第9章　用户中心与统一权限管理

如果说技术架构是平台的骨架，那么用户中心就是平台的心脏，统一权限管理就是平台的免疫系统。心脏负责将血液——用户的身份信息、认证凭据、家庭关系——输送到每一个业务模块；免疫系统负责识别和拦截任何未经授权的访问，确保数据在正确的边界内流动。

在第三章“建设原则与阶段划分”中，我们将用户中心和统一权限管理列为第一阶段P0优先级的核心模块，是所有后续业务模块运行的前提。在第六章“数据库架构与安全体系”中，我们为这两个模块设计了独立的数据库Schema和安全策略。本章将在此基础上，深入阐述这两个模块的完整设计。

本章将覆盖用户中心的注册登录、实名认证、家庭账户三大核心功能，以及统一权限管理的RBAC权限模型、多层级数据权限、操作审计日志和行级数据隔离机制。同时，本章将从“全国一张网”的战略视角出发，在用户体系和权限体系中预留跨区域互认的标准化接口——让老百姓的“一个账号”能够走遍全国供销平台，让各级管理员的“一套权限”能够跨区域生效。

9.1 用户中心

9.1.1 用户注册与登录

用户中心的首要功能是管理用户的身份认证。平台支持多种注册和登录方式，以适应不同用户群体的使用习惯和技术条件。

手机号验证码登录是最基础的登录方式，面向所有用户群体。用户输入手机号后，系统发送六位数短信验证码，验证码有效期五分钟，每日发送次数有限制以防止恶意刷取。验证码校验通过后，系统查询该手机号是否已有注册用户——已有则直接登录并返回JWT令牌，未注册则自动创建新用户并完成登录。这种“即登即注”的模式大幅降低了农村用户的使用门槛，不需要记住密码，也不需要经历复杂的注册流程。

微信授权登录面向习惯使用微信的用户。用户在微信小程序中授权后，系统获取微信OpenID，查询是否有关联的本地用户——已关联则直接登录，未关联则引导用户绑定手机号。微信登录的优势在于用户不需要额外输入手机号和验证码，一键即可完成登录。

电脑端扫码登录面向桌面端用户。电脑端展示一个包含临时令牌的二维码，用户使用手机端扫描二维码并确认后，电脑端自动完成登录。这种设计解决了桌面端输入不便的问题，同时利用手机端的已登录状态作为安全验证。

JWT令牌管理是用户认证的技术核心。用户登录成功后，系统生成一个JWT令牌，令牌中包含用户ID、角色列表、所属区域代码等基本信息，使用HMAC-SHA256算法签名，有效期为两小时。令牌通过Redis缓存管理，支持主动失效。用户退出登录或修改密码时，对应的令牌立即从缓存中删除，确保令牌的安全性。

9.1.2 实名认证

对于需要使用助餐服务、健康管理、金融服务等涉及补贴发放和个人隐私功能的用户，平台要求完成实名认证。实名认证采用“OCR识别+活体检测+公安三要素验证”的三步流程。

第一步，OCR识别。用户上传身份证正面照片，系统通过OCR技术自动提取姓名、身份证号、出生日期等信息，填入用户档案。第二步，活体检测。用户按照提示完成眨眼、张嘴等动作，系统通过人脸识别技术验证用户为真人而非照片。第三步，公安三要素验证。系统将姓名、身份证号、人脸照片提交至公安部门的实名认证接口，验证三要素的一致性。

认证通过后，用户的实名认证状态标记为“已认证”，人脸特征向量保存在用户档案中——这个特征向量后续将用于助餐核销时的刷脸验证、年审认证时的身份确认等场景。对于无法完成线上认证的老年人，可以在村级服务站由健康管家协助完成线下核验。

9.1.3 家庭账户

家庭账户是平台为农村家庭设计的特色功能，也是“亲情树”社交功能的数据基础。一个家庭可以有一个主账户和多个家庭成员。主账户通常是家庭中较为年轻的成员（如在外的子女），可以绑定年迈的父母、配偶和子女。

家庭账户的核心价值在于：子女可以远程查看父母的健康数据（血压、血糖、体检报告）、代父母下单（购买生活用品、预约上门服务）、接收父母的异常预警（SOS报警、未到店预警、检测指标异常）。这种设计解决了农村留守老人使用智能设备困难的问题——老人只需要到服务站刷脸即可享受服务，子女在远程通过手机完成管理和监护。

家庭账户的关系类型包括：本人、配偶、父亲、母亲、儿子、女儿、其他。每个家庭成员通过唯一的用户ID进行关联。同一用户只能归属于一个家庭，避免关系冲突。家庭账户的绑定需要双方的确认——子女发起绑定请求，父母在服务站刷脸或通过短信验证码确认。

