DOI:10.13718/j.cnki.xsxb.2019.09.013

基于角色和数据可视域的农业科研协同办公平台设计①

李　昀[1]，　吴华瑞[2,3,4]，　邓　颖[2,3,4]，　李庆学[2,3,4]，　顾静秋[2,3,4]

1. 北京市农林科学院，北京 100097；2. 国家农业信息化工程技术研究中心，北京 100097；
3. 北京市农业信息技术研究中心，北京 100097；4. 农业农村部农业信息软硬件产品质量检测重点实验室，北京 100097

摘要： 农业科研单位信息类型和用户组成复杂，业务流程繁琐，给农业科研单位的协同办公、信息共享利用和信息安全管理等带来许多问题和困难. 为了适应科技管理工作发展和科技信息共享服务的需要，系统研究和构建了基于角色和数据可视域，针对多源、复杂和多层级用户的高效管理流程与信息安全主动管理系统；将平台用户横向按部门、纵向按管理等级等进行划分，并对数据资源进行可视域限定，形成用户和数据双向控制的用户权限管理及数据安全控制体系. 构建了既可以实现高效信息加载和共享，又可保持信息安全的农业科研协同办公平台.

关　键　词： 信息流；数据可视域；协同办公；数据分发

中图分类号： TP317.1；S-3　　**文献标志码：** A　　**文章编号：** 1000－5471(2019)09－0082－07

长期以来，农业科研办公数据如项目、文章、成果及专利等多源科研信息，都是按照个人申报、单位内管理、科研处备案的方式，形式上以纸件统计上报、电子文档(Word、Excel) 存档备案为主，查阅和统计时需要翻阅存档资料进行逐一搜寻和信息核实，工作流程和手续较为繁琐、缓慢，并且对于信息的共享效率和安全管理存在一定的制约. 21 世纪以来，许多农业科学院所相继将信息化手段引入办公系统当中，经历了电话通知、纸件报送到使用电子邮件、QQ、Excel 等工具的过渡，工作效率显著提高[1]. 但是，随着科研数据量的逐年增加以及数据安全共享需求的提出，上述办公手段已经造成技术瓶颈，不能适应管理需求，导致了科研数据信息的统计难度逐年增大、准确性降低等问题. 随着大数据、云计算、人工智能技术的日趋成熟，我国农业发展借助信息化的翅膀产生着量的变化与质的飞跃[2-3]. 在农业信息化高速发展的过程中，农业信息资源数量激涨，跨单位、跨部门合作的需求快速增加，农业科研项目实施的敏捷度不断提升，在此形势下如何进行科学高效的科研管理和协作成为亟待解决的重要问题[4-5]，而信息共享和信息安全更成为规范科研管理、提高科技资源共享效率所关心和关注的重要问题.

1　农业科研信息管理存在的问题

1.1　数据使用问题

过去 10 余年间，我国科研机构陆续开展了信息化管理系统开发应用，但所建立的现有农业科研协同办公系统大多只是具有简单的存储和查询功能，已经不能满足现代农业科研快速发展以及精细化管理的需

① 收稿日期：2019－08－08
基金项目：2019 年度农业农村部农业信息软硬件产品质量检测重点实验室建设项目(PT2019－28).
作者简介：李　昀(1969－)，男，高级工程师，主要从事信息化管理应用.
通信作者：邓　颖，研究实习员.

求. 以农业科研项目信息化管理为例，从用户的角度出发，在农业科研项目申报及执行过程中，由业务部门建立及更新项目数字档案，由科研管理部门及科研院所领导进行垂直的信息化过程监管. 对于科研机构纵向管理体系来说，科研部门、科研管理部门和院所领导等不同层级用户可见的数据范围不同，可操作性亦不相同；而对于单位内横向机构，同层级不同业务部门的用户，他们可见和可操作的数据范围也不一样. 此外，从数据的角度来看，同样的农业科研项目，若其尚处于申报过程，则只产生申报过程的相关信息，保密级别较高，仅对项目申报部门内部的申报工作参与人员可视共享，若为多部门共同申报项目，还需要进行跨部门信息共享，项目申报信息则需提交至更高层级进行协调管理，直至项目获得审批之前该信息要保持对上级和相关下级的可见，并开放对该层级用户的可视、可操作性权限；若项目处于执行过程中，科研数据保密性相对降低，项目执行部门的项目参与科研人员均可进行操作，但科研数据对上层管理用户不可见；项目结束之后，科研成果及可共享的科研数据将对院所内部所有用户乃至浏览游客公开展示，而管理平台根据科研历史信息挖掘的农业科研管理决策数据仅对管理层级用户共享. 传统的企业管理软件显然无法满足这样的多角色多层次的科研办公流程，需要经过详细地设计和精确地管理来实现.

