基于资产依赖的医院网络安全精准防御新路径研究与应用

焦一凡　李　伟　魏　菲　王东宇*
天津康复疗养中心　天津　300000

摘　要：目的：聚焦当前医院网络安全防护存在防御体系碎片化、响应效率低、安全策略与医疗业务脱节等痛点问题，构建以资产依赖关系为核心的医院网络精准防御路径，提升防护效能，为医院网络安全运行提供技术支撑。**方法：**构建动态资产依赖图谱，刻画医疗业务链与网络资产“物理、系统、应用、数据”四层关联，搭建一体化联防体系，并在HIS、PACS系统中开展实践验证。**结果：**该防御路径实现医院网络安全防护从被动向主动精准转型，实施后安全事件平均响应时间缩短至3分钟（P=0.023），漏洞精准处置率提升至92%（P=0.018），医疗物联网设备漏扫覆盖率达98%（P=0.031），核心诊疗业务年均中断次数为0。**结论：**基于资产依赖的医疗网络联防体系可打破传统防护孤立局面，契合医疗业务优先级与合规要求，可行性、实用性较强，可为医院及医疗行业网络安全建设提供实践参考。

关键词：医院网络安全；资产依赖；精准防御；动态资产依赖图谱；医疗网络联防体系；医疗数据安全

引言

本中心运维面临三大问题：资产管理存盲区，医疗物联网设备及哑终端管控缺失，易成攻击突破口[7]；防御模块相互独立，防火墙、IDS、WAF等设备单独运行，缺乏协同联动[2]；安全响应耗时较长，海量告警分散在不同系统，难以快速精准判断攻击意图与影响范围，无法第一时间处置[3]。剖析成因，问题根源在于传统安全策略与医疗业务脱节，防护偏向单点设备，忽视资产与诊疗业务关联，威胁评估滞后，无法保障核心业务连续[3]。精准梳理资产依赖关系是破解关键，可展现组件间功能、数据、服务关联，推动防护从单点安全转向业务连续性保障[4]。国内研究多聚焦单一技术，缺少系统性思维。本研究立足医院实际，构建以资产依赖为核心的精准防御模式，破解碎片化难题，输出系统化可落地方案。

一、医院网络资产依赖关系的内涵与多维分析

构建科学合理的医院网络安全精准防御路径，首要任务是明确医院网络资产的独特属性及资产依赖关系的核心内涵，这是构建精准防御体系的基础，也是保障医院网络安全稳定运行、适配医疗业务需求的重要支撑。

（一）医院网络资产的特性

医院网络环境是一个高度异构、实时性要求极为严苛的复杂生态系统，其网络资产价值密度高，且与日常诊疗活动紧密关联，直接关系到患者的生命健康安全。结合医院运营实际，这些网络资产主要呈现三大核心特征：业务相关性、实时性极端化、技术架构异构化。

业务相关性具体体现为，医院网络中的每一项资产都与一项或多项诊疗业务存在强关联，是医疗服务正常开展的必要支撑，资产出现安全问题可能直接导致相关诊疗业务中断；实时性极端化主要体现在急救、手术等核心诊疗业务中，对数据传输与处理的低延迟要求极高，一旦网络中断或数据传输延迟，可能直接危及患者生命安全；技术架构异构化则是由于医院网络中各类技术、设备的接口标准、通信协议存在显著差异，导致网络管理复杂度大幅提升，也增加了安全防护的难度[5]。

（二）构建动态资产依赖图谱

1.资产依赖关系的多维度建模

医院信息系统的资产依赖关系是动态交织的复杂网络，可从四个维度建模刻画[1]：

物理层依赖：基于网络连接、电力等基础设施。如急诊CT机依赖接入交换机，交换机又依赖核心网络，任一环节中断将直接导致业务瘫痪，须优先保障该链路稳定性。

系统层依赖：体现于操作系统、数据库、中间件等服务调用与资源竞争。以PACS系统（优先级5级）为例，其稳定运行依赖Oracle数据库支撑数据持久化；若数据库异常，影像调阅即受影响，进而波及临床决策与手术规划，埋下安全隐患。

应用层依赖：业务应用通过API、Web Service等接口交互形成服务网络。如门诊工作站发起CT申请时，需调用PACS预约接口并联动收费系统，任一应用故障将沿依赖链传导，阻碍就诊流程。

