科研机构信息系统人员账号及账号权限管理模式探究

魏旗鹏　李金定　徐崇智　宋含露　蔡　宁　李亚子

（中国医学科学院　北京 100730）

〔摘要〕　目的/意义 逐渐完善科研机构信息系统人员账号及账号权限管理模式，提升系统效率和安全性。方法/过程 基于中国医学科学院内部信息系统建设实践，聚焦科研场景下机构内部信息系统的用户账号及权限管理需求，探究适配管理模式。结果/结论 针对信息系统中人员多权限管理难点，提出解决方案并开展实践，为同类科研机构信息系统人员账号及账号权限管理提供参考。

〔关键词〕　科研机构；账号管理；用户权限管理；信息系统

〔中图分类号〕R－058　〔文献标识码〕A　〔DOI〕10.3969/j.issn.1673－6036.2025.11.015

Exploration on the Management Mode of Personnel Accounts and Account Privileges in the Information System of Scientific Research Institutions

WEI Qipeng, LI Jinding, XU Chongzhi, SONG Hanlu, CAI Ning, LI Yazi

Chinese Academy of Medical Sciences, Beijing 100730, China

〔Abstract〕　**Purpose/Significance** To gradually improve the management mode of personnel accounts and account privileges in the information system of scientific research institutions, and to enhance the efficiency and security of the system. **Method/Process** Based on the construction practice of the internal information system of the Chinese Academy of Medical Sciences (CAMS), focusing on the personnel accounts and account privileges management requirements of internal information system in scientific research institutions, the adaptation management mode is explored. **Result/Conclusion** Aiming at the difficulties in the multi－authority management of personnel in the information system, a solution is proposed and practiced, providing references for the management of personnel accounts and account privileges in the similar information systems of scientific research institutions.

〔Keywords〕　scientific research institution; account management; user privilege management; information system

1　引言

近年来，科研机构依靠信息化手段开展日常管理工作已经成为常态。随着科技进步以及科研机构对外合作步伐加快，科研机构人员流动频繁，部分人员承担多重身份。如何做好人员流动管理及身份管理已成为用户管理的重要课题。

传统信息系统中，为解决人员多重身份的问

〔修回日期〕　2024－11－08

〔作者简介〕　魏旗鹏，工程师，发表论文 10 余篇；通信作者：李亚子，研究员。

〔基金项目〕　中国医学科学院科技创新体系与核心基地建设数字化支撑工程项目（项目编号：2018－I2M－2－001）。

题，常为其建立多个账号。这不仅增加了管理部门的负担，也容易造成混淆。随着信息化建设的持续推进，科研机构的人员账号管理已成为一项重要的日常工作，不同人员账号权限的合理分配成为信息化管理的重点和难点。对此亟须探索和实践适用于复杂场景的用户账号管理模式，以提升人员账号管理的效率和安全性，为科研机构的信息化建设提供有力保障。

中国医学科学院北京协和医学院（以下简称院校）作为我国最高医学研究和教育机构，目前正处于各项业务的数字化转型关键时期。人员账号的信息化管理是其中的核心环节之一，影响着跨部门、跨所院的交叉协作管理及医学科研项目的高效推进。尤其近年来院校医学研究与临床应用深度融合、对外学术合作日益频繁，人员账号权限动态调整需求显著增加，因此针对院校实际场景探索科学的账号及权限管理模式，既是破解当前管理痛点的现实需要，也是保障院校数字化转型平稳推进的重要支撑。

2　人员账号管理现状分析

2.1　国内外研究现状

目前，国内外学者对用户账号管理的研究主要聚焦于管理模式、技术手段和安全防范等方面，特别是在保护患者隐私和医疗数据安全方面，而对用户账号权限复杂管理模式的研究相对较少。许多医学科研机构仍沿用传统的账号管理模式，缺乏对不同类型人员账号的精细化管理。

国内大型企业信息系统用户账号管理模式一般采用 3 层结构体系，包括表示层、功能层、数据层。其中，表示层又称人机页面，是用户与系统之间的交互接口；功能层的核心在于构建机构内部的数据逻辑；数据层则负责用户数据及系统数据的交互[1]。这种用户账号管理模式在面临多重身份情境时，主要通过控制可访问的菜单以及按钮来实现权限管理[2]。此方式要求及时维护用户信息，并确保数据库能安全、及时地与表示层对接，对数据管理工作人员的专业素养要求较高。

国内医学院校信息系统管理面临人员不足且专业性不强的问题，难以胜任数据层的增删改查工作。对此常见的优化举措是建立一套账号目录树，在数据层创建阶段就明确用户账号管理的所有需求信息，并与目标数据进行关联，将账号数据的管理简化为目录树的更新[3]。然而，该方法更适用于账号信息需求变化较小、人员身份相对单一且较稳定的机构。

2.2　院校人员账号管理需求与面临的挑战

院校自 1957 年起形成院校合一、所院两级法人管理模式。多年来，院校与下属各所院互为补充，充分发挥独立法人优势，展现出较强的特殊性[4]。这种管理模式下，同一人员在多个所院拥有多重身份的情况普遍存在，院校及所院人员抽调频繁，且各所院的人员账号管理制度及编码规则等不一致，给人员管理带来挑战。

