医院信息化建设中计算机网络安全的管理与维护探究

韩冰心
郑州大学第一附属医院　河南 郑州　450052

摘　要　分析医院信息化建设中网络安全现状、风险及针对性优化策略。现状显示：网络架构多采用三层拓扑结构，虚拟化集群RPO≤15 s，但东西向流量可视化不足；安全管理中，账号变更SLA达标率78.3%，外包账号双因子认证缺失率12%。风险上，内部管理漏洞致权限失控事件占37%，外部勒索软件利用系统补丁延迟（21 d）入侵，数据隐私泄露重识别概率22%。优化策略构建三级体系：内部管理推行RBAC+ABAC混合授权，权限细化到按钮级；技术防护部署NDR流量分析平台，误报率降至2%；隐私保护用AES-256-GCM全字段加密与k-匿名化（k≥5），结合五环应急响应机制，Ⅰ级事件8 h闭环。

关键词　医院信息化；网络安全管理；数据隐私保护；应急响应；安全防护体系

Research on the Management and Maintenance of Computer Network Security in Hospital Information System Construction

Han Bing-xin
The First Affiliated Hospital of Zhengzhou University, Zhengzhou 450052, Henan Province, China

Abstract　This study analyzes the current status, risks, and targeted optimization strategies for network security in hospital information system construction. The current status shows that network architecture predominantly adopts a three-tier topology structure, with virtualization clusters achieving RPO ≤ 15s, yet east-west traffic visibility remains insufficient. In terms of security management, the SLA compliance rate for account changes is 78.3%, while 12% of outsourced accounts lack two-factor authentication. Key risks identified include internal management vulnerabilities leading to permission control incidents (37%), external ransomware attacks exploiting system patch delays (21 days), and a 22% probability of data privacy leakage through re-identification. Optimization strategies are proposed as a three-tier system: internal management adopts hybrid RBAC+ABAC authorization, refining permissions to the button level; technical protection deploys NDR traffic analysis platforms, reducing false positives to 2%; privacy protection employs AES-256-GCM full-field encryption and k-anonymization (k≥5), combined with a five-level emergency response mechanism achieving an 8-hour closed-loop for Level I incidents.

Key words　Hospital Information System; Network Security Management; Data Privacy Protection; Emergency Response; Security Protection System

医疗行业数字化转型加速，电子病历、远程诊疗、物联网设备深度应用，让医院网络成为承载核心业务与敏感数据的关键基础设施。2023年全球医疗数据泄露平均成本为1 080万美元，较其他行业高60%，外部攻击导致的占比72%。我国三级医院信息化投入年均增长15.8%，网络安全投入占比不足3%，防护能力与攻击复杂度失衡。现有研究多聚焦技术防护单点优化，缺少管理体系、数据流动、应急协同的系统方案。本研究实证分析42家三甲医院安全现状，揭示架构脆弱性与管理断层关联，提出“技术—管理—响应”全链条防御框架，为等保2.0安全体系提供可落地的理论与实践支撑。

1　医院信息化建设中计算机网络安全的现状分析

1.1 医院信息化网络安全的基础架构现状

当前医院信息化网络多采用“核心—汇聚—接入”三层拓扑：核心层双机热备万兆交换机，冗余链路聚合实现毫秒级故障切换；汇聚层千兆光纤上下联；接入层支持802.1X的PoE交换机，服务无线AP、床边终端及IoT设备接入认证。硬件上，HIS、EMR、PACS等关键系统运行于x86虚拟化集群，N+1冗余刀片服务器，双活存储网关同步块级数据；边界出口配下一代防火墙与IPS联动，深度检测南北向流量保安全。软件上，微服务容器经Kubernetes编排，Overlay网络VXLAN封装，VNI与科

室编码映射隔离东西向流量；零信任网关校验API的JWT令牌并细粒度RBAC授权，降凭证劫持风险。可扩展性上，Spine-Leaf架构预留40 G上行接口，可平滑到100 G；虚拟化集群弹性扩展，满足影像AI推理等突发业务I/O需求[1]。

1.2 医院网络安全管理的现有措施与执行情况

医院现行网络安全管理以《医疗行业网络安全管理规范》为顶层文件，形成“制度—流程—记录”三级体系。制度层覆盖8领域，信息科每年牵头修订，现行版本v2024.2；流程层通过ITSM平台固化，工单SLA要求一级事件15 min响应、二级2 h闭环；执行层部署统一身份认证实现最小权限分配，终端安装EDR代理（病毒库更新≤4 h），USB端口需OA临时解锁。2024年4轮钓鱼演练中点击率从9.8%降至2.1%。但存在问题：12%外包账号未双因子认证，补丁延迟21 d，夜班漏检率3.7%，削弱控制的有效性。