1.2　使用效率问题

目前大多数协同办公平台完全采用第三方权限管理工具和工作流控制工具[6]，但是农业科研单位不论是从服务地理区域划分(国家、省、市、区、县级)，还是从服务专业领域划分(种植业、畜牧业、林业、渔业)，表现为院所种类差异大，数量众多，各单位之间人员组成、业务职能、工作流程、办公模式等的统一度低. 而现有的第三方工具普遍存在收费高、工作模式固定、定制化程度低、维护和更新困难等局限性，且大多第三方工具都进行了封装，只能通过接口实现功能的调用，无法从外部进行改良和完善，不能满足不同单位和部门对用户权限、数据可视域调整、工作流程定制化设置、灵活性调整的需求，制约了科研人员对数据的管理和共享积极性，不利于科学研究的交流共享，同时影响平台的数据积累与分析决策.

信息化建设已经成为开展科学高效的农业科研工作的重要手段，在此过程中，需借助一个体现信息集成和信息共享的标准化信息管理系统平台，既能为领导及科研管理者在科研经费管理、智能分析及决策方面提供便捷高效的服务，又能为科研人员提供个人科研信息管理及项目全过程实施管理的服务. 同时，在对系统进行不断的升级更新中保持数据的连续性、完整性[7]. 本研究在完成了农业科研单位的人事管理、科研管理、财务管理、综合办公管理、决策信息等子系统与功能模块的研发基础上，开发的基于角色和数据可视域的农业科研协同办公平台[8-10]，特别是面对日益复杂的用户角色组成、多样化的数据类型及繁多的功能模块和数据共享规则，基本实现了农业科研单位的人事、财务、科研数据、办公流程的电子化管理，以及科研项目的智能决策分析. 并针对农业科研信息管理中复杂用户角色组成及不同数据共享规则等问题，研究并提出了基于用户角色划分及数据可视域双向控制的农业信息数据安全及权限控制方法，不但实现对用户权限和数据域的灵活设置，还通过用户-角色-权限三者之间的数据库策略[11]，实现了规则与封装程序的脱离，提高网络环境下数据共享的安全性和灵活性.

2　方法设计

2.1　技术框架

本平台基于 Spring MVC[12-14] + Hibernate[15-16] + MySQL 框架，嵌入 Shiro[17-19] 安全管理框架进行认证、授权、加密及会话管理. 本文改写 Shiro 原有权限控制方法，添加数据可视域逻辑，优化用户与信息的精准配对，实现了本平台对于定制化多样数据和复杂角色之间的灵活分配.

如图 1 所示，Shiro 对用户登录请求进行身份认证，在 Shiro session 中保存用户登录信息；用户进行页面访问时，Shiro 将判断用户角色是否包含于被访问页面所要求的角色群组，这样的简单匹配明显不能满足农业科研信息复杂多变和数据共享规则的要求. 因此，本研究开发了新的授权方法并替换了原有的授权方法.

新开发的平台架构图如图 2 所示. 当用户对平台发起访问请求时，Shiro 安全管理模块将拦截请求并判断是否通过，通过验证的请求被送至控制层(Controller)，而通过验证的用户在同样的页面能看到的数据

域却是不同的. 因此我们通过在控制层添加用户-功能模块权限判断方法、在数据访问对象层(DAO)中添加数据域筛选模块，再从 Shiro session 中提取用户信息，根据当前访问页面对数据可视域规则进行数据筛选，实现对用户和信息的精准匹配. 具体方法将在下文进行详细描述.