从“全国一张网”的视角来看，家庭账户的设计预留了跨区域家庭关联的能力。当老人的子女在外地工作、使用其他区域的供销平台时，通过统一的家庭账户关联接口，仍然可以远程关注老人的健康和服务数据。这种跨区域的家庭纽带，正是平台从“离不了”到“喜欢”的情感连接核心——让距离不再成为亲情的阻隔。

9.2 统一权限管理

9.2.1 RBAC权限模型

统一权限管理采用基于角色的访问控制模型（RBAC）。这一模型的核心思想是：不直接将权限授予用户，而是将权限授予角色，再将角色分配给用户。当平台拥有数十种用户类型、数百个功能模块、数千个操作按钮时，RBAC模型能够大幅简化权限管理的复杂度。

权限资源按照“模块→菜单→按钮”三级结构组织。每个业务模块（如助餐服务、健康管理、城乡通）是一个一级权限节点；模块下的每个功能页面（如套餐管理页面、核销记录页面）是一个二级权限节点；页面上的每个操作按钮（如新增按钮、编辑按钮、删除按钮）是一个三级权限节点。管理员在配置角色权限时，可以精确到按钮级别进行授权。

权限资源树的设计遵循“最小权限原则”——每个角色只被授予完成其工作所需的最小权限。例如，配餐员角色只能查看自己的配送订单，不能查看其他配餐员的订单；健康管家角色可以进行健康检测数据采集，但不能修改检测结果。

权限的校验在前后端双重进行。前端根据用户权限控制菜单和按钮的显示与隐藏，但这只是提升用户体验的“浅层防护”。后端在每个接口请求时，由权限校验拦截器进行强制校验——即使前端绕过了权限控制直接调用接口，后端也会拦截未授权的请求。这种双重校验机制确保了权限控制的可靠性。

9.2.2 内置角色体系

平台预置了一套完整的内置角色体系，覆盖从系统管理员到普通居民的各个层级。内置角色不可删除，其核心权限不可修改，确保平台的基本权限结构稳定可靠。

角色	权限范围	数据可见性
系统管理员	全部功能、权限分配、系统配置	全平台数据
运营管理员	运营管理功能（不含权限分配）	全平台数据
国家级监管员	国家级数据驾驶舱	全国汇总数据，可下钻至省级
省级监管员	省级数据驾驶舱	本省及下辖区域
市级监管员	市级数据驾驶舱	本市及下辖区域
县级监管员	县级数据驾驶舱	本县及下辖区域
乡镇级监管员	乡镇级数据驾驶舱	本乡镇及下辖村
村级管理员	村级看板、两委公开栏管理	本村数据
健康管家	助餐核销、健康检测、样本采集	所属站点服务数据

配餐员	助餐配送接单	本人配送订单
上门护工	居家养老服务接单	本人服务订单
村委委员	两委公开栏编辑	本村公开内容
村支书/主任	两委公开栏审核发布	本村公开内容
居民	基础服务使用、乡音社交	本人及授权数据
家属	绑定老人数据查看、代下单	被绑定老人授权数据
农户	城乡通产品管理	本人产品及订单
部门宣传编辑	多知多福栏目内容编辑	本部门栏目内容

内置角色体系的设计充分考虑了平台的多层级管理需求。六级监管员角色对应了第七章中阐述的六级行政区域体系，每个级别的监管员只能看到自己管辖范围内的数据。健康管家、配餐员、护工等服务人员角色的数据权限被严格限定在“本人经手”的范围内，确保服务数据的安全可控。

9.2.3 多层级数据权限

数据权限管理是多层级架构最核心的安全保障。功能权限控制的是“能做什么”，数据权限控制的是“能看到什么”。一个县级监管员和另一个县级监管员在功能权限上完全相同——都可以查看县级数据驾驶舱，但数据权限将他们看到的数据限制在各自的辖区内。

数据权限范围有三种配置模式：第一种是“本层”——用户只能看到自己所属行政区域的数据，不能看到下级区域的数据。第二种是“本层及下级”——用户可以看到自己所属区域及其所有下级区域的数据，这是最常用的配置模式。第三种是“自定义”——用户可以查看指定的特定区域数据。

数据权限的注入通过MyBatis拦截器自动实现。拦截器在SQL执行前，从当前用户的上下文中获取其数据权限配置，动态生成区域过滤条件并追加到原始SQL中。整个注入过程对业务代码完全透明——业务开发人员不需要在每个查询方法中手动添加区域过滤逻辑。

从“全国一张网”的视角来看，这套数据权限体系为跨区域的数据共享提供了清晰的安全边界。当一个县级平台需要向市级平台上报数据时，上报的是经过脱敏处理的汇总数据，而不是原始的明细数据。当需要跨区域业务协同时，数据共享的范围由数据所有者通过权限配置进行精确控制。

