信息系统管理对系统运行中的问题及对策分析

韦秋林
忻城县安东乡便民服务中心（退役军人服务站） 广西 来宾 546202

摘 要：在数字化浪潮下，信息系统成为各行业运转核心支撑，但实际运行中面临诸多问题。本文深入剖析信息系统运行的核心要素与管理逻辑，从硬件、软件、数据、环境、人员与管理层面分类典型问题，深度探究其技术、管理、人员层面成因，针对性提出优化对策，并构建全周期运行管理体系，以提升系统稳定性与可靠性，为业务持续发展提供坚实保障。

关键词：信息系统；运行问题；成因剖析；解决对策；全周期管理

引言：在数字化浪潮席卷的当下，信息系统已成为各行业运转的核心支撑，其稳定运行关乎业务连续性与竞争力。从硬件设施到软件系统，从数据资源到运行环境，每一环节都紧密相连，共同构建起信息系统的复杂生态。然而，在实际运行中，信息系统面临着诸多挑战，各类问题频发，给业务带来不同程度的影响。深入剖析这些问题成因，并探寻针对性解决对策，对提升信息系统运行质量具有重要意义。

1 信息系统运行的核心要素与管理逻辑

1.1 系统运行的核心构成要素

信息系统运行的核心构成要素为硬件设施、软件系统、数据资源、运行环境、人员与管理制度，六者相互依存、协同联动，共同支撑系统功能实现。硬件设施是物理基础，涵盖服务器、存储设备、网络设备等核心硬件，为系统运行提供算力与承载载体；软件系统是功能核心，包括操作系统、应用软件及数据库管理系统，是业务逻辑落地的关键载体[1]。数据资源是系统运行的核心对象，包含业务办理数据等各类结构化与非结构化数据，是决策与服务的重要依据。运行环境涉及网络传输、机房物理环境及安全防护环境，直接影响系统运行稳定性。人员包括运维技术人员与终端使用人员，前者负责系统维护与故障处置，后者通过规范操作发挥系统效能，且需承担日常运行检查、简单故障排查及上下协同沟通的桥梁作用，比如定期登录各系统检查运行状态与数据交换接口，对系统报错、网络连接失败等常见问题初步诊断，无法解决时准确描述并协同上级处理。管理制度是保障体系，涵盖巡检规范、操作流程、应急预案等，为各要素有序运转提供规则指引，确保系统整体运行高效可控。

1.2 信息系统运行管理的核心逻辑

运行管理始终以保障系统持续稳定为首要准则，通过构建预防性维护机制降低突发故障概率。管理流程遵循全周期闭环原则，从风险预判阶段的数据建模分析，到实时监测环节的智能告警系统，再到故障处置阶段的快速响应预案，最终通过性能调优实现系统能力迭代与提升。在这一闭环管理过程中，各要素间形成动态平衡关系，硬件扩容需同步调整软件参数，数据增长倒逼存储架构优化，人员技能提升推动管理流程革新，这种协同联动机制确保系统始终处于最佳运行状态。

2 信息系统运行中的典型问题分类

2.1 硬件设施层面问题

硬件设施是支撑系统运转的物理基础，长期运行后性能容易衰减，计算速度逐步降低、指令响应时间延长，进而影响业务处理效率。而且，硬件设备更新频率受经费预算、审批流程等因素制约，部分超期服役设备未能及时更换，硬件故障发生率大幅上升。服务器宕机会致使整个业务系统瘫痪，老旧服务器散热效率下降、元器件老化，在业务高峰期更易过载宕机；存储设备损坏会引发关键数据丢失，网络设备失效会造成通信中断，这些突发故障常造成严重业务损失。此外，硬件兼容性问题多出现在系统扩展阶段，新增设备与原有硬件在接口标准、驱动协议等方面存在差异，致使它们无法正常协同工作。

2.2 软件系统层面问题

应用程序故障直接影响用户体验，功能异常表现为特定模块无法调用，闪退现象多由内存泄漏或代码缺陷引发，死锁问题则导致系统资源被无效占用。软件兼容性冲突体现在跨平台运行时，不同开发框架编写的程序可能存在依赖库版本不一致，或与操作系统内核存在兼容性缺口。系统更新升级伴随技术风险，新版本可能因测试不充分导致核心功能缺失，或因参数配置变更引发性能波动。数据库问题集中表现为查询效率下降，事务