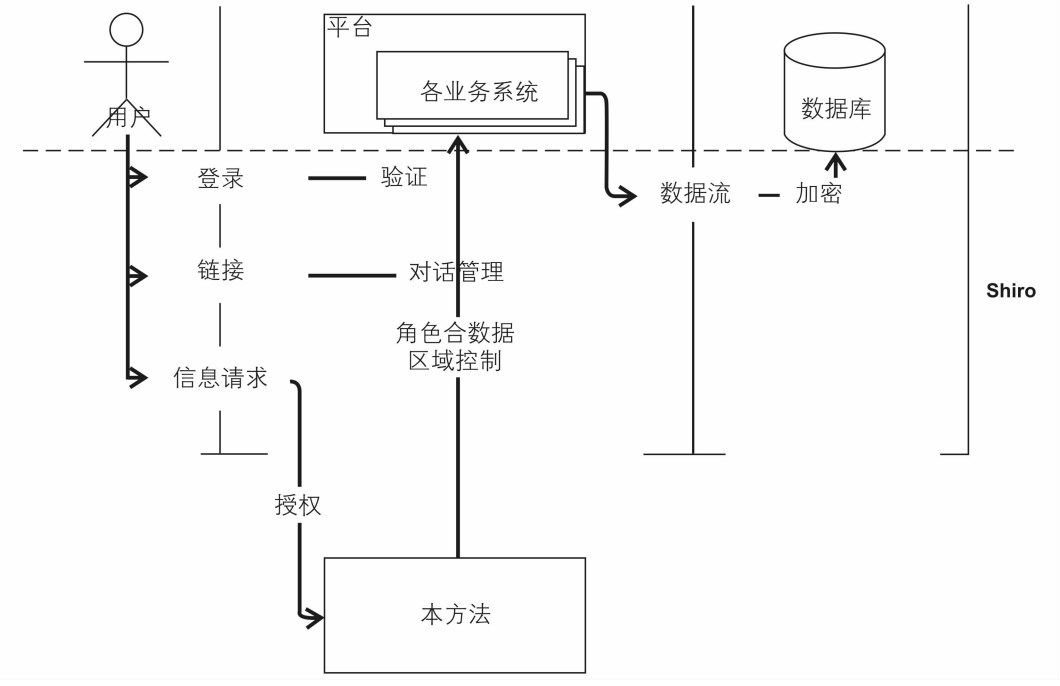

图1 平台安全模块工作模式

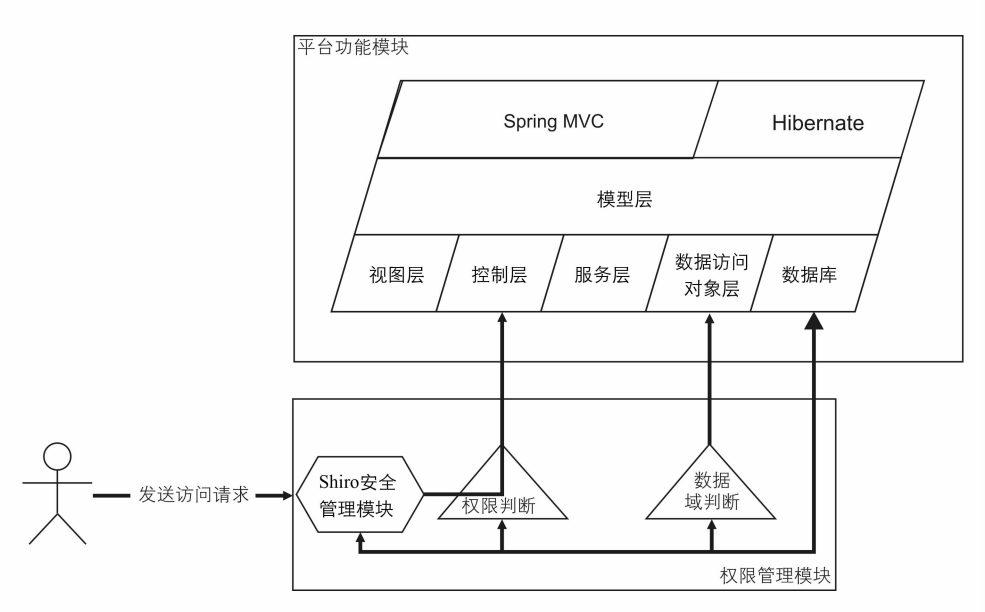

图2 平台安全技术框架

2.2 功能框架

本平台主要服务于农业科研单位的信息化办公与管理，着眼于农业科研单位的人事管理、综合办公管理、科研管理、财务管理等，通过本项目建设可最大限度实现资源的最优化利用，提高科研单位的研发水平、实验能力和科研管理效率. 面对管理业务内容多、科研项目多、研究方向广等问题，拟通过信息化手段直观、准确、实时地反映全院各所(中心)科研、人事、财务、推广、产业化的发展情况，实时了解和督促有关部门的工作进展，协调好物资供应、资金配套、技术攻关、信息服务等各个环节的控制管理，为领导层掌控整体运行情况和决策提供依据，从而促进院、所科研协同创新和科技研发能力的提升.

如图 3 所示，本平台内涉及的子系统、功能分支较多，加上各系统内角色亦多，用户在不同系统中所任角色、所有权限也有所差异，因此增加了信息共享管理的难度. 