2.2.1　多系统导致多账号　目前，院校可以生成人员账号的系统有 5 个，包括本科教务系统、研究生院管理系统、教职工人事系统、中国医学科学院信息管理系统 MacRP、院校用户管理系统。这些系统可以创建 5 类用户账号：本科生账号、研究生账号、教职工账号、外单位账号、第三方账号。由于多系统之间未实现完全对接，且账号未及时更新，同一用户拥有多个账号的情况时有发生。

2.2.2　多岗位、多重身份导致的账号问题　部分人员在院校各部门及各所院同时担任多个职位，部分人员同时兼具学生和教师身份。系统中存在人员岗位调整、工作调动后账号身份未及时变更、未注销导致的新账号、新身份无法生效的问题。

2.2.3　人员流动复杂　近年来，院校人员管理复杂性提升。例如，院校内师生经常有所院内转系、流动的情况；部分教职工工作调动后，仍具备院校系统项目申报资格等。

2.2.4　特殊用户需求　在部分情况下，某些用户希望能够建立仅拥有账号部分功能的特殊账号。例如，部分退休专家、院校领导仍主持科研项目，要授权他人进行部分操作。在此情形下，使用主账号风险过大，而新建账号可能会导致数据信息不连续、事项中断。因此，须在主账号下创建拥有局部

权限及数据的特殊账号。

因此，传统的账号管理模式已经难以维持较好的系统整洁度、数据安全性及用户满意度，亟须建立符合院校实际情况的人员账号与用户权限管理模式。

3 人员账号及权限管理模式设计

3.1 设计原则

一是绝大多数用户只拥有一个账号，部分特殊用户通过增加账号的多重属性（如岗位、授权等），实现用户账号的复杂化管理[5]，从而确保在院校信息系统中，用户信息与账号之间保持一对一的对应关系。二是数据安全性原则。对于敏感或重要的用户账号数据，系统在传输、存储、显示过程中进行加密处理，以确保数据的安全性。三是适配性与规范性原则。与院校及各所院的人员信息管理规则保持一致，符合信息系统数据管理规范，遵循账号信息分级管理流程要求，以确保使用人员操作的便捷性。

3.2 设计方案

分析院校师生、外单位、第三方等用户流动关系，以 MacRP 系统为例，用户流动关系，见图 1。设计 4 种管理方案：人员流动管理、人员岗位管理、分层级管理和授权管理。

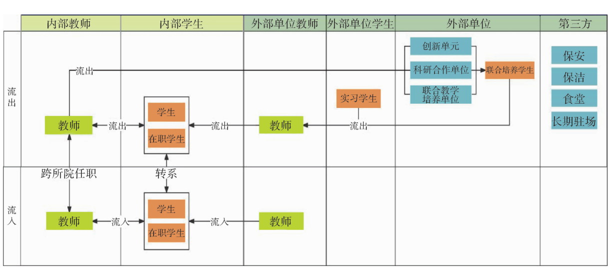

图 1 MacRP 系统用户流动关系

3.2.1 人员流动管理 建立人员流动管理流程，见图 2，以解决人员流动造成的同一人员在不同系统中重复创建多个账号的问题。针对院校能自主创建人员账号的系统或功能模块，建立信息传输通道。针对各子系统，区别于传统直接创建账号的操作模式，要求子系统提交账号创建请求时，先经院校用户管理系统查询，如果账号已存在，直接进行账号关联；如果账号不存在，则新建账号并推送至相应子系统进行管理。优化后的人员流动管理模式可实现一个用户只有一个账号（以 ID 为系统唯一标识）的目标。无论是留校任教（如学生转为教职工）还是学生学位变动等情况，都不再需要停用或重新创建账号。同时，考虑各所院个性化工号编码需求，系统支持修改工号。

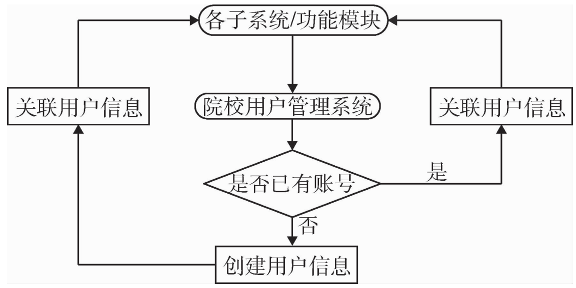

图 2 人员流动管理流程

3.2.2 人员岗位管理 所院两级法人管理模式下，存在人员在院校各部门及各所院同时承担不同工作职能的情况，传统管理模式要为同一人员每个工作岗位创建不同账号。优化后采用基于角色的访问控制（role – based access control，RBAC）模型。该模型包含用户、角色和权限 3 大实体，其基本思想是在用户和访问权限之间引入角色的概念，用户通过切换角色获得相应权限[6]。结合院校用户权限需求实际情况，引入岗位及机构两个概念进行用户账号权限管理[7]，构建用户 – 机构 – 岗位 – 权限 4 级管理制度。其中“机构 + 岗位”对应 RBAC 模型中的角色，可进一步细化和区分用户角色。不同机构不同岗位的账号权限与数据流相互独立，通过切换机构及岗位实现身份角色的切换。