处理时出现数据一致性异常，连接池耗尽导致业务系统无法访问存储层。

2.3 数据资源层面问题

数据质量问题贯穿数据全生命周期，缺失值影响分析准确性，错误数据误导决策制定，冗余数据增加存储成本，不一致数据破坏业务逻辑连贯性。数据安全风险呈现多样化特征，泄露途径包括未授权访问与传输拦截，篡改行为多发生于数据落地环节，丢失风险则与存储介质故障密切相关。数据存储压力随业务增长日益凸显，存储容量不足迫使频繁扩容，归档策略混乱导致历史数据检索效率低下。

2.4 运行环境层面问题

网络环境问题直接影响系统互联能力，拥堵现象多发生于业务高峰期，断网事故可能由线路老化或施工破坏引发，带宽不足制约大数据传输，延迟与丢包降低实时交互质量[2]。物理环境异常中，机房温湿度失控加速硬件老化，电力中断导致服务中断，电磁干扰引发数据传输错误。外部环境威胁日益严峻，恶意网络攻击手段持续升级，病毒通过供应链渗透或社会工程学方式入侵系统。

2.5 人员与管理层面问题

运维能力短板体现在技术储备不足，对新型故障模式缺乏诊断经验，处置流程不规范直接导致故障修复时间延长。使用人员操作不规范现象普遍，误删除关键文件或配置错误参数常引发系统异常，数据录入错误更会直接影响业务准确性。管理机制缺失表现为责任划分模糊，跨部门协作流程存在空白，应急预案未定期演练进一步造成响应滞后。沟通协同障碍突出体现在运维、业务、管理部门间信息传递失真，直接导致问题定位与资源调配效率低下。

3 信息系统运行问题的成因深度剖析

3.1 技术层面成因

技术选型偏差是引发系统适配性问题的根源。硬件配置未充分考虑业务峰值需求，导致服务器在高峰时段负载过重，存储设备容量规划不足引发频繁扩容。软件选型忽视技术生态兼容性，部分业务系统与基础平台存在版本冲突，或开发框架与运维工具链不匹配，造成部署与维护困难。系统架构设计缺陷集中体现为扩展性不足，单体架构难以支撑业务快速增长，分布式架构未合理划分服务边界导致资源争抢，关键路径缺乏冗余设计形成单点故障风险。技术更新滞后现象普遍，旧系统因架构封闭难以集成新技术组件，开发语言版本过时导致安全漏洞修复困难，数据库引擎未升级引发性能瓶颈。安全防护体系薄弱表现为防护手段单一，仅依赖防火墙等边界防护设备，缺乏数据加密、行为审计、入侵检测等多层防护机制，难以应对日益复杂的网络攻击手段。

3.2 管理层面成因

管理制度缺失导致运维工作缺乏标准指引。常态化巡检机制未建立，设备健康状态监测依赖人工抽查，故障隐患难以及时发现。例如，某企业每月仅对关键设备进行1-2次巡检，导致一些潜在故障未能及时发现和处理。应急处置流程未文档化，突发故障时相关人员依赖经验判断，处置效率与质量参差不齐。数据管理规范不完善，数据分类分级标准模糊，备份策略未根据业务重要性差异化制定。资源投入失衡现象突出，业务部门扩张期优先保障功能开发预算，硬件升级、工具采购等运维相关投入受限，最终导致系统带病运行。风险防控意识薄弱，建设期过度关注功能实现，忽视架构可维护性设计；运行期缺乏定期压力测试与容灾演练，对潜在风险预判不足。绩效考核机制存在偏差，导致运维工作价值被低估，系统稳定运行等隐性成果未纳入考核体系，相关工作重心偏向短期可见的项目交付。

3.3 人员层面成因

培训体系断层造成技能传承困难。运维人员未接受架构设计、自动化运维等进阶培训，对新型故障模式缺乏诊断能力；使用人员未掌握标准化操作流程，误操作引发系统异常现象频发。职业素养缺失表现为责任意识淡薄，部分人员对巡检、日志分析等基础工作敷衍了事，故障处置时推诿现象时有发生。人才流失危机加剧技术断层风险，核心运维人员离职导致关键配置信息流失，新员工接手后需重新熟悉系统逻辑，故障处置周期显著延长。跨部门协作障碍进一步放大人员问题影响，运维人员与业务部门人员沟通存在信息壁垒，需求变更未充分评估对系统的影响，问题定位时责任划分不清导致处置效率低下。