我们在平台设计时根据实际人员组成将平台用户分为系统管理员、院管理员、所管理员、部门管理员、职工等不同用户角色，并赋予各角色不同的权限和可视域范围；在信息处理和公文处置上，根据数据流程分为个人起草、部门处理、所管理部门处理、院管理处室处理等程序；根据数据当前所处流程对数据保密性的要求，将数据的编辑(添加、修改、删除)、查看、审核(同意、拒绝)等操作权限最低要求分为院管理、所管理、部门管理、个人、无要求等 5 个层级. 从平台角色权限划分和数据可视域制定双向出发，通过用户当前角色权限范围和所访问信息的最低权限要求综合判断，实现协同办公环境中的业务交叉而有序，数据共享而精准，信息公开而安全.

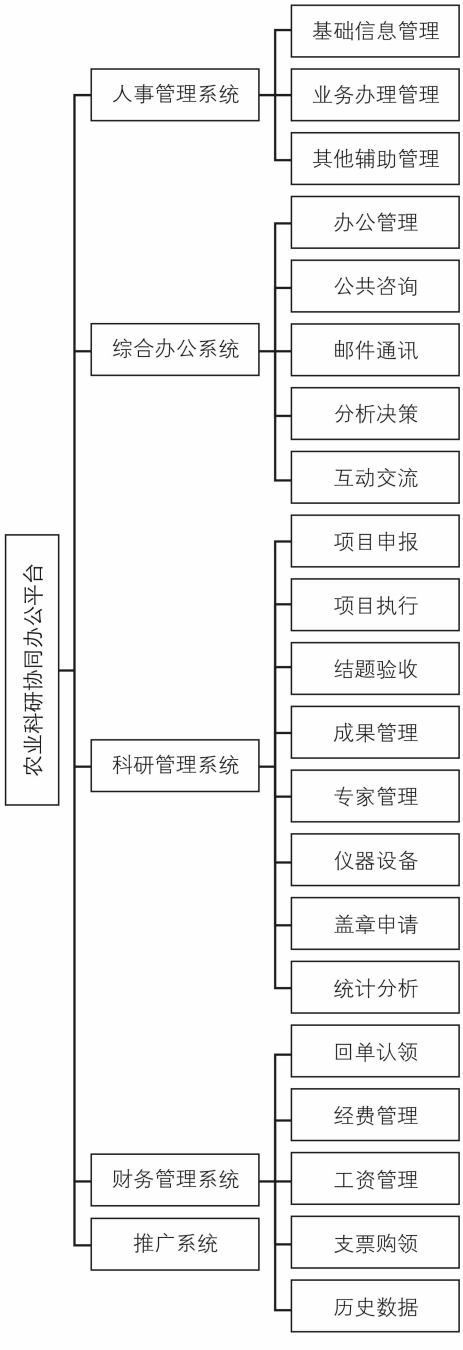

图 3　平台子系统及功能模块结构

2.3　方法实现

2.3.1　角色权限分配

农业科研管理体系的用户包括院处室、所/中心两级用户，本研究将用户角色划分为普通科研人员、部门主任、所科研管理人员、院科研处管理人员等，各角色操作权限设置设计如下：

(1) 普通科研人员具有项目申报、执行、验收各阶段数据管理和个人的科研成果数据管理以及向科研处申请盖章的功能.

