 DOI: https://doi.org/10.12345/bdai.v7i2.37663

# Research on Intelligent Risk Management System for Computer System Operation and Maintenance Based on Security Barrier

**Yuanlin Zou**

Shanghai Dongxin Information Technology Co., Ltd., Shanghai, 200000, China

**Abstract**

With the expansion of computer system scale and the complexity of operation and maintenance scenarios, traditional risk management models are unable to meet dynamic security requirements due to issues such as lagging static assessments and inefficient passive responses. This article focuses on intelligent management and control of computer system operation and maintenance risks, proposing a comprehensive management and control system based on security barriers: by extracting hardware, software, network, and data layer risk factors, a dynamic evaluation index model is constructed; Research the application of intelligent technologies for security barriers such as access control, data encryption, fault isolation, and emergency response; Design the architecture of the risk management platform and validate the quantitative evaluation and strategy iteration path. Research provides theoretical support and practical solutions to enhance the proactive defense capability against operational risks.

**Keywords**

computer system operation and maintenance; Risk identification; Safety barrier

# 基于安全屏障的计算机系统运维风险智能管控体系研究

邹元林

上海冬新信息技术有限公司，中国·上海 200000

**摘　要**

随着计算机系统规模扩大与运维场景复杂化，传统风险管控模式因静态评估滞后、被动响应低效等问题，难以满足动态安全需求。本文聚焦计算机系统运维风险智能管控，提出基于安全屏障的全维度管控体系：通过提取硬件、软件、网络及数据层风险因子，构建动态评估指标模型；研究访问控制、数据加密、故障隔离及应急处置等安全屏障的智能技术应用；设计风险管控平台架构并验证量化评估与策略迭代路径。研究为提升运维风险主动防御能力提供理论支撑与实践方案。

**关键词**

计算机系统运维；风险识别；安全屏障

## 1 引言

在数字化转型加速推进的背景下，计算机系统作为关键信息基础设施的核心载体，其运维安全性直接关系到业务连续性与数据资产保护。随着系统架构复杂化、攻击手段多样化及运维场景动态化，传统风险管控模式因依赖人工经验、缺乏实时感知能力及跨系统协同机制，逐渐暴露出风险识别滞后、管控措施碎片化等弊端。构建融合全维度风险识别、智能安全屏障技术及动态优化能力的运维风险管控体系，成为提升系统韧性的迫切需求。本文基于此背景展开研究，旨在为计算机系统运维安全提供理论支撑与技术实践路径。

【作者简介】邹元林（1985–），男，中国上海人，本科，从事计算机系统运维研究。

## 2 构建运维风险的全维度识别与分类体系

### 2.1 风险因子提取方法

风险因子的有效提取是全维度识别的核心基础，需兼顾技术脆弱性与业务关联性。在硬件层，重点识别物理设备老化、供电稳定性不足及环境控制失效等风险，例如通过传感器实时采集设备温度、振动频率等参数，结合设备历史故障数据建立老化预测模型；软件层聚焦漏洞利用、版本兼容性冲突及配置错误，利用静态代码分析工具与动态模糊测试结合，挖掘潜在漏洞，同时通过配置审计工具检测非合规配置项；网络层风险涵盖 DDoS 攻击、数据泄露及协议漏洞，需结合流量分析技术与入侵检测系统，提取异常流量模式、非法端口访问等特征；数据层风险则围绕存储完整性、传输加密性及访问权限滥用展开，通过数据库审计日志与数据血缘分析技术，追踪数据流转路径中的敏感操作。四层风险因子提取需统一数据格式，并通过知识图谱技术构建跨层关联

关系，例如将软件漏洞与网络攻击路径、数据访问权限进行映射，形成立体化风险视图。

### 2.2 风险等级划分标准

风险等级划分需综合技术严重性与业务影响度，避免单一指标导致的评估偏差。本文采用基于 CVSS 评分与业务关键性加权的动态评估模型：技术严重性通过 CVSS 3.1 标准量化，涵盖攻击向量、攻击复杂度、权限需求等维度，例如远程代码执行漏洞因攻击向量为网络且无需用户交互，其基础评分可达 9.8；业务影响度则结合系统可用性、数据敏感性及合规要求，通过层次分析法确定权重，例如金融交易系统的业务连续性权重为 0.6，数据保密性权重为 0.3，合规性权重为 0.1。最终风险等级由技术评分与业务权重加权求和得出，并划分为“低危”“中危”“高危”“极高危”四级，例如某数据库配置错误导致敏感数据暴露，若其 CVSS 评分为 5.3 但涉及千万级用户信息，业务影响度加权后可能升级为高危。