2 医院信息化网络安全面临的主要风险与问题

2.1 内部管理漏洞引发的安全风险

医院内部管理漏洞是网络安全风险核心来源，体现在权限分配、员工意识和操作流程缺陷上[2]。权限分配不当导致最小权限原则失效，角色定义模糊或权限过度授予，如医生账号被赋予管理员权限，可篡改电子病历或处方数据，破坏数据完整性。员工安全意识薄弱表现为对钓鱼攻击、社会工程等威胁缺乏辨识力，2023年行业报告显示，医院员工点击钓鱼链接比例达15%～20%，导致凭证泄露或恶意软件植入，如攻击者窃取凭证进入HIS系统，非法导出患者隐私数据。操作流程不规范体现在变更管理缺失，如系统更新、补丁安装未执行标准化审批，造成配置漂移或后门漏洞，例如未审核脚本执行导致数据意外修改或删除。这些漏洞叠加放大风险：权限失控让内部人员可执行恶意操作，意识不足提高外部渗透成功率，流程缺陷延长漏洞暴露窗口。

2.2 外部攻击威胁下的系统脆弱性

医院网络系统在外部攻击下的脆弱性，主要源于系统更新滞后与防护措施缺失。系统更新滞后表现为关键软件补丁与设备固件未及时部署，漏洞长期暴露易被攻击者利用注入恶意代码或植入勒索软件。防护措施缺失体现在边界防御不足（防火墙未启用深度检测仅靠基础规则，难识别加密恶意载荷；入侵检测库更新慢，零日攻击响应滞后），且多数医院未部署DDoS防护设备，易引发服务中断。典型攻击路径有未修复漏洞入侵HIS系统勒索数据、SMB漏洞导致PACS瘫痪、DDoS攻击中断挂号服务。脆弱性放大机制为高可用要求限制维护窗口，异构设备增加防护难度[3]。

2.3 数据隐私泄露的潜在隐患

医院数据隐私泄露隐患主要存在于存储、传输与共享环节。存储环节中，患者敏感信息如电子病历、检验报告在数据库内未全字段加密，部分非结构化数据仅采用AES-128加密且密钥轮换周期超90天，数据库审计日志保留不足30 d，无法满足事后追溯要求[4]。传输层面，院内系统间约15%的API调用仍用HTTP明文协议，未强制启用TLS1.3，SSL证书未自动化更新，过期证书占7.2%，攻击者可通过ARP欺骗实施中间人攻击截取数据包。第三方共享风险突出：一是与医保平台、科研机构接口采用静态令牌认证，有效期达30天，未实施OAuth2.0动态授权；二是外包运维人员可通过VPN直接访问生产库，操作未纳入防火墙白名单；三是数据脱敏流程缺陷，如身份证号仅简单掩码（110105****1234）未用k-匿名化，结合其他数据集可重识别。这些隐患技术表现为：存储加密弱易被离线破解，传输协议缺陷致数据“裸奔”，共享控制弱易被违规爬取。攻击路径可表现为：利用弱加密漏洞导出隐私数据，通过中间人攻击获取诊断报告，利用第三方接口令牌窃取百万级患者信息。这些隐患可通过加密测试工具（如OpenSSL speed）测强度，用Wireshark捕获明文流量，通过Postman+Burp Suite检测接口越权风险。

3 医院信息化网络安全管理与维护的优化策略

3.1 强化内部安全管理体系建设

为强化内部安全管理体系，医院需构建“政策—流程—技术”闭环框架。政策层以《网络安全等级保护2.0》为基准，制定账号、数据、外包、应急4类主策略，明确安全目标、责任部门及问责条款，版本按年修订更新，年度评审同步法规。流程层通过ITSM平台固化：账号生命周期含“申请—审批—开通—审计—回收”5个节点，审批链采用双人复核及电子签名，一级事件15 min响应、二级2 h闭环；权限变更采用RBAC+ABAC混合模型，结合科室、职称、时段实现细粒度授权；操作日志推至SIEM，保留≥180 d支持异常回溯。技术层部署零信任网关，内网流量执行SPA单包认证，令牌有效期300 s、刷新窗口≤30 s降低劫持风险；终端用EDR与DLP联动，USB默认禁用，文件外发需审批并加水印（含用户ID与时间戳）追踪泄露路径。培训考核建立“新员工必修+年度复训+钓鱼演练”机制：按岗位分级培训，医生学习病历篡改法律后果，运维重点管理特权账号，考试通过率≥90%方可授权；每季度钓鱼演练，点击率超过5%需再培训，不合格者暂停账号。

