查询时间。图 1 用到的表的数据量是二十万条左右。

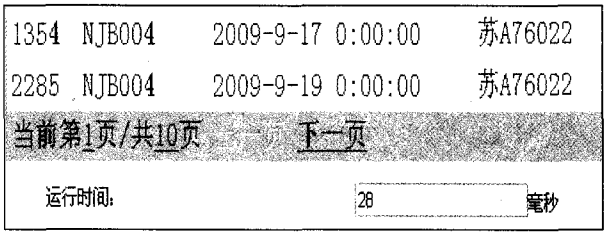

图 1　车辆过车记录查询时间

文中着重从数据库层和应用层方面对查询优化技术进行了详细的讲解,如使用索引技术、分区技术、SQL 语句优化技术和分页查询等等。另外,还可通过升级硬件的方法来提高查询速度。

参考文献:

[1] Willis D, Pearce D J, Noble J. Efficient Object Querying in Java[C]//Proceedings of the European Conference on Object-Oriented Programming (ECOOP). [s. l.]: [s. n.], 2006.

[2] Lee Hyunho, Lee Wonsuk. Query Optimization for Web BBS by Analytic Function and Function-Based Index in Oracle DBMS[C]//Proceedings of Sixth International Conference on Advanced Language Processing and Web Information Technology. SoutheastCon: IEEE, 2007.

[3] Gibbons P B, Matias Y, Poosala V. Fast Incremental Maintenance of Approximate Histograms[J]. ACM Transactions on Database Systems, 2002, 27(3): 261-298.

[4] Conn S S. OLTP and OLAP data integration: a review of feasible implementation methods and architectures for real time data analysis[C]//Proceedings of IEEE. SoutheastCon: [s. n.], 2005.

[5] 袁爱梅. ORACLE 数据库性能优化研究[D]. 上海: 华东师范大学, 2007.

[6] 周　彦, 陈　梅, 王翰虎, 等. 基于层次位图连接索引的数据仓库查询优化[J]. 计算机技术与发展, 2011, 21(3): 41-43.

[7] 刘　博. ORACLE 数据库性能调整与优化[D]. 大连: 大连理工大学, 2007.

[8] 许华容. Oracle 数据查询优化方法研究[D]. 贵阳: 贵州大学, 2008.

[9] 王　君, 祝永志, 魏榕晖, 等. 基于 Oracle 分布式数据库的查询优化[J]. 计算机技术与发展, 2008, 18(1): 157-160.

[10] 杨小艳, 尹　明, 戴学丰. Oracle 数据库查询优化方法研究[J]. 计算机与现代化, 2008(4): 4-7.

[11] 周志德. Oracle 数据库的 sql 查询优化研究[J]. 计算机与数字工程, 2010(11): 173-178.

[12] 邓春娜, 周晓红. Oracle 数据库的查询优化方案[J]. 信息科技, 2010(5): 19-20.

(上接第 164 页)

[10] 陈凤珍, 洪　帆. 基于任务的访问控制(TBAC)模型[J]. 小型微型计算机系统, 2003, 24(3): 621-624.

[11] Joshi B D, Bertino E, Latif U, et al. A generalized temporal role-based access control model[J]. IEEE Transactions on Knowledge and Data Engineering, 2005, 17(1): 4-23.

[12] 陈泉冰, 王会进. 一种改进的基于任务-角色的访问控制模型[J]. 暨南大学学报(自然科学版), 2010, 31(1): 29-34.

[13] Damiani M L, Bertino E, Perlasca P. GEO-RBAC: a spatially aware RBAC[C]//Proceedings of the 10th ACM Symposium on Access Control Models and Technologies. Stockholm, Sweden: [s. n.], 2005: 29-37.

[14] Bertino E, Kirkpatrick M. Location-aware authentication and access control-concepts and issues[C]//Proceedings of the 23rd International Conference on Advanced Information Networking and Applications Workshops. Bradford, England: [s. n.], 2009: 10-15.

[15] Barka E, Sanduhu R. A role-based delegation model and some extensions[C]//Proceedings of the 23rd National Information Systems Security Conference. Baltimore, USA: [s. n.], 2000.

[16] Zhang L H, Ahn G J, Chu B T. A rule-based framework for role based delegation[C]//Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies. Chantilly, Virginia, United States: [s. n.], 2001: 153-162.

[17] Zhang X W, Oh S, Sandhu R. PBDM: a flexible delegation model in RBAC[C]//Proceedings of the eighth ACM symposium on access control models and technologies. Como, Italy: [s. n.], 2003: 149-157.

[18] Crampton J, Khambhammettu H. Delegation in role-based access control[J]. International Journal of Information Security, 2007, 7(2): 123-136.

[19] 廖俊国, 洪　帆, 朱更明, 等. 基于信任度的授权委托模型[J]. 计算机学报, 2006, 29(8): 1265-1270.

[20] 徐　震, 李　斓, 冯登国. 基于角色的受限委托模型[J]. 软件学报, 2005, 16(5): 970-978.

[21] 翟征德. 基于量化角色的可控委托模型[J]. 计算机学报, 2006, 29(8): 1401-1407.

[22] 翟征德, 冯登国, 徐　震. 细粒度的基于信任度的可控委托授权模型[J]. 软件学报, 2007, 18(8): 2002-2015.

[23] Schaad A, Moffett J, Jacob J. The role-based access control system of a european bank: a case study and discussion[C]//Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies. Chantilly. VA, USA: [s. n.], 2001: 3-9.