空管生产数据中心访问控制机制对数据安全的保障作用

符博时

民航重庆空管分局 重庆 401120

【摘　要】：在智慧民航建设加速推进的背景下，空管生产数据中心成为保障航班运行与空域管理的核心枢纽，集中承载多种关键数据，其数据特性决定了未授权访问或权限滥用将直接威胁飞行安全。访问控制机制作为数据安全防护体系核心支撑，通过四大核心功能构建全生命周期安全屏障。本文结合空管数据中心技术特点，梳理访问控制机制演进脉络与适配类型，从四大维度剖析保障机理，分析实践难点并提出优化路径，为智慧空管数据安全防护体系建设提供支撑与参考。

【关键词】：空管生产数据中心；访问控制机制；数据安全；保障作用

DOI:10.12417/2811-0722.26.03.093

1 空管生产数据中心访问控制核心机制与技术演进

1.1 传统访问控制模型的空管适配局限性

传统访问控制模型（访问控制列表、自主访问控制、强制访问控制）在小规模静态数据环境中曾发挥作用，但与空管生产数据中心业务特性存在明显适配缺口。空管数据中心连接多节点、数据链路跨区域，攻击面大幅扩大，传统模型缺陷被放大：访问控制列表在主体数量达百级后，权限维护成本指数级上升，无法适配跨区域协作；自主访问控制允许主体自主授权，违背空管数据“最小权限”原则；强制访问控制难以响应动态业务场景的权限临时调整需求，不适应空管柔性调度。

1.2 空管场景下访问控制技术的演进方向

为应对空管数据中心特性挑战，访问控制技术形成“角色化筑基、属性化适配、零信任强化”三维演进体系。基于角色的访问控制（RBAC）构建“用户－角色－权限”三元映射，契合空管组织架构，实现权限批量配置与集成管理，降低跨部门权限调整成本。基于属性的访问控制（ABAC）通过多维属性动态匹配实现决策，能精准适配空管动态场景。零信任架构以“默认不信任任何主体”为核心，构建“持续验证+动态授权”机制，适配外部协作与远程运维的安全管控需求。

1.3 空管适配的主流访问控制机制对比分析

结合空管数据中心安全需求与运行特性，主流访问控制机制适配性差异显著：

机制类型	核心原理	空管适配优势	空管场景局限	空管适配性等级
访问控制列表（ACL）	为每个资源关联允许访问的主体列表	实现简单，可快速部署于单节点设备	跨区域多节点场景维护成本高，无法适配多角色协作	低（仅适用于边缘节点）
基于角色的访问控制（RBAC）	通过用户－角色－权限三元组映射实现管控	契合空管岗位架构，支持权限批量管理，适配日常管制业务	紧急场景下权限调整滞后	中（核心日常管控手段）
基于属性的访问控制（ABAC）	通过多维属性动态匹配实现访问决策	支持场景化权限动态调整，适配应急、跨部门协作场景	多源数据属性融合难度大，策略设计复杂	高（动态场景核心机制）
零信任架构（ZTA）	默认不信任任何主体，持续验证访问合法性	支持跨区域、远程访问持续管控，构建纵深防御体系	与现有系统兼容性需改造，部署成本（全域安全防护核心）	

2 访问控制机制对空管生产数据安全的保障维度

2.1 身份认证筑牢空管数据访问第一道防线

身份认证作为前置关口，通过“静态认证+动态核验+场景管控”三重体系确保访问主体合法性。静态认证采用“密码+生物特征+岗位密钥”多因素认证模式；动态认证结合业务场景，实时分析访问主体行为基线与环境参数，异常时触发二次认证；外部主体采用“临时权限+全程监控”模式。技术上，采用 Kerberos 协议结合 SM 系列国密算法，实现双向认证，防范身份伪造与会话劫持攻击。

2.2 权限管控实现空管数据精细化治理

权限管控基于空管数据分类分级标准，通过“角色筑基+属性调优”实现精细化授权。角色权限分配层面，采用 RBAC 模型实现岗位与权限精准匹配，规避越权风险；动态权限调整层面，通过 ABAC 模型适配场景化需求，在应急场景下自动赋予临时权限并及时回收；针对多租户特性，结合数据脱敏与权限隔离，平衡安全与协同。