9.2.4 操作审计日志

操作审计日志是平台安全体系的最后一道防线。所有涉及权限变更、数据修改、敏感操作的行为，都全量记录审计日志。日志内容包括：操作用户、操作时间、操作类型、操作对象、请求来源IP、操作结果。

审计日志存储在独立的数据库Schema中，与业务数据隔离。日志表按月分区，便于历史数据的归档和查询。平台设置了异常行为检测规则——高频权限变更、非工作时间大量操作、异地登录后立即进行敏感操作等行为，自动触发告警通知系统管理员。

审计日志不仅是安全事件追溯的工具，也是平台运营管理的重要数据来源。通过分析审计日志，可以了解各级管理员的活跃程度、各业务模块的使用频率、权限配置的合理性等，为权限体系的持续优化提供数据支撑。

9.3 用户体系与“全国一张网”

用户中心和统一权限管理不仅服务于单个平台的内部管理，更是实现“全国一张网”战略的基础。当一个老百姓在浚县的平台上注册了账号、完成了实名认证，这个身份凭证能否在滑县的平台上被识别？当一个县级监管员被借调到市级部门工作，他的权限能否临时扩展到全市范围？

平台通过以下设计为跨区域用户互认和权限协同预留了标准化接口：第一，统一用户标识体系。每个用户拥有全局唯一的用户标识，由区域代码和本地用户ID组合而成，确保在全国范围内的唯一性。第二，联邦认证机制。当用户跨区域访问其他平台时，通过JWT令牌中的区域代码和用户标识，目标平台可以向用户归属平台发起认证请求，确认用户身份和权限。第三，临时跨区域授权。支持为特定用户开通临时跨区域数据访问权限，设置有效期限，到期自动失效。第四，统一的实名认证标准。各地的实名认证采用相同的标准（OCR+活体检测+公安三要素），确保认证结果在全国范围内互认。

这种设计使得老百姓的“一个账号”能够走遍全国供销平台——在本地注册的用户，到外地同样能被识别；在本地完成实名认证的用户，到外地不需要重新认证。各级管理员的权限体系也支持跨区域的临时扩展和互认。这正是“全国一盘棋、服务无差别”的用户基础。

9.4 从“离不了”到“喜欢”：用户中心的情感价值

用户中心不仅是一个技术模块，更是平台与用户建立情感连接的起点。当老人第一次刷脸领到助餐时，系统准确地叫出了他的名字，显示了补贴金额——这不是冷冰冰的“账号001”，而是被尊重、被记住的“张大爷”。当子女在异地打开手机，看到父母今天的血压数据正常时，这不是冷冰冰的“数据同步”，而是跨越距离的牵挂和安心。当一家人通过家庭账

户绑定在一起，在亲情树上看到完整的家族关系时，这不是冷冰冰的“用户关联”，而是“我们是一家人”的归属感。

这些情感价值，正是平台从“离不了”走向“喜欢”的关键。老人离不开助餐，这是功能依赖；但老人每次刷脸时都被准确识别、被亲切问候，这才是情感认同。子女离不开健康数据，这是刚需；但子女看到的不只是数据，更是父母的平安，这才是喜欢。

用户中心的设计，始终在技术功能之外，保留着对人的关怀。每一个用户标识背后，是一个活生生的人、一个家庭、一份牵挂。技术只是手段，让人感受到被尊重、被记住、被关心——这才是用户中心的真正使命。

9.5 总结

用户中心是平台的心脏，统一权限管理是平台的免疫系统。用户中心通过手机号、微信、扫码等多种登录方式降低使用门槛，通过OCR+活体检测+公安三要素实现可靠的实名认证，通过家庭账户连接跨越距离的亲情。统一权限管理通过RBAC模型实现精细的功能权限控制，通过行级数据注入实现严格的数据权限隔离，通过审计日志实现全链路的操作追溯。

面向“全国一张网”，用户体系预留了统一标识、联邦认证、临时授权和实名互认等标准化接口，为跨区域的用户互通和权限协同奠定基础。更重要的是，用户中心的设计始终保留着对人的关怀——技术只是手段，让人感受到被尊重、被记住、被关心，才是真正的使命。

> 本章核心观点
>
> 用户中心是平台的心脏——通过多种登录方式降低门槛，通过三步认证确保身份可信，通过家庭账户连接亲情。统一权限管理是平台的免疫系统——RBAC模型控制功能权限，行级数据注入隔离数据权限，审计日志追溯操作轨迹。内置角色体系覆盖从系统管理员到普通居民的各个层级。面向“全国一张网”，用户体系预留了统一标识、联邦认证和实名互认接口。用户中心不仅是技术模块，更是建立情感连接的起点——让人感受到被尊重、被记住、被关心。