数据层依赖：围绕数据全生命周期关联。电子病历（优先级5级）需数据支撑，医保结算依赖HIS费用数据；数据泄露或篡改可引发临床误诊或结算错误，损害患者权益。

2.信息采集

建立精准的动态资产依赖图谱，需从多类数据源获取内容并清洗整合，为图谱构建奠定数据基础。过程包括多源数据采集和数据清洗整合两部分。

（1）多源数据采集

采用多手段协同互补方式开展采集。通过镜像核心网络流量，运用DPI与NTA技术反演资产通信行为，捕捉医疗物联网设备与HIS、PACS的交互数据，提取关键信息以识别潜在依赖关联。针对未备案设备及哑终端管控盲区，采用无侵入式端口扫描进行探测，确保采集无遗漏。同时，从CMDB、APM系统及各类日志中提取资产配置依赖与服务调用链数据，重点关联核心业务系统信息。借助专业监控工具实时采集服务器资源占用情况，监测PACS数据库服务器等核心设备运行状态。此外，对接应用系统日志接口，结合HIS挂号、就诊记录与系统间调用信息，围绕诊疗数据流转链路梳理应用层资产依赖关系。

（2）数据清洗与整合

数据清洗与标准化是保障资产依赖关系精准梳理的关键环节。清洗阶段对多源数据筛选提纯，剔除重复、错误数据，如过滤异常流量、修正日志时间戳偏差，保留与医疗业务关联紧密的有效数据。标准化阶段统一不同来源的数据格式与命名规范，如服务器时间戳统一采用UTC，确保业务流转链路可追溯。最后通过数据关联，以IP、MAC地址为纽带整合同一资产的多源信息，重点梳理医疗设备与核心系统的依赖关联，构建完整资产档案，满足动态依赖图谱构建的核心数据需求。

3.数据处理与图谱构建

采集并处理完成的标准化数据，用于搭建动态资产依赖图谱，图谱以属性图形式完成存储，Node即节点对应医院网络内的各类资产，Edge即边对应资产之间存在的依赖关系，携带的流量、频率、协议等属性，可对依赖强度做量化计算，节点和边都会标注对应资产的医疗优先级，最终完成资产依赖关系的精准刻画。

二、基于资产依赖的医院网络安全精准防御新路径构建

基于医院网络资产特性、资产依赖关系及业务优先级，构建分层协同的网络安全精准防御新路径。架构包含资产感知、智能分析、统一展现三层，实现“采集–分析–指挥”全流程协同；明确核心医疗适配点：感知层精准识别医疗物联网设备，分析层聚焦PACS/EMR依赖分析，展现层侧重核心诊疗业务安全评分，确保防御体系与医疗业务深度适配。

（一）资产感知层

资产感知层是数据基石，负责医院全域网络资产的发现清点与实时监控，重点保障医疗优先级5级资产的实时感知，输出精准数据，支撑后续决策。该层混合采用主动与被动探测：主动探测为无侵入式扫描，发掘未备案资产和哑终端；被动探测依托流量分析，捕捉资产的通信行为和状态变化，确保无遗漏。面向物联网设备，借助协议仿真与深度包解析技术，实现特定品牌型号设备的精准识别。资产感知层会持续输出标注医疗优先级的资产清单，输出网络流量元数据资产性能指标、安全事件原始日志，定向捕获核心业务系统和高优先级医疗设备的运行数据，完成医疗资产全生命周期的可视化管理，支撑后续智能分析差异化防护。

（二）智能分析层

智能分析层是整个防御模式的核心大脑，承担资产依赖分析、风险研判与优先级排序，核心组件包括动态资产依赖图谱引擎和风险传导分析模型。图谱引擎基于感知层数据，调用图计算算法构建并实时更新动态资产依赖图谱，支持正向查询（明确某资产依赖的其他资产）和反向影响分析（某资产被哪些关键诊疗业务依赖），梳理高优先级资产的完整依赖链路，展示资产安全问题波及的业务范围。风险传导模型依托动态资产依赖图谱，自动计算资产安全风险对关联业务的影响程度，对应BIA，计算过程结合资产的医疗优先级，完成差异化风险评估，输出安全处置的决策依据。