3.2.3 分层级管理 （1）对多岗位人员进行副账号管理。主账号包含副账号的全部信息，副账号是主账号部分数据与权限信息的集合。为保证账号信息的数据安全，当有副账号创建需求时，向用户管理员提出申请。由用户管理员在主账号下创建副账号，并进行数据及权限信息的授权配置，以确保副账号与主账号之间数据联通。副账号操作时产生的数据流将自动同步至主账号；主账号与副账号相

关的数据流也会同步更新至副账号，无关数据信息将被隔离。如此副账号与主账号在物理上相互独立，即账号、密码是独立的，但由于数据联通，在信息管理层面属于一个统一的账号集群。这有利于对该账号集群进行同一用户身份标记，并将其视为该用户的唯一账号信息。在有特定需求时可删除主账号保留副账号，反之亦然。这种设计保证了在不同场景下身份信息鉴别的唯一性，同时通过限制副账号的权限范围，降低了安全风险。（2）对多重身份人员进行关联账号管理。通过建立一套相互关联的账号实现更细粒度的权限控制和任务分配。例如，对于在职读研的职工，由于职工与研究生权限几乎没有交叉，可设置一套账号进一步区分用户角色。以身份证号作为关联依据，用户登录时系统会自动提示不同账号信息供选择，以进入不同的用户空间并被分配相应的功能权限。账号均须遵循密码复杂度和定期更换要求，以确保系统的安全性[8]。

3.2.4 授权管理　授权管理指用户授权其他人登录并使用其本人账号的部分权限。采用两级授权管理机制：一是用户本人在系统中输入被授权人的账号信息（即手机号）并确认授权范围（即被授权人可查看和使用的数据范围），随后系统生成临时账号口令发送至被授权人手机；二是被授权人使用授权账号以及该临时账号口令登录系统，查看并操作授权范围内的数据。授权系统本质是通过授权信息、授权范围、授权码（即临时账号口令）3 重验证机制，允许他人登录并使用用户账号处理特定功能或事务。鉴于授权功能的安全性和信息安全技术要求，目前该功能仅支持院校使用，并限定于特定的短期任务，如临时访问或测试等。

4 结语

院校 MacRP 系统自 2023 年 6 月正式启动二期建设，并基于人员账号管理模式对原有功能进行升级改造，旨在更好地服务于医学科研管理。目前系统已基本满足院校师生的使用需求。人员账号管理模式设计为系统的应用带来便利，促进了科研项目申报、日常校园访客管理等业务的开展。但该模式仍存在若干待优化之处。其一，系统框架虽已搭建完成，但各子系统在规则设定时认定的账号唯一标识存在差异，要全面实现院校 MacRP 系统的功能，须先对历史数据进行处理，这是一个长期且持续的工作过程。其二，各二级所院作为独立法人，在人员管理制度方面存在差异，须根据其需求进一步完善个性化设置。其三，尽管优化后的管理模式增设了授权登录功能，并通过 3 重验证降低了安全风险，但仍存在一定安全隐患。为持续提升系统安全防护能力并确保数据安全，后续将评估是否在授权登录模块实施数据的二次加密传输，是否对被授权人登录后的操作进行记录，以及是否对授权频次进行限制等。目前，信息系统用户权限管理模式已完成整体框架搭建，后续研究将针对上述不足进行改进，以期逐渐完善管理模式。

作者贡献：魏旗鹏负责研究设计、论文撰写；李金定负责研究设计、论文撰写与修订；徐崇智、宋含露、蔡宁负责参与系统构建与维护；李亚子负责研究设计、提供指导、论文修订。

利益声明：所有作者均声明不存在利益冲突。

参考文献

1 夏晔. 信息系统用户权限管理分析［J］. 计算机产品与流通，2020（7）：116.

2 古扎努尔·艾合买提. 管理信息系统中用户权限管理实现方法探析［J］. 信息系统工程，2019（6）：54.

3 安军. 高校信息系统用户及权限统一管理的规划研究［J］. 电脑知识与技术，2022，18（18）：12－14.

4 魏旗鹏，李亚子. 基于数据共享的高校全量人员管理体系研究与设计［J］. 软件，2023，44（8）：53－55.

5 邓哲. 多元管理模式下基建档案管理工作创新［J］. 黑龙江档案，2023（1）：71－73.

6 苏德，韦统边，吴江波，等. 基于 RBAC 的汽车企业通用权限管理系统设计［J］. 汽车电器，2023（7）：48－50，54.

7 朱仙林. 多元管理模式下的基建档案工作创新［J］. 城建档案，2021（11）：110－111.

8 黄文斌. 利用信息化手段强化加管系统特殊账号权限管理的实践［J］. 信息系统工程，2021（9）：115－117.