医疗机构信息系统网络安全风险评估与防护策略研究

汪靖朝

（峨眉康复疗养中心，四川　乐山　614200）

摘　要： 针对医疗机构信息系统面临的网络安全威胁，从外部攻击、内部管理和技术架构3个维度对安全风险进行系统分析；在此基础上，参照ISO 27005和等级保护2.0标准，构建涵盖风险评估框架与“管理—边界—系统—数据”四层递进防护策略的综合安全体系，旨在为医疗机构提升信息系统安全韧性提供可落地的技术参考。

关键词： 医疗机构；信息系统；网络安全；风险评估；防护策略

中图分类号： TP393　　**文献标识码：** A

Research on network security risk assessment and protection strategies for medical institution information system

WANG Jingzhao

（Emei Rehabilitation and Sanatorium，Leshan，Sichuan 614200，China）

Abstract: The security risks posed by external attacks, internal management, and technical architecture to medical institution information systems are systematically analyzed from three dimensions. On this basis, a comprehensive security system is constructed with reference to the ISO 27005 standard and the Level Protection 2.0 standard, incorporating a risk assessment framework and a four-layer progressive protection strategy covering management, network boundaries, systems, and data. The proposed system is intended to provide an implementable technical reference for enhancing the security resilience of information systems in medical institutions.

Key words: medical institution，information system，network security，risk assessment，protection strategy

1　引言

近年来，医疗卫生行业信息化步入加速发展阶段，电子病历、远程诊疗、移动护理等业务对信息系统的依赖程度持续加深。医疗数据具有高度私密性和不可替代性，一旦发生泄露，极易引发隐私侵害、医疗欺诈甚至身份盗用。同时，医疗机构内网发生异常可能直接影响医疗业务运行，甚至危及患者生命安全。因此，开展医疗领域网络安全研究具有突出的现实紧迫性。

围绕上述问题，国内外学者已从不同视角开展相关研究。在技术安全层面，董良[1]探讨了医院信息化建设中的网络安全防护方法；李铮等[2]从安全架构角度提出了医院信息系统改造思路；杨霞等[3]针对智慧医院场景分析了安全隐患及应对措施；张舒[4]研究了网络环境下医院信息系统数据安全保障体系的构建；瞿朗等[5]结合实际总结了网络安全规划与建设经验。在法律合规与隐私保护层面，韩作为等[6]系统研究了医疗机构个人信息保护合规体系；侯爽等[7]基于等保2.0开展了互联网医疗三级等保测评实践；张思梦等[8]从人工智能视角提出了完善个人医疗信息法律保护的建议；于沈悦等[9]关注了大数据时代公权力行使与患者信息保护之间的冲突；么晓月等[10]分析了大数据背景下电子病历的法律合规问题。

现有研究或侧重技术防护，或侧重法律合规，将风险评估框架与多层次防护策略相结合的研究相对较少。基于此，本文融合技术与合规双重视角，在风险识别与分析的基础上提出分层防护方案：系统梳理医疗机构面临的技术安全风险；借鉴相关国际标准构建网络安全风险评估框架；提出由管理制度、网络边界、系统安全和数据安全构成的四层防护体系。

2　医疗机构信息系统网络安全风险分析

2.1　外部网络攻击风险

（1）勒索软件攻击：典型攻击链通常遵循“初始渗透—横向移动—数据加密”的过程：攻击者常通过鱼叉式钓鱼邮件（Spear Phishing）诱导用户点击恶意附件并建立C2通道，随后借助Pass-the-Hash和Mimikatz等手段获取更高权限，进一步横向渗透至HIS及PACS等核心业

务系统，最终投放加密载荷（Payload）并索取赎金。近年来，勒索攻击逐步呈现针对医疗机构定向化发展的趋势，攻击者通常会提前侦察目标机构的网络环境和业务特征，再制定针对性的攻击方案，以提高攻击成功率和获利能力。

（2）SQL注入：部分早期开发的在线预约、报告查询等外部接口缺乏参数化查询机制，攻击者可能通过构造恶意SQL语句绕过身份认证或直接访问后端数据库。

（3）高级持续性威胁（APT）：攻击周期可能持续数月甚至数年，通常涉及侦察、武器化、投递、利用、安装、控制和行动等阶段。

2.2 内部安全管理风险

相较于外部攻击的技术复杂性，内部安全管理风险更多源于人员因素和管理制度不完善。部分医院员工仍存在使用弱口令或默认密码登录系统的情况，为暴力破解等攻击提供了可乘之机；在权限管理方面，“一人多权”、离职人员账号未及时回收等问题较为突出。此外，部分医疗机构专职信息安全人员不足，中小型医院的信息部门往往同时承担系统运维和安全管理职责，难以投入足够力量开展安全基线核查、风险排查和应急演练。