4 解决信息系统运行问题的针对性对策

4.1 硬件设施优化对策

电脑硬件全生命周期管理需贯穿设备选型至退役全流程。通过部署智能监控工具，对办公电脑CPU利用率、内存占用率、硬盘读写速度及外接设备兼容性等关键指标实施实时采集，结合历史数据建立性能衰减模型，提前识别潜在故障风险。电脑硬件资源配置应遵循适度超前原则，根据业务增长预测预留20%-30%性能冗余，避免频繁更换硬件带来的业务中断。关键岗位办公电脑采用双硬盘备份架构，实施RAID6与多路径访问技术，确保单点故障不影响整体可用性，重要业务数据通过外接移动存储或云端备份实现容灾。

4.2 软件系统保障对策

软件管理流程需构建标准化管控体系[3]。建立软件准入白名单机制，所有上线软件必须通过兼容性测试与安全扫描，开发环境与生产环境实施严格隔离。测试环节增加混沌工程实践，模拟网络抖动、服务降级等异常场景，验证系统容错能力。故障响应机制建立三级处置流程，一级故障要求15分钟内定位问题根源，30分钟内提供临时解决方案，2小时内完成根本修复。数据库管理实施索引健康度检查，每周自动生成慢查询分析报告，对历史数据按访问频度实施冷热分离存储。

4.3 数据资源管理提升对策

数据质量管控构建五维管理体系。从完整性、准确性、一致性、及时性、唯一性五个维度制定校验规则，数据录入环节嵌入强制校验逻辑，流转过程实施全链路血缘追踪。安全防护采用分层防御策略，静态数据实施AES-256加密存储，传输过程启用SSL/TLS协议加密，访问控制基于RBAC模型实现最小权限原则。存储策略根据数据价值实施分级管理，热数据采用高性能SSD存储，温数据迁移至大容量HDD，冷数据归档至蓝光库或磁带库。

4.4 运行环境优化对策

网络环境优化实施SDN架构改造，通过软件定义网络实现流量智能调度，核心交换机部署负载均衡模块，边缘路由器启用QoS策略保障关键业务带宽。机房环境管理引入物联网传感器，对温湿度、粉尘浓度、电力质量等参数实施7×24小时监测，UPS系统配置双总线供电架构，防雷模块通过三级防护认证。安全防护构建纵深防御体系，边界部署下一代防火墙实施应用层过滤，内网部署IDS/IPS系统监测异常流量，终端安装EDR工具防范未知威胁。例如，某企业通过实施网络环境优化，将网络延迟从原来的50-100毫秒降低至10-30毫秒。

4.5 人员与管理机制完善对策

培训体系建立三维培养模型，基础层开展设备操作规范培训，进阶层实施故障模拟演练，专家层组织架构设计研讨。运维岗位实施岗位认证制度，核心岗位需持有ITIL、PMP等专业证书，建立AB角备份机制防止人员单点风险。管理制度编制运维操作手册、应急预案库、知识转移文档三套标准化文件，考核机制将MTTR（平均修复时间）、MTBF（平均无故障时间）等指标纳入KPI体系。跨部门协同建立联席会议制度，业务部门提交需求时需附带影响分析报告，运维人员处置故障时业务部门人员需配合进行业务验证。例如，某企业通过建立联席会议制度，将跨部门问题解决时间从原来的3-5天缩短至1-2天。

4.6 构建全周期运行管理体系

常态化监测机制搭建智能监测平台，通过数据对比分析自动识别系统运行的异常状态，取代传统依靠固定数值阈值触发告警的方式。风险预警体系设置四级预警机制，从设备性能偏离基线到业务服务不可用实施梯度化告警。应急处置流程编制标准化处置剧本，针对不同故障场景预设处置步骤与回退方案，每季度组织跨部门联合演练。持续优化机制建立PDCA循环，每月生成运行分析报告，识别高频故障根源，针对性实施架构优化或流程改进，形成闭环管理链条。

结束语

信息系统运行管理是一项长期且复杂的系统工程，涉及技术、管理、人员等多个层面。通过实施硬件设施优化、软件系统保障、数据资源管理提升、运行环境优化、人员与管理机制完善以及构建全周期运行管理体系等一系列对策，能够有效解决信息系统运行中的各类问题，提升系统稳定性与可靠性，为业务持续发展提供坚实保障，推动各行业在数字化道路上稳健前行。

参考文献

[1]魏翠萍.计算机应用中网络信息安全问题及解决对策[J].重庆电力高等专科学校学报,2024,29(4):22-26.

[2]林杰,姜天晗.企业管理信息系统的数据安全治理能力成熟度模型研究[J].上海管理科学,2025,47(2):32-42.

[3]邱勇灵,陆永,罗丹,等.公共安全视频图像信息系统运维管理体系研讨[J].中国安全防范技术与应用,2025(1):33-36.