### 2.3 动态风险评估指标体系设计

静态风险评估难以适应运维场景的动态变化，需构建实时感知与动态调整的评估指标体系。指标选取遵循“可量化、可追溯、实时性”原则，覆盖风险发生概率与影响程度双维度：发生概率指标包括漏洞修复时效、异常流量频率、权限变更次数；影响程度指标包括系统宕机时长、数据泄露规模、合规处罚金额等。评估模型采用机器学习与专家规则结合的方式：基于历史风险数据训练随机森林模型，预测未来 24 小时风险趋势；同时通过专家规则库对模型输出进行动态修正。例如某 Web 应用在高峰时段出现 SQL 注入攻击，流量分析模块检测到异常 SQL 语句频率激增，模型结合当前漏洞修复状态与业务负载，实时将风险等级从“中危”调整为“高危”，并触发隔离机制。动态指标体系通过 API 接口与运维平台对接，实现风险评估结果的实时可视化与自动化处置联动。

## 3 安全屏障在运维风险管控中的技术应用

### 3.1 基于零信任架构的访问控制技术

传统基于边界防护的访问控制模型在运维场景中存在显著局限性：内部网络与外部网络的物理边界逐渐模糊，且运维人员需跨系统、跨层级访问资源，导致权限滥用风险加剧。零信任架构通过“默认不信任、始终验证”原则，重构访问控制逻辑。其核心组件包括持续身份认证、动态权限管理及最小权限分配：持续身份认证采用多因素认证与行为分析技术，例如结合生物特征识别与设备指纹验证用户身份，同时通过机器学习模型分析用户操作习惯，识别异常行为；动态权限管理基于属性基访问控制模型，根据用户角色、资源敏感度及环境上下文实时调整权限，例如运维人员仅在办公网络内且设备已安装安全补丁时，方可访问生产环境服务器；最小权限分配通过自动化工具实现权限的按需分配与及时回收，例如临时授予开发人员调试权限后，系统在任务完成后自动撤销权限，避免权限残留。零信任架构的应用显著降低了内部人员误操作或恶意攻击导致的风险，某金融机构实践表明，部署零信任后，内部违规访问事件减少 72%，权限滥用导致的系统故障率下降 65%。

### 3.2 数据全生命周期加密与脱敏技术

数据作为运维风险的核心载体，其存储、传输及使用过程中的安全性直接影响业务连续性。数据全生命周期加密技术通过分层加密策略保障数据机密性：存储层采用透明数据加密技术，对数据库文件进行全盘加密，密钥由硬件安全模块管理，确保即使物理存储介质被盗，攻击者也无法解密数据；传输层基于 TLS 1.3 协议构建加密通道，结合国密算法实现数据传输的国产化安全防护，例如金融交易系统通过 TLS 1.3+SM4 加密，可抵御中间人攻击与数据截获；使用层采用动态脱敏技术，根据用户权限对敏感数据进行实时脱敏处理，例如审计员查询用户身份证号时，系统自动返回“*”号替代部分数字，而管理员则可查看完整信息。此外，同态加密技术的应用支持在加密数据上直接进行计算，无需解密，既保障了数据隐私，又满足了业务分析需求。某电商平台实践显示，部署全生命周期加密后，数据泄露事件减少 89%，且因加密对系统性能的影响控制在 5% 以内，实现了安全与效率的平衡。

### 3.3 基于微隔离的故障隔离与容错技术

运维场景中，单一组件故障可能通过服务调用链扩散至整个系统，导致级联故障。微隔离技术通过软件定义网络实现工作负载间的精细化流量控制，构建故障隔离的“逻辑边界”。其核心原理是将系统划分为多个微服务单元，每个单元通过安全策略定义允许的通信路径，例如 Kubernetes 集群中通过 NetworkPolicy 资源限制 Pod 间的网络通信，防止恶意软件横向传播；结合服务网格实现流量镜像与熔断机制，当某个微服务响应延迟超过阈值时，系统自动将流量切换至备用实例，避免故障扩散。容错技术则通过冗余设计与自动恢复机制提升系统韧性，例如分布式数据库采用多副本同步确保数据高可用，主节点故障时，系统在 10 秒内自动选举新主节点并恢复服务；容器化部署通过 Kubernetes 的滚动更新与自愈能力，实现故障实例的自动替换。微隔离与容错技术的结合使系统故障恢复时间缩短至分钟级，某云服务提供商实践表明，部署后系统可用性提升至 99.995%，年宕机时间减少至 26 分钟以内。

### 3.4 自动化应急处置与攻击溯源技术

运维风险处置的时效性直接影响损失程度，自动化应急处置技术通过预设规则与智能决策实现风险的快速响应。其核心组件包括安全编排自动化响应平台与威胁情报集成：SOAR 平台将安全事件与处置流程编码为可执行剧本，例如当 IDS 检测到 DDoS 攻击时，平台自动触发流量清洗脚本，同时通知运维人员；威胁情报集成则通过 API 对接外部情