2.3 行为审计构建空管安全追溯体系

行为审计通过全链路日志记录与实时监控，构建“可追溯、可问责”体系，覆盖数据全生命周期。技术上采用“集中化审计平台+实时流处理”架构，整合多节点操作日志，实时分析操作行为，建立角色行为基线，异常时触发三级告警并阻断操作。对审计日志不可篡改存证，满足监管要求。

3 空管生产数据中心访问控制机制优化路径

3.1 构建分布式细粒度权限校验架构

针对空管数据“多节点协同、高实时性”的特性，构建“区域分布式+核心集中式”的权限校验架构，平衡细粒度管控与性能开销。在架构设计上，将雷达站、导航台等边缘节点的权限校验任务本地化部署，通过缓存常用权限策略（如日常管制权限）减少核心节点压力；核心数据中心采用集中式校验，对航班计划、跨区域管制数据等敏感资源实施严格校验。结合空管数据分类分级结果实施差异化策略：公开类数据（如机场航班动态）简化校验流程，采用缓存授权模式提升访问效率；敏感类数据（如雷达原始数据）采用“字段级+操作级”双重校验，确保权限精准管控。技术实现上，采用 Apache Ranger 结合空管业务定制开发，实现对 Hadoop、Spark 等组件的统一权限管控，支持目录级、文件级、字段级的精细化权限分配，同时通过分布式节点并行处理提升校验性能，适配 ADS-B 数据等高频实时数据的访问需求。

3.2 引入 AI 技术实现权限动态适配与风险预警

融合 AI 技术构建空管场景化访问控制模型，提升动态适配与风险防控能力。基于多智能体系统构建用户行为分析模型，通过学习管制员、运维人员等角色的历史访问行为（如访问时段、数据类型、操作频率），建立个性化行为基线，实现权限的智能推荐与动态调整——当管制员轮岗至新扇区时，系统自动推荐该扇区的标准权限集，经审批后快速配置。构建实时风险评估模型，结合空管运行场景（如航班高峰、恶劣天气、应急救援）动态调整风险权重，例如在雷雨天气航班备降高峰期，提高异常访问行为的检测灵敏度。针对异常行为检测，采用深度学习算法实时分析访问行为，当检测到管制员突然访问非责任扇区的敏感数据、运维人员在非维护时段操作核心设备等异常情况时，系统自动临时限制权限并推送告警信息至安全管理平台。通过 AI 技术的引入，实现“事前预警、事中控制、事后追溯”的全流程风险管控，提升访问控制的智能化水平。

3.3 搭建统一权限管理平台实现协同管控

遵循民航局“7+1”治理规范要求，搭建空管生产数据统一权限管理平台，整合管制、通导、气象、运维等各业务系统的权限管理模块，实现“一次认证、全网通行”的协同管控。平台采用“标准化接口+数据同步机制”，解决传统多系统权限孤岛问题——通过标准化权限接口实现与空管自动化系统、气象服务系统、设备监控系统的对接，确保权限信息在各系统间实时同步。平台具备全流程管控功能：身份管理模块实现用户全生命周期管理，支持岗位变动时的权限自动调整；权限分配模块融合 RBAC 与 ABAC 模型，支持日常场景与应急场景的权限快速配置；审计分析模块实现多系统日志的集中分析与可视化展示，满足监管审计要求。在实际应用中，该平台可实现跨部门权限的统一调配，例如在区域航班流量管控时，为气象、管制、机场等多部门人员配置临时协同权限，提升应急处置效率。