(2) 部门主任(课题组长)，除了具有普通科研人员的功能外，还可以对本部门(课题组)的普通科研人员的数据进行查看和审核.

(3) 所级科研管理人员，除了具有普通科研人员的功能外，还可以对本所(中心)内所有科研人员的数据进行查看和审核，还具有创新平台、仪器设备、专家、废弃物等的管理功能，以及数据的查询统计，本所人员的系统管理设置等功能.

(4) 院科研处管理人员，可以对全院科研数据进行查看、审核与管理.

2.3.2　工作流程规则

平台以“个人成果，个人录入，部门审核，科管核查，科研处确认，责任明确，各有分工”为原则，设置所有农业科研数据的管理工作流程.

图 4、图 5 分别展示了所级和院级科研数据审核流程. 职工在申报项目与成果时，填写项目或成果基本信息，保存并提交后，等待部门主任进行审核；部门主任进入系统后可以查看本部门职工提交的基本信息，部门主任审核通过后进入科管审核阶段；科管审核通过，提交科研处审核确认或结束审核流程(部分数据科研处也可不审核，以所内审核结果为准).

2.3.3　设计详解

图 6 是本平台构建的权限控制模块工作原理图. 用户经过 Shiro 验证登录平台；选择访问系统后确定

用户所在该系统的角色与其对应各个功能模块的权限层级，权限层级为1～4；访问功能模块时，系统将获取该模块的最低要求层级，层级范围为1～4；遍历数据库表中的所有数据，并获取该模块数据所处工作流的位置以及实体类；通过实体类、操作类型以及所处工作流位置，在三者的关联表中确定每条数据当前的编辑、查看、审核操作数据域范围，亦为1～4；对比用户角色对应当前功能模块的安全层级和模块的最低要求层级，若角色权限层级≥模块最低要求层级，则用户具有对当前模块的访问权限，反之则将拦截用户对模块的访问请求，实现对功能安全性的保证；对比用户角色对应当前模块的权限层级和逐条数据编辑、查看、审核操作的安全层级，若角色－模块的权限层级包含于数据域范围内，则以最大数据域及用户角色所对应的“所、中心、部门、个人”进行数据域筛选匹配，若角色－模块的权限层级未包含于数据域内，则对该用户隐藏对应数据的编辑、查看、审核操作.

