集团型信息系统统一权限管控与风险管理

杨晓亮

江苏中天科技股份有限公司，江苏 南通 226000

摘　　要： 本研究探讨了集团型信息系统中的统一权限管控与风险管理策略，重点分析了集团系统的复杂性及其在权限管理中面临的问题。文章通过设计统一权限管控框架，介绍了权限分配、技术架构选择以及权限生命周期管理的重要因素。同时，深入探讨了权限风险的来源、评估与监控机制，提出了预防策略。研究表明，通过合理的权限管理体系和有效的风险控制策略，集团型企业能够提升系统管理效率，降低安全隐患。

关 键 词： 集团型信息系统；统一权限；风险管理

Group-Type Information System Unified Authority Control and Risk Management

Yang Xiaoliang

Jiangsu Zhongtian Technology Co., Ltd. Nantong, Jiangsu 226000

Abstract: This study explores the unified permission control and risk management strategies in group information systems, with a focus on analyzing the complexity of group systems and the problems they face in permission management. The article introduces the important elements of permission allocation, technical architecture selection, and permission lifecycle management by designing a unified permission control framework. At the same time, the sources, evaluation, and monitoring mechanisms of permission risks were thoroughly explored, and prevention strategies were proposed. Research has shown that through a reasonable permission management system and effective risk control strategies, group enterprises can improve system management efficiency and reduce security risks.

Keywords: group type information system; unified permissions; risk management

引言

随着信息技术的不断发展，集团型企业信息系统在企业管理运营中发挥着十分重要的作用。然伴随着信息系统规模的扩大，权限管理和风险控制的难度也日益增加。权限管控涉及企业内部的访问控制与数据安全，直接影响到业务流程的效率。一个合理的权限管控体系能够减少因权限分配不当导致的安全隐患，有效提升信息系统的管理效率。因此，企业亟须建立统一的权限管控框架，以应对潜在的安全风险，确保系统的稳定运行。

一、集团型信息系统概述

1. 多层级架构与多系统集成的特点

集团型企业的信息系统具有显著的多层级架构和复杂的系统集成特点，通常覆盖多个业务单元、子公司、分支机构和外部合作伙伴多租户多层次的架构反映在信息系统的分布式特征上，使得不同的部门或子公司拥有独立的业务系统和数据库。系统涵盖从研、产、供、销、服等各个业务领域，而每个业务领域的业务系统在系统设计和用户使用上可能都有各自的权限管理需求。例如，财务部门可能需要严格的权限控制，以确保敏感的财务数据访问控制在有效的管控范围内；销售系统则更强调灵活性，以应对跨区域的销售队伍。[1] 同时，集团型企业往往会涉及不同的供应商，导致集团内的信息系统具有多样性和复杂性，不同平台间的权限管理机制存在较大的差异，异构环境增加了权限管理的难度，也给安全性带来了更大的问题。特别是当各个子公司需要与集团总部进行系统对接时，权限设计理念的不统一会产生数据孤岛效应，阻碍信息的有效共享，甚至增加业务决策中的信息滞后性，增加了 IT 系统集中运维的难度。

2. 权限管控难点分析

由于集团型企业的跨部门和跨地区运作，权限管理需要在不

作者简介：杨晓亮（1986.01- ）男，汉族，江苏南通，工程师，本科，研究方向：智能制造。

同的业务单元之间保持一致性，要能够适应各自的业务需求和本地法规。传统的权限分配方式通常依赖于静态规则，即事先为岗位分配固定的权限。但静态权限管理模式在面对复杂多变的业务环境时，显得难以灵活调整。比如，当员工在集团内不同部门间流动时，如何及时更新或收回其权限成为一大难题。如果权限无法及时调整，容易导致权限滥用或越权操作的风险，进而威胁信息系统的安全。特别是在大规模员工队伍中，手动管理权限效率低下，极易出现错漏。[2] 不同系统之间的权限也随业务场景的变化需要微调，传统的手动管理权限难以应对这种对立又统一的复杂场景，难以达到高效的管控，而自动化权限管理工具虽然能够减轻部分工作量，但其复杂的设置和规则管理又给 IT 部门带来了新的负担。

