医院网络安全风险评估与技术防御体系构建

杜东林

身份证号：440602198903201510

摘　　要： 医疗行业数字化转型进程中，物联网设备泛在连接与数据共享机制加剧网络安全风险，2024年《医疗卫生机构网络安全管理办法》的颁布推动行业安全治理进入新阶段。研究聚焦医疗系统脆弱性特征与新型攻击场景，构建基于ISO 27005的多维度风险评估模型及智能化防御体系，通过AI异常检测、零信任架构等技术实现勒索软件、深度伪造等社会化攻击的有效遏制。结合协同化管理制度与ATT&CK应急框架，形成“技术－管理－人员”联动的动态防护机制，为平衡医疗业务效率与网络安全提供实践路径。

关 键 词： 医疗网络安全；风险评估；协同防御体系

Construction of Network Security Risk Assessment and Technical Defense System in Hospitals

Du Donglin

ID: 440602198903201510

Abstract: In the process of digital transformation in the healthcare industry, ubiquitous connectivity of IoT devices and data sharing mechanisms have exacerbated cybersecurity risks. The promulgation of the "Cybersecurity Management Measures for Medical and Health Institutions" in 2024 has ushered in a new phase of industry safety governance. This study focuses on the vulnerability characteristics of medical systems and new types of attack scenarios, constructing a multi-dimensional risk assessment model and intelligent defense system based on ISO 27005. By utilizing technologies such as AI anomaly detection and zero trust architecture, it achieves effective containment of social engineering attacks like ransomware and deepfakes. Combined with coordinated management systems and the ATT&CK emergency framework, it forms a dynamic protection mechanism that links "technology-management-personnel", providing practical paths to balance medical business efficiency with network security.

Keywords: healthcare cybersecurity; risk assessment; collaborative defense system

引言

随着“互联网＋医疗健康”战略的推进，医疗数字化转型加速，医疗信息系统与物联网设备互联在提升效率的同时扩大了网络攻击面。2024年5月发布的《医疗卫生机构网络安全管理办法》强调构建全生命周期安全管理体系，强化“三化六防”，标志着治理进入新阶段。医疗数据因高价值成为主要攻击目标，如2024年英国Synnovis医疗组织遭受勒索攻击导致血液供应危机所示。政策要求落实等级保护、动态防御及数据分类分级管理，并强调“管理、技术、运营”三位一体框架，提供从风险识别到应急响应的闭环指引。研究表明，医疗设备协议漏洞、供应链攻击和深度伪造加剧了脆弱性，需要智能化技术和制度创新来平衡安全与发展。探讨这些内容对保障患者安全和健康数据主权至关重要。

一、医院网络安全风险特征分析

（一）医疗信息系统脆弱性分析

医疗设备联网化进程加速了医疗服务的智能化转型，但嵌入式系统固件更新机制缺失、默认密码配置普遍化等问题，导致呼吸机、影像设备等关键医疗终端成为攻击渗透的突破口[1]。在系统集成层面，医院信息系统（HIS）、影像归档系统（PACS）与物联网设备的异构互联，因DICOM、HL7等医疗专用协议的安全校验机制薄弱，形成跨系统的横向攻击向量。患者隐私数据风险贯穿于采集、传输、存储及共享环节，电子病历（EMR）集中化存储与多机构数据交换需求，加剧了数据泄露风险，尤其当数据脱敏不彻底或访问权限失控时，可能触发HIPAA等合规性违规事件。

（二）新型攻击场景演化趋势

勒索软件攻击呈现医疗行业定向化特征，攻击者通过加密患者诊疗数据与设备控制系统，迫使医疗机构支付高额赎金，2023

年北美医院因 NotPetya 变种攻击导致急诊系统瘫痪即为典型案例。供应链攻击通过医疗设备固件、第三方运维软件植入恶意代码，利用医疗机构对供应商的安全信任链实现隐蔽渗透，研究显示医疗行业供应链漏洞利用率较其他领域高出37%。社会工程学攻击则针对医护人员职业特性，伪造医保机构通知、伪装临床研究合作等钓鱼手段，结合医疗敏感信息构建高欺骗性话术，2022年医疗行业钓鱼邮件打开率超过行业均值12个百分点，暴露行业特定防御短板。

二、医院网络安全风险评估方法

（一）多维度风险评估模型构建

基于 ISO 27005标准的风险评估框架，需系统性识别医疗场景核心资产（如电子病历、影像数据、医疗设备控制权限），通过威胁建模技术关联勒索攻击、数据泄露等典型威胁与系统脆弱性，建立资产价值 – 威胁频率 – 脆弱性评分的三维量化矩阵。在业务连续性评估维度，引入医疗专属风险评估矩阵（Risk Assessment Matrix），结合恢复时间目标（RTO）与最大容忍中断时间（MTD），量化网络攻击对急诊调度、手术室运维等关键业务的影响等级[2]。研究表明，当 HIS 系统中断超过4小时，三级医院日均经济损失可达常规营收的68%，凸显业务连续性评估的必要性。