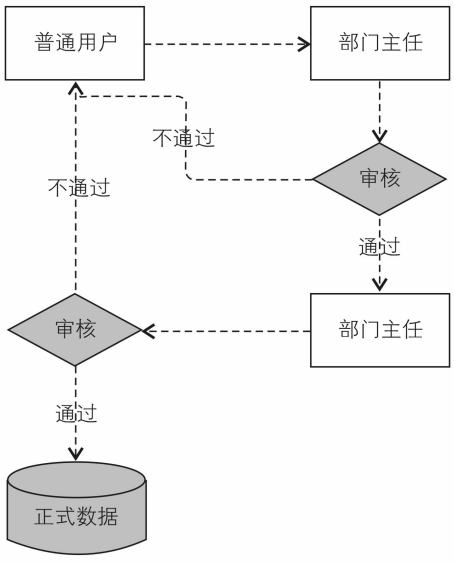

图4 无需科研处审核的平台工作流程

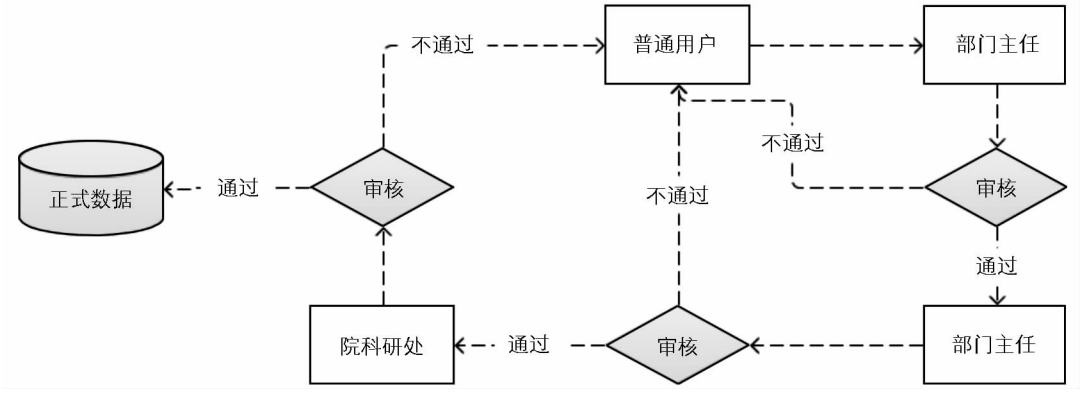

图5 需科研处审核的平台工作流程

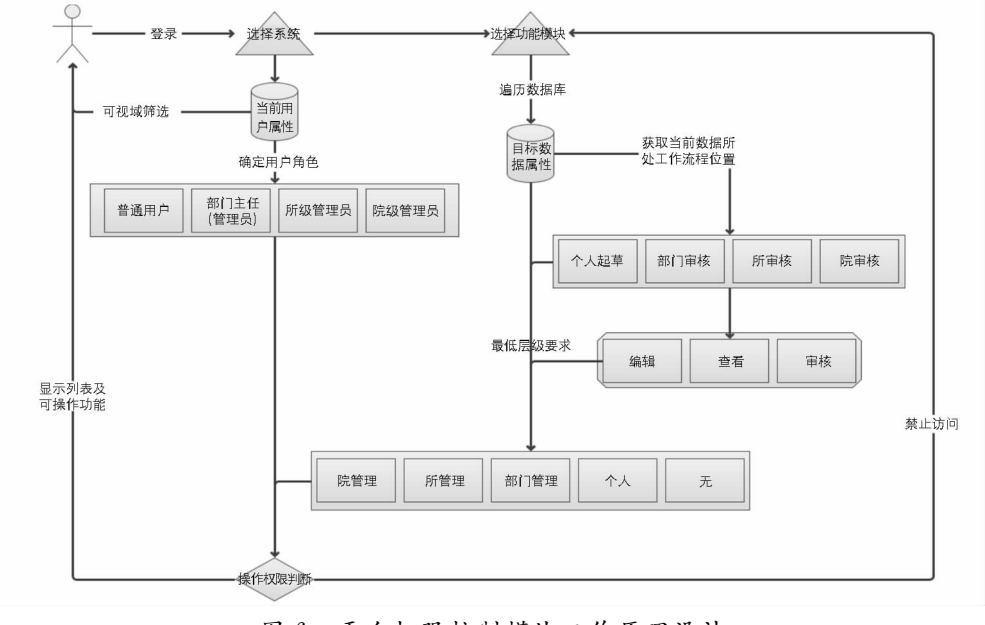

图6 平台权限控制模块工作原理设计

2.3.4 实例分析

以内部信息发布为例. 如表1所示，其编辑模块设置最低安全层级要求为2，院管理员对内部信息编辑

模块的权限层级为 4，所管理员对应的权限层级为 3，部门主任对应的权限层级为 2，普通用户对应的权限层级为 1；则部门主任以上的用户才可以编辑、发布内部通知信息，而普通用户不具有编辑和发布的权限，因而普通用户对应编辑信息模块的数据域不存在，固设置为“NONE”. 内部信息发布前，处于草稿编辑状态，设置此时的信息数据域为 1，当用户进行访问时，将对个人 id 进行匹配，即只有用户自身可以获取编辑权限；通知发布后的数据域范围设置为发布人权限层级的向下整数集合(部门主任发布的信息数据域为 2,1，所管理员发布的数据与为 3,2,1，院管理员发布信息的数据域为 4,3,2,1). 设置内部信息查看模块最低层级为 1，由于部门、所、院管理员发布的数据域都包含 1，则他们发布的信息都能被所有用户访问，并且在访问时，判断当前信息的数据域，如所管理员发布的信息数据域最大值为 3，则判断当前用户的所 id 和发布信息的管理员的所 id 是否一致，若一致则显示该信息，若不一致则隐藏；如此就实现了用户只能访问自身所在部门、所、院的信息，而不能越线查看其他部门、所、院通知内容的分类管理.