报源，获取攻击者 TTPs 信息，优化处置策略，例如识别到攻击者使用“钓鱼邮件 +PowerShell 后门”的组合攻击时，系统自动加强邮件过滤规则并禁用 PowerShell 脚本执行。攻击溯源技术通过全流量采集与日志关联分析，还原攻击路径并定位根源，例如基于 NetFlow 的流量分析工具可追踪攻击者从初始渗透到横向移动的全过程，结合终端日志确定受感染主机；区块链技术则用于存储关键操作日志，确保溯源数据的不可篡改性。某能源企业实践显示，自动化应急处置使风险处置时间从小时级缩短至分钟级，攻击溯源准确率提升至 92%，为后续安全加固提供了精准依据。

## 4 管控体系的落地与优化

### 4.1 实施路径规划：分阶段推进与试点验证

管控体系的落地需遵循“先局部后全局、先核心后边缘”的分阶段实施原则，以降低转型风险并积累实践经验。第一阶段为试点验证阶段，选择业务关键性高、风险暴露面大的系统作为试点对象，基于全维度风险识别框架完成风险因子提取与等级划分，例如在金融交易系统中，重点识别交易链路中的软件漏洞、网络攻击及数据泄露风险；第二阶段为工具部署阶段，根据试点风险特征选择适配的安全屏障技术，并完成工具链的集成与测试，例如在试点系统中部署基于 ABAC 模型的动态权限管理系统，验证其与现有身份认证平台的兼容性；第三阶段为全面推广阶段，将试点经验复制至其他业务系统，并通过自动化脚本实现工具链的批量部署，例如通过 Ansible 自动化工具在 10 个业务系统中同步部署流量清洗设备，缩短部署周期 60%；第四阶段为体系固化阶段，将管控流程纳入组织标准操作程序，例如制定《运维风险处置手册》，明确风险上报、评估、处置及复盘的标准化流程。试点验证阶段需重点关注技术可行性与业务连续性，某银行实践表明，通过分阶段实施，管控体系上线后业务中断事件减少 85%，转型风险可控。

### 4.2 工具链整合：平台化集成与接口标准化

管控体系的有效性依赖于工具链的协同能力，需通过平台化集成实现风险识别、评估、处置及溯源的全流程自动化。工具链整合的核心包括统一数据接口、流程引擎与可视化看板：统一数据接口采用 RESTful API 或消息队列实现风险数据的实时采集与共享，例如将 IDS 告警、漏洞扫描结果、配置审计日志等结构化数据通过 Kafka 推送至风险评估平台，避免数据孤岛；流程引擎基于 BPMN 2.0 标准定义风险处置流程，例如当风险等级达到“高危”时，流程引擎自动触发隔离主机、通知运维人员及生成工单等并行任务，并通过状态机跟踪任务执行进度；可视化看板通过 ECharts 或 Grafana 等工具展示风险热力图、处置时效统计等关键指标，例如以颜色深浅区分不同系统的风险等级，红色代表极高危系统需立即处置。接口标准化是工具链整合的关键，需定义统一的数据格式与交互协议，例如某云服务商通过制定《运维安全工具接口规范》，实现 20 类工具的互操作，工具链集成效率提升 70%。平台化集成后，风险处置时效从平均 4 小时缩短至 20 分钟，且因人工操作导致的误处置率下降 90%。

### 4.3 人员能力建设：培训体系与考核机制

管控体系的落地需配套建设人员能力体系，通过分层培训与量化考核确保运维团队具备风险识别、工具使用及应急处置能力。培训体系采用“基础 + 进阶 + 实战”的三级模式：基础培训覆盖风险管控理论、工具操作及安全规范，面向全体运维人员；进阶培训聚焦高级技术与案例分析，面向安全专员与系统管理员；实战培训通过沙箱环境模拟攻击场景，提升团队应急响应能力，例如某企业通过每月一次的“红蓝对抗”演练，使团队平均攻击拦截时间从 30 分钟缩短至 5 分钟。考核机制结合理论考试与实操评估，例如理论考试占比 40%，考察对风险等级划分标准的掌握；实操评估占比 60%，考察工具配置、攻击溯源等操作熟练度，考核结果与绩效挂钩，激励团队主动提升能力。某金融机构实践显示，培训体系实施后，运维人员风险识别准确率提升 65%，工具使用合规率达到 98%。

## 5 结论

本文从安全屏障技术应用到管控体系落地优化，系统构建了运维风险管控的理论框架与实践路径。研究结果表明，基于零信任、数据加密及微隔离的安全屏障技术可显著降低风险发生概率，而分阶段实施、工具链整合与人员能力建设等策略则保障了管控体系的有效落地。未来研究可进一步探索 AI 驱动的动态风险评估模型，结合量子加密等前沿技术提升安全防御深度，同时完善跨组织协同管控机制，以应对云计算、物联网等新兴场景下的复合型运维风险挑战。

## 参考文献

[1] 杨文保,陈家静,王文平,等.网络安全与系统运维领域的新技术应用[J].数字技术与应用,2025,43(10):58-60.

[2] 赵慧一.智能运维在计算机系统故障预警与诊断中的应用[J].信息与电脑,2025,37(07):181-183.

[3] 张俊峰.计算机网络安全的软件编程与系统运维分析[J].软件,2022,43(07):180-182.