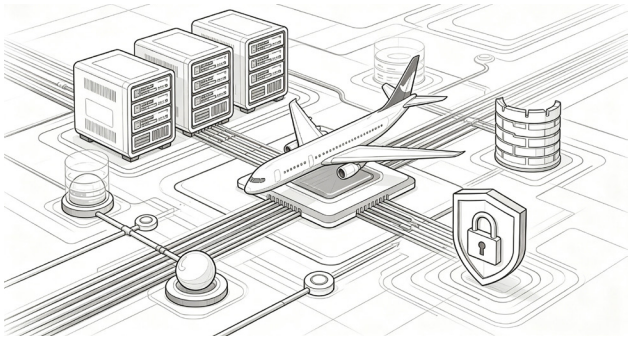
民航运行信息平台网络安全保障体系优化策略

文丨 费斐 刘海鹏

民航业数字化转型不断深入，运行信息平台数据与业务复杂性持续增长，网络安全风险进一步加剧。针对民航信息系统的网络攻击手段多样且隐蔽，对飞行安全构成严重威胁。现有保障体系在防护架构、技术配置和制度执行方面存在不足，难以应对复杂的安全形势，因此，优化民航运行信息平台的网络安全保障体系具有重要现实意义。



（配图由 AI 生成）

民航网络安全保障的理论基础

网络安全保护涉及技术、管理、法律等多个维度，明确其核心要素和理论体系是提升民航信息系统安全防护水平的关键前提，也为后续问题诊断和对策拟定提供了必不可少的保障。

网络安全保障体系的核心概念界定

网络安全防护体系是把技术方法、管理规则和法律法规结合起来，为信息系统提供全面保护的综合性框架。该体系基础是保障信息保密性、完整性和可用性，即防止数据被未授权访问、确保信息内容不被非法修改、维持系统服务稳定运行。它不是简单叠加各种产品或技术工具，而是包含风险评估、威胁遏制、实时监测、应急处置与系统恢复等环节的动态管理循环，该体系整体防护效能取决于各组成部分协调联动，任何一环薄弱都会削弱整体安全性。正确理解这一概念是分析民航信息系统薄弱环节、提出有效改进方案的理论基础。

民航运行信息平台的安全保障体系特征

民航运行信息平台整合了飞行计划管理、航班动态监控、气象数据传输和空管协同指挥等多项核心功能，其系统运行的持续稳定和数据传输的精确性对飞行安全有着决定性影响。和常规信息系统相比，该平台的安全保障体系呈现出明显区别，它的高可用性标准非常严格。平台得确保全天候无间断运行，任何服务的中断都可能引发严重的安全连锁反应，其数据敏感性比较强，涵盖航班动态、飞行员资料、空管指令等多类敏感信息，一旦发生信息泄露，将会造成难以估量的后果。系统具有开放性与封闭性特点，平台既要实现与气象、海关、公安等外部系统的数据互通，又要对核心控制模块实施严格的访问隔离与安全防护。上述这些特性决定了民航运行信息平台的安全保障体系不能直接采用通用安全框架，必须依据行业特性进行专门化设计并持续改进。

民航信息平台网络安全的现实问题

民航运行信息平台在网络安全方面承受的压力持续增大，潜在风险因素变得越来越复杂多样。当前安全防护机制不管是在技术水平还是管理模式上，都显现出一些亟待解决的实际缺陷，需要进行全面且细致的检视与深度分析。

民航网络安全威胁的主要类型特征

目前民航运行信息平台面临的网络威胁呈现明显多样化特征。从攻击方式方面分析，高级持续性威胁凭借长期潜伏和定向渗透特性，已成为针对民航信息系统最具破坏力的威胁类型之一。勒索软件、供应链攻击等新型攻击手段也逐渐向民航领域渗透，传统边界防护体系难以有效阻挡此类攻击。从攻击目标角度来看，飞行计划数据、空管通信链路、航班动态系统等关键业务节点成为重点攻击目标，若这些节点被破坏将直接威胁运行安全。同时内部人员违规操作和误操作引发的数据泄露问题也不能忽视，部分安全事件的根源并非外部入侵，而是内部管理机制失效。威胁来源复杂性和攻击路径隐蔽性相互叠加，使民航信息平台安全防护面临持续挑战。

技术防护体系建设的突出短板

虽然民航信息系统在安全保障技术领域已经进行一定程度的资源投入，但实际防护水平和业务场景的安全保障需求之间存在显著差距。在网络防护边界，现有防护策略较为局限，部分安全体系过度依赖常规防火墙及入侵监测装置，对加密传输流量深度解析与识别功能缺失，无法有效识别和阻断新型隐蔽式网络攻击手段。在数据安全保障层面，数据