（二）社会化攻击专项评估体系

针对钓鱼攻击的评估应构建多变量预测模型，结合邮件特征（发件人可信度、附件类型）、医护人员行为画像（科室职能、历史点击率）及上下文语义特征，使用逻辑回归与随机森林算法预测攻击成功概率。实验显示，该模型对医疗钓鱼邮件的识别准确率比传统规则引擎高29%。在 APT 攻击仿真中，基于 MITRE ATT&CK 框架还原攻击链，通过渗透测试验证从供应链入侵到横向移动的风险，蒙特卡洛模拟表明数据平台暴露面每增加10%，APT 攻击成功率上升17%。人员安全意识评估需设计动态指标体系，包括模拟钓鱼响应率、安全规程偏离度及培训后知识留存率，并通过时序数据分析揭示医护人员风险行为的波动规律[3]。

三、智能化技术防御体系构建

（一）基础防御架构优化

1. 医疗物联网设备准入控制技术

医疗物联网设备准入控制需建立动态设备指纹库，基于设备类型、固件版本、通信行为特征生成唯一身份标识，通过 IEEE 802.1X 协议实现网络层认证，并联动微隔离技术对监护仪、输液泵等设备实施最小权限访问控制[4]。实践表明，部署设备行为基线建模后，未授权设备接入尝试降低73%，异常协议流量下降58%。针对遗留设备兼容性问题，采用虚拟补丁技术拦截漏洞利用流量，在保持设备功能完整性的同时阻断攻击渗透路径。

2. 基于 AI 的异常行为检测系统

基于深度学习的异常检测系统需构建医疗专属行为特征库，采集电子病历访问模式、医嘱开立频次、设备操作日志等多模态数据，利用时序卷积网络（TCN）捕捉医护人员的操作时序关联性。当检测到超权限数据导出、非工作时段高频查询等异常行为时，系统可实时触发多因子身份核验，临床测试显示对内部数据泄露事件的检出时效提升至传统规则引擎的4.2倍。模型通过联邦学习实现跨院区知识共享，在保护数据隐私前提下将误报率控制在3% 以下。

（二）社会化攻击防范技术

1. 医疗场景深度伪造检测方案

针对伪造医生语音指令、篡改医学影像等新型攻击，需开发医疗专用检测模型。在音频维度提取梅尔频率倒谱系数（MFCC）与基频微扰动特征，结合临床术语数据库构建语音语义一致性校验模块[5]。在影像检测层面，通过残差网络分析 DICOM 文件头信息与像素级篡改痕迹，实验证实对 AI 生成的虚假 CT 图像识别准确率达98.7%。系统集成数字水印技术，在医学影像采集端嵌入不可见标识符，实现伪造溯源与证据固定。

2. 零信任架构在远程医疗中的应用

远程医疗场景中零信任架构的实施需构建软件定义边界（SDP），对移动终端、家庭监护设备进行持续设备健康度评估，结合上下文感知引擎动态调整访问策略。医生通过5G 网络调阅患者数据时，系统实时验证设备证书、地理位置与操作行为基线，若检测到跨地域异常访问立即启动会话终止与密钥轮换[6]。部署基于属性的加密（ABE）技术，确保电子病历仅在满足预设属性条件（如执业医师资格、特定时间窗）时方可解密，临床验证显示该方案将越权访问风险降低89%。

四、协同化安全管理机制

（一）制度保障体系建设

1. 医疗网络安全合规性框架设计

医疗网络安全合规性框架需整合 HIPAA、GDPR 与《网络安全法》等法规要求，构建覆盖数据采集、传输、存储的全周期管理矩阵。框架设计采用层次化结构，底层对接 ISO 27001信息安全管理体系，中间层嵌入医疗行业专属控制项（如 DICOM 影像加密标准），顶层建立自动化合规监测工具链。通过部署实时审计模块与风险评估引擎，实现合规差距的动态可视化呈现，某三甲医院实施后年度合规违规事件减少61%。

2. 第三方服务商风险管理规范

第三方风险管理需建立供应商安全准入评估模型，涵盖代码安全审计、数据接口防护等级、应急响应承诺书等12项核心指标。在服务存续期实施持续监控，采用区块链技术对运维操作日志进行分布式存证，确保服务商行为可追溯。针对医疗设备维保等高风险场景，规范要求签署网络安全连带责任协议，2023年某省级医疗集团通过该机制成功追责3起供应链安全事件。