（三）统一展现层

统一展现层作为防御体系的可视化窗口与协同指挥平台，为运维人员和管理者提供差异化视图，深度融合安全数据与医疗业务。面向运维人员，提供全链路攻击路径可视化分析功能，重点标记高优先级医疗资产的关联依赖链路，助力快速定位攻击源头、研判影响范围并提供处置指引；面向管理者，其展示的核心诊疗业务链安全健康度评分，基于风险传导模型BIA结果与资产医疗优先级计算生成，直观呈现核心业务安全状态，支撑安全投入决策落地。

三、实施效果评估

（一）量化指标对比

选取我中心2025年6–12月（防御体系实施前）与

表1

指标名称	实施前	实施后	提升幅度	统计显著性（P值）
安全事件平均响应时间	150分钟	3分钟	97.5%	0.023
漏洞精准处置率	45%	92%	47%	0.018
核心业务中断次数（年均）	3次	0次	100%	0.027
安全告警误报率	38%	7%	81.6%	0.015
漏洞修复平均周期	72小时	4小时	94.4%	0.021

注：检验水准 $\alpha=0.05$。

2026年1–3月（防御体系实施后）的网络安全运维统计数据，对比实施前后的5项核心安全指标，所有数据经配对t检验，差异均具有统计学意义（$P<0.05$），具体对比情况如表1。

（二）效果分析

该防御体系实现决策数据化与运营高效化双重收益：安全团队依托风险传导模型量化的业务影响度及资产优先级，以量化形式向院领导汇报网络安全风险，为安全投入决策提供支撑，推动资源向高优先级医疗资产倾斜，优化资源配置并提升安全投入性价比；自动化处置替代人工完成大量告警排查与处置工作，安全运维效率提升60%，且适配等保2.0三级要求，减少合规整改成本。同时，漏洞检测与医疗业务依赖关系、资产医疗优先级深度结合，使漏洞处置精准度提升47%，有效规避“重检测、轻处置”、“无差别处置”问题，贴合医院“业务优先、安全护航”的运营需求，保障核心诊疗业务连续运转。

四、结论与展望

（一）研究成果总结

本研究聚焦医院网络安全碎片化、响应滞后、业务脱节难题，构建以资产依赖为核心的医疗网络联防体系。通过动态资产依赖图谱精准映射诊疗业务链路，融合资产优先级与合规规则，实现防护与医疗业务深度适配，推动被动响应向主动精准转型[6]。实践表明，该体系显著提升响应效率与漏洞管理水平，强化高级威胁防御能力。实施后安全事件平均响应时间由150分钟缩至3分钟，漏洞精准处置率达92%，医疗物联网漏扫覆盖率升至98%，核心业务年均中断归零，有效破解传统防御与业务脱节困境，为医疗数字化转型提供系统化、可落地的安全路径。

（二）研究局限与未来展望

本研究仍存局限：其一，云端资产依赖分析尚未全覆盖，如互联网医院平台在混合云场景下的适配效果需进一步验证；其二，风险传导模型权重多基于历史数据与运维经验，面对新型物联网攻击手段，动态适配能力待提升。后续研究可从两方向深入：一是扩大资产覆盖范围，重点补充云端与边缘设备依赖建模，优化图谱更新机制，增强对混合IT架构的适配能力；二是融合医疗合规要求，构建整合预警、应急、审计的安全模式，为智慧医院建设筑牢合规防线，推动行业防护水平稳步提升。

参考文献

[1]郭晓佳，谢丹，周伟名，等.市级气象信息网络防护体系构建与AI驱动防御展望[J].网络安全技术与应用，2026，(02)：116-119.

[2]马丽明，黄少斌，江卓斌，等.多院区医院网络安全及边界防护体系建设与实践[J].中国数字医学，2025，20(12)：93-98.

[3]董成银.探讨基于攻防实战的医院网络安全防护体系构建与优化[J].网络安全和信息化，2025，(07)：37-39.

[4]侯爽，李寅，杜元太.医院态势感知网络安全平台建设实践[J].中国卫生信息管理杂志，2023，20(05)：808-813.

[5]胡俊，潘永红.医院信息化网络安全防护体系的多层架构设计与技术保障[J].中国高新科技，2025，(06)：55-57.

[6]贾志勇.智慧医院网络安全体系的构建与优化[J].网络安全和信息化，2025，(08)：147-149.

[7]于雪梅.医疗设备网络与数据安全防护体系研究[J].中国数字医学，2022，17(02)：12-16.