二、统一权限管控框架设计

1. 统一权限管控模型设计

常见的权限管理模型主要包括基于角色的访问控制（RBAC）和基于属性的访问控制（ABAC）。RBAC 是一种较为成熟的权限管理模型，通过为用户分配角色，每个角色对应一组权限，从而简化了权限的管理过程。在集团型企业中，RBAC 可以通过定义不同业务单元、部门和职位的角色，设置标准化的权限分配流程，确保权限管控的一致性。但是，RBAC 模型在应对动态的业务环境时，灵活相对不足。因此，基于属性的访问控制（ABAC）作为补充模型被广泛应用。ABAC 通过用户的属性、环境的属性以及资源的属性来决定是否授予访问权限。例如，系统可以基于用户的工作地点、时间或设备类型动态调整其访问权限，更适合复杂的集团架构，尤其是在需要跨部门、跨地区，甚至跨国的权限管控场景中，ABAC 的优势更加明显。[3] 通过 RBAC 和 ABAC 的结合，企业能够设计出既灵活又统一的权限管控体系，在不同业务场景下实现准确的权限分配。在此框架下，集团级的权限管理往往涉及大面积范围内的操作，因此需要在权限分配时兼顾全局性。权限分层管理可以分为全局权限和本地权限：全局权限由集团总部统一制定和管理，确保在整个集团范围内的权限控制标准化；而本地权限则由各子公司或业务单元根据具体需求进行灵活设置，既能保证权限的一致性，又能灵活应对不同区域业务的具体要求。[4]

2. 技术架构与工具选择

在现有技术中，统一身份认证管理（Identity Access Management，IAM）和单点登录（Single Sign-On，SSO）是实现集团级权限管理的重要工具。IAM 系统通过集中化管理用户的身份认证、权限分配和访问控制，确保用户在登录任何子系统时都能遵循统一的权限规则。IAM 能够帮助集团企业整合多个异构系统，简化用户身份管理，减少不同系统之间的权限冲突，从而提升信息安全性。SSO 则是集团型企业提高用户体验和权限管理效率的重要手段。通过 SSO，用户只需进行一次身份认证，即可访问集团内所有经过授权的系统，无需重复登录。结合 IAM 系统，SSO 能确保用户的权限在不同系统间保持同步，避免权限错配问题。同时，SSO 能增强审计，便于 IT 部门记录用户的访问行为。通过集成日志审计系统，企业可以实时监控用户的访问行为，利用大数据分析，识别异常行为或潜在的安全威胁。基于行为的分析（UBA）能够帮助识别异常的权限使用行为，及时发现和预防权限滥用。[5]

3. 权限生命周期管理

统一权限管控框架的设计要注重权限的授予，必须考虑权限的全生命周期管理，包括授权、变更、回收等环节。在集团型企业中，员工的岗位变化频繁，权限管理需要具备足够的灵活性和自动化特征，以应对员工职责变化所带来的权限调整需求。在传统的静态权限管理模式下，用户的权限通常在入职时确定，在其整个任期内保持不变。为了实现动态授权，企业可以基于实时的行为分析，自动调整用户的权限。[6] 例如，当某个员工在不同的项目或部门之间流动时，系统能够根据其实际工作需求，动态调整其访问权限，确保其只拥有当前岗位所需的最小权限。在实际操作中，企业往往会忽视员工离职或岗位变动后的权限回收工作，导致大量无效的权限继续存在于系统中，增加了安全隐患。企业可以采用自动化权限回收机制，确保在员工离职、岗位调动时，系统能够直接消费人事系统（HRM）产生的事件，经过预设置好的代码支持一般业务变更情景，自动注销用户账号或收回其不再需要的权限，重新为其赋予新的角色及权限。同时，企业可以设定权限的过期机制，即权限在一段时间内自动失效，防止长期存在的“僵尸权限”成为潜在的安全漏洞。