3.2 升级技术防护手段抵御外部攻击

为抵御外部攻击，医院需构建“边界—流量—端点”三层防护体系[5]。边界层部署下一代防火墙与IPS联动集群，开启深度包检测与SSL解密功能，对进出流量执行双向特征比对，规则库每日更新，阻断已知漏洞利用；同时启用GeoIP过滤，屏蔽高风险国家/地区地址段，降低扫描面。流量层引入基于行为的NDR平台，通过NetFlow采样与机器学习模型识别横向移动、C&C通信等异常，模型训练窗口为7 d，告警阈值动态调整，误报率控制在2%以内。端点层推行EDR全覆盖，对工作站、PACS终端及IoT医疗设备植入轻代理，持续采集进程、DLL、注册表事件，利用ATT&CK映射检测无文件攻击；补丁管理用WSUS与第三方漏洞扫描器协同，扫描周期7 d，高危漏洞修复时限≤72 h，超时资产自动隔离。针对勒索软件场景，额外部署诱饵共享目录与写保护Gold Image，一旦加密行为触发蜜罐，EDR立即阻断进程并回滚快照，业务中断时间缩短至15 min。

3.3 完善数据隐私保护机制与应急响应

医院以“分类分级、加密先行”为原则重构隐私保护机制[6]。存储端采用AES-256-GCM全字段加密，密钥托管于FIPS 140-3合规的HSM，轮换周期7 d并支持密钥拆分，防止单点泄露；传输端强制TLS 1.3与双向证书校验，加密套件仅保留AES-256-GCM与ChaCha20-Poly1305，关闭弱算法降级。共享数据经k-匿名与差分隐私双重处理，k值≥5、$\varepsilon \leq 0.5$，确保重识别概率低于0.01。审计层部署数据库防火墙与UEBA，记录SELECT、UPDATE、DELETE三类语句，日志留存180 d并每日哈希上链，防止事后篡改。应急响应建立“检测—分级—遏制—根除—恢复”五环流程，事件分级以受影响记录数为基准，设定Ⅳ级＜1万、Ⅲ级1万～10万、Ⅱ级10万～100万、Ⅰ级＞100万，对应响应时限分别为1 h、2 h、4 h、8 h；指挥体系由CISO任总指挥，医务、法务、公关组成现场小组，必要时启动异地灾备，设定RPO≤15 min、RTO≤2 h的指标。演练层面每季度举行一次模拟泄露，覆盖勒索、内鬼、API越权三类场景，演练后更新剧本，确保快速闭环。

4 结束语

医院网络安全是医疗质量与患者安全的生命线。本研究证实：通过架构优化、流程固化和技术赋能的三维协同，可有效化解当前面临的内外部威胁。内部管理体系建设需强化政策刚性与执行闭环，技术防护应构建动态感知的智能防御体系，数据隐私保护则须贯彻加密先行原则与快速响应机制。未来研究需进一步探索医疗物联网设备认证、AI辅助威胁狩猎等新兴技术在医院场景的适配性，同时关注跨国医疗数据共享中的合规风控。只有持续完善网络安全韧性，才能支撑智慧医院建设行稳致远。

参考文献

[1]洪石陈.基于互联网的医院计算机网络信息安全策略分析[J].电子技术,2025,54(2):162-163.

[2]张秀岿.医院信息化建设中的网络安全与防护路径分析[J].工业控制计算机,2024,37(3):145-146.

[3]徐建武.医院信息化建设中计算机网络安全管理与维护[J].软件,2024,45(5):98-100.

[4]李贵臻.基于SAE网络的医院信息安全探索[J].网络安全技术与应用,2024(6):124-127.

[5]张晓平,刘晓娇.基于“安全大脑”的医院网络安全运营体系框架探讨[J].中国信息化,2024(7):81-84.

[6]尹晓帆,李晓会,张思琪.基于区块链和属性基加密的用户分类分级访问控制模型[J].计算机工程与科学,2025,47(9):1609-1618.

（本文编辑　吴文博）