（二）人员能力提升工程

1. 分岗位网络安全培训体系

基于医疗岗位风险画像构建差异化培训模型，临床医生侧重

患者数据保护规程，设备操作人员聚焦物联网安全操作规范，行政人员强化钓鱼邮件识别技能[7]。培训系统集成自适应学习引擎，根据模拟攻击测试结果动态调整课程内容，某区域医疗中心应用后医护人员安全规程执行合格率提升47%。建立培训效果量化评估体系，将钓鱼邮件点击率下降幅度与岗位晋升资格挂钩。

2. 社会工程攻击模拟演练方案

设计医疗场景专属攻击剧本库，包含伪造医疗设备召回通知、虚假学术会议邀请等12类高危场景。演练采用红蓝对抗模式，红队利用开源情报（OSINT）生成个性化钓鱼内容，蓝队通过行为分析平台捕获员工响应数据[8]。2023年某三甲医院演练数据显示，放射科医师对伪造影像会诊邀请的识别耗时平均缩短38秒，但行政人员对虚假采购邮件的误判率仍高出临床岗位23%。

（三）应急响应机制创新

1. 基于 ATT&CK 框架的医疗应急预案

参照 MITRE ATT&CK 企业版构建医疗攻击战术库，将初始访问（如鱼叉式钓鱼）、横向移动（利用 PACS 系统漏洞）等11个战术阶段映射到具体处置流程。预案集成自动化剧本执行引擎，当检测到勒索软件加密行为时，自动隔离感染设备并启动备用 HIS 系统，某省级医院实测将应急响应时间从127分钟压缩至19分钟[9]。建立跨机构协同处置流程，通过医疗安全信息共享平台实现威胁情报实时同步。

2. 事件溯源与知识库建设机制

构建多维度溯源分析体系，结合网络流量镜像、终端行为日志与沙箱动态分析，还原攻击者从社工钓鱼到数据渗漏的完整攻击链。知识库采用本体论建模方法，将事件案例、漏洞特征、处置方案等要素结构化存储，2023年收录的427起医疗安全事件分析显示，68% 的 APT 攻击存在相似战术模式[10]。开发智能检索接口，通过自然语言处理（NLP）技术实现历史案例的相似性匹配，辅助制定处置策略。

五、总结与展望

医疗网络安全体系建设融合了风险治理与技术防御，通过资产 – 威胁 – 脆弱性关联分析和业务连续性评估矩阵，实现了从静态到动态的风险量化评估。AI 驱动的异常行为检测系统在医疗物联网准入控制、深度伪造检测等场景的应用，使内部威胁检出时效提升4.2倍，零信任架构降低远程医疗越权访问风险89%。基于 ATT&CK 框架的应急预案压缩典型应急响应时间85%，知识库为68% 的 APT 攻击提供处置参考。然而，仍面临5G+ 边缘计算扩展攻击面、外包人员生物识别凭证滥用等挑战。未来需研究数字孪生安全防护、量子密钥分发等技术，深化技术与管理、人员能力的耦合，构建弹性自适应的安全生态，实现暴露面收敛、攻击链阻断与事件响应闭环的协同。

参考文献

[1] 王颖 . 医院信息化网络安全防御对策分析 [J]. 世界最新医学信息文摘 ,2022,22(98):52-56.

[2] 覃德泽 , 蒙军全 . 网络安全风险评估方法分析与比较 [J]. 网络安全技术与应用 ,2011(4):23-25.

[3] 徐慧琼 . 有关大数据时代背景下网络安全风险评估关键技术研究 [J]. 网络安全技术与应用 ,2017(7):72,89.

[4] 吴金宇 . 网络安全风险评估关键技术研究 [D]. 北京邮电大学 ,2013.

[5] 罗旭 . 网络安全风险评估系统的研究与设计 [J]. 信息与电脑 ,2018(8):125-126,129.

[6] 袁泉 . 医院网络安全管理方案与措施 [J]. 中国新通信 ,2019,21(15):169.

[7] 胡正刚 . 医院信息系统内外网合并面对的挑战和应对方法 [D]. 北京 : 北京邮电大学 ,2009.

[8] 贡觉拉姆 , 仁青青措 , 琼吉 . 医院网络信息安全问题与安全防护方案分析 [J]. 电脑采购 ,2023(52):37-39.

[9] 文伟平 , 郭荣华 , 孟正 , 等 . 信息安全风险评估关键技术研究与实现 [J]. 信息网络安全 ,2015(2):7-14.

[10] 杨君普 . 网络安全防御与风险评估 [J]. 网友世界 · 云教育 ,2014(16):11-11.