3.4 融合零信任架构强化纵深防御体系

结合空管安全需求，构建“以身份为中心、持续验证、微分段隔离”的零信任访问控制体系。在网络层面，采用微分段技术将空管生产网络划分为管制区、运维区、数据存储区等独立安全域，限制域间横向渗透，即使某一域被突破也可避免攻击扩散至核心管制数据。在身份验证层面，实施“全场景多因素认证”，针对本地访问采用“密码+生物特征”认证，针对远程访问（如异地运维）采用“VPN+动态令牌+岗位授权”三重认证。在授权机制层面，采用“实时信任评估+动态授权”模式，结合用户身份、设备状态、环境参数、业务场景等多维度信息实时计算信任值，当信任值低于阈值时自动降低权限级别。例如，当运维人员使用未备案终端接入时，仅开放设备状态查询权限，无法执行配置修改操作。通过零信任架构与传统访问控制机制的融合，构建覆盖“网络－数据－应用－终端”的纵深防御体系，提升空管生产数据中心的抗攻击能力。

4 案例分析：某空管生产数据中心访问控制体系实践

某空管分局为支撑智慧空管建设，搭建涵盖雷达导航、航班运行、气象服务的一体化生产数据中心，集中管理多个雷达站、导航台、管制中心的核心数据，面临跨区域数据传输安全、多角色权限协同、应急场景动态适配等核心挑战。该局采用“RBAC+ABAC+零信任”融合的访问控制体系，实现数据安全与运行效率的平衡，具体实践如下：

在身份认证环节，构建“三级认证体系”：管制员执行“指纹+岗位密钥+值班调度令”认证，确保上岗人员资质合法；运维人员采用“人脸+设备备案+临时授权码”认证，其中临时授权码由值班领导实时签发；外部协作单位（如机场、航空公司）通过“VPN 接入+动态令牌+数据脱敏”模式认证，仅能访问非敏感协同数据。针对远程运维场景，采用国密 SM4 算法加密传输，同时对操作过程全程录像审计，有效防范外部接入风险。

在权限管控环节，基于空管业务场景制定“角色－属性”双重权限策略。按 RBAC 模型划分 12 类标准角色，其中进近管制员仅能访问本进近区域的实时航班轨迹、气象实况数据，且仅具备读取权限；通导工程师按设备类型分配权限，仅能访问负责的雷达或导航设备运行数据。通过 ABAC 模型实现动态适配。

在行为审计环节，搭建集中化审计平台，整合多节点操作日志，采用 Flink 实时分析与区块链存证结合的方式。平台建立管制员、运维人员的行为基线，2024 年运行期间成功检测 3 起异常行为并阻断。

该访问控制体系部署后，实现连续 18 个月无数据安全事件，权限调整效率提升 70%，应急场景权限响应时间从原来的 10 分钟缩短至 30 秒内，同时满足《智慧民航数据治理规范》等 6 项行业标准要求，为区域航班安全运行提供了坚实保障。

5 结论

空管生产数据中心的访问控制机制是保障飞行安全的核心技术支撑，其适配性直接决定数据安全防护效能。本文研究表明：传统访问控制模型无法满足空管数据“多节点、动态化、高敏感”的特性需求，而“RBAC+ABAC+零信任”的融合体系能够实现身份精准核验、权限动态适配、行为全程追溯的全流程管控。通过身份认证筑牢源头防线、权限管控实现精细治理、行为审计构建追溯体系、合规适配满足监管要求四大维度的协同作用，可有效防范未授权访问、权限滥用等安全风险。

案例实践证明，科学的访问控制体系能够在保障数据安全的同时提升运行效率，为智慧空管建设提供核心支撑。未来研究可聚焦 AI 与空管业务场景的深度融合，构建更具适应性的动态访问控制模型，进一步提升空管数据安全防护的智能化水平。

参考文献：

[1] 计通智能. 如何确保智慧空管集中监控系统的数据安全？[EB/OL].

[2] Zhang S, Li M, Wang Q. Agent based adaptive risk aware access control for air traffic control system[J]. Journal of Intelligent & Robotic Systems, 2025, 105(3): 47.

[3]田溪.空中交通管理生产数据中心建设思路及设计[J].数字通信世界,2020,(05):112-113.

[4] 张彦伟.基于云计算的空管生产数据处理系统设计[J].长江信息通信,2024,37(10):153-155.