2.3 技术架构层面的安全隐患

部分医疗机构核心业务系统建设时间较早，底层仍运行 Windows Server 2008 甚至 Windows XP 等已经停止技术支持的操作系统，中间件和数据库版本也相对滞后，大量已披露的CVE漏洞因厂商不再提供补丁而长期处于暴露状态。

在系统架构方面，C/S架构的老旧HIS与B/S架构的新建子系统长期并存，部分系统缺乏统一的API网关和企业服务总线（ESB），系统之间主要采用点对点方式进行连接，使各类开放接口成为潜在的横向渗透入口。同时，智能输液泵、心电监护仪等IoT医疗设备大量接入医院内网。由于部分设备硬件资源有限，可能存在明文通信、缺乏固件签名校验以及升级能力不足等问题。部分医院内网仍采用相对扁平的二层组网方式，缺少必要的微分段（Microsegmentation）机制，一旦某个节点遭到入侵，攻击者可能进一步向其他网络区域横向扩散。

3 网络安全防护策略研究

3.1 网络安全风险评估框架构建

科学、持续的风险评估是实施网络安全防护的基础。本文参照 ISO 27005 信息安全风险管理标准、GB/T 20984 信息安全风险评估规范及等保 2.0 基本要求，构建“资产识别—威胁分析—脆弱性评估”的三维综合评估方法。

如图 1 所示，资产识别以配置管理数据库（CMDB）为基础建立信息资产台账，并借助 Nmap 等工具探测活跃主机、开放端口和运行服务，再依据资产的业务重要性进行分级赋值。威胁分析接入 CNVD，并通过 STIX/TAXII 对接外部威胁情报，形成持续更新的威胁图谱，重点跟踪针对医疗行业的攻击组织及其战术手法。脆弱性评估则定期使用 Nessus 及 OpenVAS 等扫描工具对全量资产进行漏洞核查，并辅以渗透测试验证漏洞的实际可利用性。在此基础上，将资产价值、威胁可能性和脆弱性严重程度纳入风险矩阵，确定各项资产的风险等级。

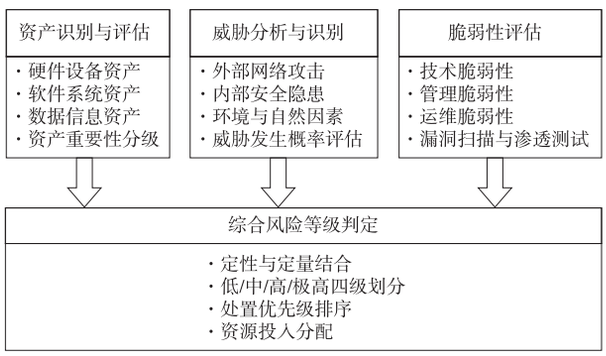

图1 医疗机构信息系统网络安全风险评估框架

风险评估应形成周期化机制，每季度开展一次全面评估，在发生重大系统变更或安全事件时及时开展复评。同时，通过风险登记册记录风险责任人、风险缓解措施及整改时限，实现风险处置过程的持续跟踪和审计。

3.2 多层次防护策略体系

基于上述风险评估结果，本文提出“管理制度与合规—网络边界防护—系统安全加固—数据安全核心”的四层递进防护体系，如图 2 所示。

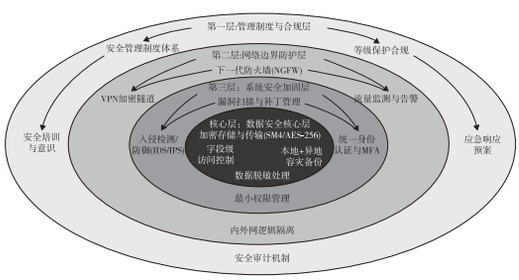

图2 网络安全多层防护策略体系

（1）管理制度与合规层：医疗机构网络安全治理的基础，核心任务是依据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》及等保 2.0 相关规定，建立涵盖安全策略、组织架构、人员管理和安全培训等内容的制度体系。同时，通过全员安全意识教育和钓鱼演练增强人员安全意识，推动安全管理制度有效落实。