三、集团型信息系统权限风险管理

1. 权限风险的主要来源

在集团型信息系统中，权限风险主要来自多个方面，内部和外部威胁并存。内部的权限风险源于权限分配不当、权限过多或冗余，以及权限管理不透明等问题。集团型企业的多层次架构，使得员工在多个系统中拥有不同的权限。当权限分配不合理时，员工可能拥有超出其职责范围的访问权限，从而增加越权操作的可能性，导致敏感信息的泄露。外部风险则主要来源于黑客攻击。外部攻击往往通过网络钓鱼、密码破解等手段获取企业内部账户，尤其是高权限用户账户。一旦黑客获得了账户的控制权，可能会利用企业的弱权限管控漏洞，进行数据窃取或破坏。同时，集团型企业分散的架构增加了外部攻击的潜在入口，尤其是在子公司和外部合作伙伴使用不严格的权限管理时，就会成为黑客的突破口，威胁整个集团的信息安全。[7]

2. 权限风险评估与监控

为了有效管理集团型信息系统的权限风险，企业需要建立全面的风险评估和监控机制。第一，风险评估。通过对用户角色、权限分配、业务需求和访问行为进行定期评估，企业可以发现权限管理中的薄弱环节。具体来说，企业可以通过权限审计，分析员工的实际权限与其职责是否匹配，评估权限授予是否符合最小权限原则。如果发现有的用户拥有不必要的高权限，则应立即调整其权限设置。[8] 第二，权限监控。通过部署权限监控系统，企

业可以实时跟踪用户的访问行为，尤其是对高权限用户和敏感数据的访问进行重点监控。行为分析技术可以帮助企业识别异常的访问行为，如频繁的夜间登录、异常数据访问请求等。一旦监测到异常行为，系统能及时发出警报且采取反制措施，防止权限滥用。

3. 权限风险的预防与应对策略

企业应严格遵循最小权限原则，确保每个用户只拥有完成其工作所需的最小权限，减少权限滥用的风险，降低权限管理的复杂性。集团型企业可以通过引入自动化权限管理工具，实现动态权限分配，根据用户的工作内容、部门变动或项目需求实时调整权限，确保权限分配始终符合实际业务需求。同时，企业应加强对权限分配和变更的审批流程，确保权限的授予和调整都经过合理的审批。[9] 通过使用自动化的权限审批系统，企业可以加快审批流程，同时提高审批的透明度，避免权限授予过程中的人为疏漏。对于外部攻击的防范，则通过要求用户提供多重验证，如密码加上动态验证码、指纹等生物识别信息，提高高权限账户的安全性。需要注意的是，企业应定期进行网络安全培训，提升员工的安全意识，防止其成为外部攻击的突破口。在应对权限风险时，企业需要制定完善的应急响应计划。[10] 应急响应计划包括识别权限滥用或攻击的早期迹象、迅速隔离受影响的系统或账户、修复权限漏洞，以及进行事后审计步骤。

四、结语

在信息化发展的背景下，集团型企业的信息系统承载着复杂的业务需求，随着业务规模的扩大，如何在保障信息系统运行的同时，确保数据安全和权限管理的合规性，成为企业管理必须直面的课题。统一权限管控与风险管理作为集团型信息系统的重要组成部分，企业管理人员必须深入思考怎样实现更具弹性、智能化的权限管控体系，以应对日益复杂的内部与外部安全风险。

参考文献

[1] 李辉. 档案信息化管理存在的风险与安全管理策略研究［J］. 数字化用户，2022(16):40-42.

[2] 李海凤. 信息化环境下应收账款的风险控制［J］. 河北冶金，2022(12):87-90.

[3] 田敏慧，李俊霖. 集团财务管理中的内部控制体系建设研究［J］. 大众投资指南，2023(19):61-63.

[4] 甄彦芳. 集团型企业母子公司管控权限体系搭建概述［J］. 中国外资，2021(4):34-35.

[5] 丛飞荣. 国有集团公司财务管理与风险管控探讨［J］. 中国集体经济，2021，(31):154-155.

[6] 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):3.

[7] 梁冬冬，魏鹏. 证券公司权限与管控——全面风险管理第一道防线［C］// 创新与发展：中国证券业2017年论文集. 2018.

[8] 李桐. 基于风险原理和信息化的企业安全精细化管理研究［D］. 天津理工大学，2015.

[9] 佚名. 统一信息系统业务权限管理方案［C］// 创新与发展：中国证券业2012年论文集. 2012.

[10] 甄彦芳. 集团型企业母子公司管控权限体系搭建概述［J］. 中国外资，2021(4):34-35.