表 1　内部信息发布权限及数据域赋值设置

用户层级	编辑信息			查看信息		
	权限层级	数据域	最低要求	权限层级	数据域	最低要求
普通用户	1	NONE	2	1	1	1
部门主任	2	1		2	2,1	
所管理员	3	1		3	3,2,1	
院管理员	4	1		4	4,3,2,1	

注：“NONE”表示普通用户对应编辑信息模块的数据域不存在.

再以科研用章申请管理为例分析工作流程的权限管理方法. 表 2 所示，用章申请的编辑模块最低安全层级要求为 1，院管理员对用章申请的编辑、审核模块的权限层级为 4，所管理员对应的权限层级为 3，部门主任对应的权限层级为 2，普通用户对应的权限层级为 1，因为所有用户对应该模块的权限层级都大于等于 1，即大于等于模块的最低安全层级要求，所以所有用户都可以新建、修改、删除、提交用章申请. 申请提交之后，进入审核流程，审核过程中申请内容不再允许被修改，即编辑权限层级不存在，因此审核阶段的编辑权限层级为“NONE”，禁止对该用章申请进行编辑、修改；申请提交之后或每审核通过一次，审核操作数据域设置为前一步操作者权限等级加 1，即院管理员提交或审核通过的用章申请的审核操作数据域为 5，则完成申请流程；所管理员提交的或申请通过的用章申请的审核操作数据域为 4，发送至院管理员处审核；部门主任提交的或审核通过的用章申请审核操作数据域为 3，发送至所管理员处审核；普通用户提交的用章申请的审核操作数据域为 2，发送至部门主任处审核；审核流程中任何一步出现审核不通过，则该用章申请的数据域重新设置为申请提交者的对应编辑权限层级.

表 2　科研用章申请审批流程权限及数据域赋值设置

用户层级	用章申请编辑阶段				下一步审核阶段			
	编辑模块权限层级	审核模块权限层级	数据域	最低要求	编辑模块权限层级	审核模块权限层级	数据域	最低要求
普通用户	1	5	1	2	NONE	NONE	2	2
部门主任	2	5	1		NONE	2	3	
所管理员	3	5	1		NONE	3	4	
院管理员	4	5	1		NONE	4	5	

注：“NONE”表示编辑权限层级不存在.

4　结　　论

本系统构建了基于多源、复杂和多层级用户的高效管理流程和信息安全主动管理系统. 经过对该平台信息发布-查看、申请提交-审核等两种形态数据生命周期变化过程分析可见，该平台建立的基于角色-功能模块的权限层级及数据可视域范围的双指标双向控制权限管理与数据分配方法，可以灵活运用于各种应用场景下的不同功能模块，高效解决了农业科研协同办公平台中用户分级复杂、平台业务功能众多、工作流当中数据域变化不规则等难题，实现了用户角色权限与功能模块之间依赖关系的准确划分判断，以及数据可视域范围内的精确分发，使农业科研协同办公平台具有更高的功能集成性和更精准的信息安全操作性，既具备高效协同办公能力，又可以良好应对敏捷农业科研工作开展对信息共享和高效管理的需求.