（2）网络边界防护层：部署具备深度包检测（DPI）能力的下一代防火墙（NGFW），利用 IPS 以在线（Inline）模式对进出网络流量进行协议解析和攻击特征匹配；远程访问统一通过 IPSec 或 SSL VPN 隧道接入，并与 DMZ 公开服务区域严格隔离；部署 NTA/NDR 设备，对东西向网

络流量进行持续监测。通过VLAN和ACL将门诊、住院、财务、科研等业务划分为相对独立的安全域，并限定跨域访问白名单；IoT医疗设备子网采用独立的物理或逻辑隔离区域，通过单向网关仅上送必要的监控信息，以收窄网络暴露面。

（3）系统安全加固层：建立覆盖“扫描—评估—修补—验证”4个环节的漏洞管理闭环，对在役系统定期开展自动化漏洞扫描，并依据CVSS评分确定漏洞修补优先级。对于无法直接进行补丁升级的老旧系统，可借助WAF或IPS规则实施虚拟补丁（Virtual Patching），在不修改系统本体的情况下降低已知漏洞被利用的风险。在关键区域部署IDS/IPS，并将可疑行为联动至SOC中的SIEM进行关联分析和告警。身份安全方面，建设统一IAM平台，支持SAML/OAuth单点登录并强制启用MFA；权限管理遵循最小权限原则和RBAC模型。终端部署EDR代理开展行为监测和威胁狩猎，新系统上线前进行安全基线检查，包括禁用冗余服务、清理默认账户和开启审计日志等，以降低系统被攻击和利用的风险。

（4）数据安全核心层：作为防护体系的最内层，数据安全直接关系到患者隐私保护和医疗数据合规。静态数据采用SM4或AES-256进行加密存储，数据传输全程强制使用TLS 1.3；数据库访问采用基于属性的访问控制（ABAC），结合字段级权限对身份证号、疾病史等敏感字段的访问和操作权限进行细粒度管理。同时，部署数据库活动监控（DAM），实时记录并审计数据库访问行为。数据备份遵循“3-2-1”原则，即保留3份数据副本、使用2种不同介质并保存1份异地备份，同时明确RPO和RTO目标。非生产环境使用的数据应进行脱敏或匿名化处理，并在数据出口部署DLP，对通过邮件、U盘或网络传输等方式进行的敏感信息外泄行为进行阻断。

4　结束语

本文从外部攻击、内部管理和技术架构3个维度分析了医疗机构信息系统面临的网络安全风险，在此基础上参照国内外相关标准构建风险评估框架，并提出管理制度与合规、网络边界防护、系统安全加固和数据安全核心四层防护策略。该体系兼顾技术防护与安全管理，可为不同规模医疗机构开展网络安全建设提供参考。对于小型医院，可优先落实网络边界防护、数据加解密等基础措施；对于大型三甲医院，则宜进一步完善整体防护体系，并结合SOC实现网络安全常态化运营。

参考文献：

[1] 董良.医院信息化建设中网络安全防护措施[J].电脑知识与技术，2021，17（16）：32-33+45.
[2] 李铮，魏星，佟明泽，等.基于网络安全的医院信息安全设计改造与分析[J].微型电脑应用，2021，37（3）：10-12.
[3] 杨霞，王菲菲，陈金栋.新形势下智慧医院网络安全风险分析及对策研究[J].网络安全技术与应用，2022（5）：126-127.
[4] 张舒.网络环境下医院信息系统数据安全保障体系构建研究[J].网络安全技术与应用，2023（2）：60-61.
[5] 瞿朗，左秀然，杨国良，等.医院网络安全规划与建设实践探讨[J].中国卫生信息管理杂志，2023，20（3）：431-435.
[6] 韩作为，李宏芳，赵韡.医疗机构构建个人信息保护合规体系研究[J].中国数字医学，2022，17（3）：26-29.
[7] 侯爽，李寅，许扬.基于等保2.0标准的互联网医疗系统三级等保测评实践探索[J].中国数字医学，2022，17（3）：101-104.
[8] 张思梦，霍增辉.人工智能时代完善个人医疗信息法律保护的研究[J].中国卫生法制，2023，31（6）：6-10.
[9] 于沈悦，王霞.大数据时代公权力执行与患者个人信息保护[J].医学与哲学，2024，45（5）：58-62+68.
[10] 么晓月，戴昱，赵因.大数据背景下电子病历的法律合规[J].医学与法学，2024，16（1）：44-47.

作者简介：

汪靖朝（1996—），本科，助理工程师，研究方向：计算机技术、网络安全。