分类与分级保护体系尚未完善，核心敏感信息在传输过程加密保护及存储环境物理隔离措施方面执行得不够规范严格。在安全监控能力方面，系统整体缺乏统一网络安全态势感知中心，各子系统产生的安全日志分散存储于不同位置，难以实现跨系统安全事件关联分析与异常行为即时告警。漏洞管控机制存在明显不足，系统补丁更新周期较长，部分陈旧设备长期在存在安全缺陷的状态下运行，已逐步演变为攻击者可利用的潜在风险点。

安全管理机制运行的主要缺失

管理层面存在的不足很值得高度关注，它削弱整体安全防护能力的效应显著。现有安全管理体系有割裂化的倾向，不同部门及系统间的安全责任边界比较模糊，责任落实缺乏刚性约束，导致制度执行常流于形式。人员安全素养培育机制存在一些漏洞，部分基层从业人员对网络安全守则的理解仅停留在浅层，面对诱骗攻击、社工欺诈等非技术类威胁时，鉴别应对能力不足。外部合作单位的安全管控属于薄弱环节，平台对接外部资源或引入第三方服务时，准入审核与动态监督机制不完善，由此产生的安全隐患难以得到有效遏制。综合来说，管理机制缺位让技术防护实际效能大幅衰减，亟需从体系层面进行系统性完善。

民航信息平台网络安全保障的优化策略

针对民航运行信息平台在技术防护和安全管理上存在的实际缺陷，要从技术革新、体系重塑、应急处置这三个维度同步推进工作，以此推动保障体系综合效能实现根本性的增强与优化。

技术防护能力提升的优化路径

强化技术防护的关键是要突破传统被动防护框架，转向主动监测和动态调整相结合模式。在网络防护边界方面应采纳零信任安全体系，用不间断身份认证替代既有边界信任模式，严格约束平台内部跨区域访问权限，以此限制攻击者在系统内的行动范围。针对数据保护要构建涵盖数据全生命周期的分类分级防护体系，尤其对飞行计划、空管指令等高度敏感信息采取端到端加密并实施存储隔离，确保数据在传递与存储环节不被非法获取或恶意篡改。在态势感知能力提升上要汇总各子系统安全记录，打造统一的安全运营平台，运用大数据分析方法实现跨系统异常行为联动检测与即时告警。漏洞管理制度也需同步完善，建立常态化扫描与快速修复的闭环流程，缩短高危漏洞暴露时长，从源头减少可被利用的攻击通道数量。

安全管理机制完善的策略选择

管理机制优化不能只对制度文本简单修改，关键是要确保安全责任真正落实到位。要从明确职责划分开始，清晰界定各部门网络防护工作的具体任务，设立可衡量的责任考核标准，把安全管理成效纳入部门综合评价体系，从根本上解决责任虚化的问题。人员管理要突破依赖集中培训的传统模式，构建常态化、实战化的安全意识培养模式，借助模拟钓鱼攻击、实战攻防演练等手段，增强基层人员安全防护实战技能。针对第三方供应商管理存在的短板，建立覆盖全流程的管控机制，包括准入审核等，对接入系统的外部实体实施严格安全基准检测，让供应链风险成为整体安全防护一部分。制度执行环节要设立独立内部审计职能，定期检查各项安全防护措施落实成效。

应急响应处置能力的强化措施

平台在抵御网络攻击后的恢复效率以及损失控制效果，完全由其应急响应能力的强弱来决定。目前，应急响应体系的改进方向应当聚焦于压缩从威胁识别直到处置完成的整个流程。在预案构建环节必须针对勒索软件入侵、机密外泄、系统崩溃等常见威胁类型，细化专项应对方案并明确各阶段响应步骤及决策权限，杜绝事件爆发时出现职责推诿与处置延误的情况。关于演练机制应该实施常态化跨部门协同应急演练，并且将演练成效作为预案优化的关键参考，促使应急处置能力在实战模拟过程中持续精进。灾备体系构建也需要给予高度重视，核心业务系统应部署跨地域容灾备份功能，保障主系统受创时关键业务能够实现无缝切换，最大限度降低服务中断对运营安全造成的冲击。同时，还需要构建与监管部门、行业组织的威胁情报互通渠道，通过整合外部资源来提升重大突发事件的联合处置效能。

结束语

民航运行信息平台的网络安全保障属于综合性工作，仅靠单一层面的优化难以彻底解决当前体系根本性缺陷。技术防护水平的增强、安全管理制度的健全以及应急处置能力的加强这三者互为依托、协同作用，共同构成保障体系完善的整体架构。网络安全环境的持续变化决定保障机制建设不能一成不变，必须实时监控风险动态、持续改进防护方案，并定期组织安全检查与系统测试，以此促进民航网络安全管理水平逐步提高，有效确保民航运行信息平台的可靠与稳定。

作者简介：费斐　刘海鹏　青岛民航凯亚系统集成有限公司

责任编辑：孙心仪　**投稿邮箱：**zhouhl@staff.ccidnet.com