参考文献:

[1] 张海峰,张 宇,唐立新,等. 黑龙江省农业科学院科研管理系统建设与应用[J],农业展望,2019(3):55-59.
[2] 王亚东,黄梯云,赵春江. 中国农业信息化建设研究[J]. 情报学报,2002,21(2):214-218.
[3] 于转利. 当代中国农业现代化发展现状及存在的问题[J]. 经济研究导刊,2010(30):28-29.
[4] 秦长江. E-Science(科研信息化)对现代科学的影响[J]. 科技进步与对策,2008,25(8):143-145.
[5] 纪素兰,张木莲,马晓杰. 农业科研单位办公自动化系统高效运行的障碍分析和对策建议——以江苏省农业科学院为例[J]. 江苏农业科学,2017,45(12):304-306.
[6] 金建宏,周 捷,许建平. 科研单位协同办公系统的设计及应用[J]. 电子技术与软件工程,2018(21):43-44.
[7] 李 飞. 农业科研院所科研管理信息化现状及措施[J]. 通讯世界,2017(5):268-269.
[8] 邓 林. 智能协同办公平台的构建方案实施[J]. 炼油与化工,2019,30(1):61-63.
[9] 程 旷,张尧弼. 协同办公平台项目实施的解决方案[J]. 计算机工程,2005,31(13):223-225.
[10] 罗杏金. 基于B/S的企业大协同办公平台设计及开发[D]. 上海:华东师范大学,2010.
[11] 何邦财. 计算机数据库安全策略研究[J]. 信息记录材料,2019,20(1):65-66.
[12] 潘益婷,潘修强,肖鹏飞. 基于NoSQL和MySQL的科研信息管理系统开发[J]. 中国教育信息化,2019(5):77-80.
[13] EPPIG J T, BLAKE J A, BULT C J, et al. The Mouse Genome Database (MGD): Comprehensive Resource for Genetics and Genomics of the Laboratory Mouse[J]. Nucleic Acids Research, 2012, 40(D1): D881-D886.
[14] 李 唯,徐玲利. 办公自动化系统的设计与实现[J]. 电脑编程技巧与维护,2019(1):18-20.
[15] YAN L. Construction and Testing of Modern Distance Learning Platform System Based on Struts and Hibernate Framework[C]// International Conference on Intelligent Transportation. IEEE Computer Society, 2018.
[16] KAI L, KAI Y, ZHU S. A Web Management Platform of Lnternet-Based Electrical Engineering Lab: Using SSH Framework [C]// 2012 7th International Conference on Computer Science & Education(ICCSE), Melbourne, Australia, July14-17, 2012.
[17] 刘全飞,周相兵. 基于Apache Shiro的站群角色管理[J]. 计算机系统应用,2015,24(6):177-182.
[18] YANG Y P, WU Z J. Application of Apache Shiro Security Framework in Technology Transfer Services System[J]. Computer and Modernization, 2014(3): 158-160.
[19] 徐孝成. 基于Shiro的Web应用安全框架的设计与实现[J]. 电脑知识与技术,2015,11(16):93-95.

On Design of Cooperative Office Platform for Agricultural Scientific Research Management Based on User Role and Data Visible Range Technique

LI Yun[1], WU Hua-rui[2,3,4], DENG Ying[2,3,4], LI Qing-xue[2,3,4], GU Jing-qiu[2,3,4]

1. *Beijing Academy of Agriculture and Forestry Sciences, Beijing 100097, China;*
2. *National Engineering Research Center for Information Technology in Agriculture, Beijing 100097, China;*
3. *Beijing Research Center for Information Technology in Agriculture, Beijing Academy of Agriculture and Forestry Sciences, Beijing 100097, China;*
4. *Agriculture Key Laboratory of Agricultural Information Software and Hardware Product Quality Testing, Ministry of Agriculture and Rural Affairs of the People's Republic of China, Beijing 100097, China*

Abstract: The agricultural scientific research unit has the characteristics of the complex information type and user composition, complicated business process, etc.. These bring the agricultural scientific research units with many problems and difficulties to the cooperative office, information utilization and security management. Taking the development and design of modern scientific research collaborative office platform of Beijing Academy of Agriculture and Forestry as an example, this study has been carried out. Through the research and construction the efficient data management process and active information security management system based on the data role and visual domain technology, as well as the multi-source data, complex and multi-level users conditions, we divide a platform users horizontally by department, vertically by management level, and define the visual field of the data resources. A user authority management and data security control system for user and data bidirectional control has been developed, and finally collaborative office platform for agricultural scientific research unit been constructed, which can not only realize efficient information loading and sharing, but also maintain information security.

Key words: information flow; data range; office automation; data dispatch

责任编辑 王新娟