医院信息网络安全风险分析与防护体系构建研究

张雅雯

（天津市眼科医院，天津 300020）

摘 要： 医院作为关键信息基础设施，其网络安全直接关系到时医疗服务连续性、患者隐私保护及医疗数据安全。文章分析了医院信息网络面临的主要安全风险，探讨了医院网络安全管理存在的问题，并构建了覆盖“技术防护—管理制度—人员培训—安全运营”四位一体的医院信息网络安全防护体系，以期为智慧医院网络安全建设提供参考。

关键词： 医院信息化；网络安全；数据安全；智慧医院；风险防护

中图分类号： TP393 **文献标识码：** A

Research on network security risk analysis and protection system construction for hospital information system

ZHANG Yawen

（Tianjin Eye Hospital，Tianjin 300020，China）

Abstract: As critical information infrastructure, the network security of hospitals directly relates to the continuity of medical services, the protection of patient privacy, and the security of medical data. This paper analyzes the main security risks faced by hospital information networks, discusses the problems existing in hospital network security management, and constructs a four-in-one hospital information network security protection system covering “technical protection—management system—personnel training—security operations” aiming to provide a reference for the network security construction of smart hospitals.

Key words: hospital informatization，network security，data security，smart hospital，risk protection

1 引言

随着智慧医院建设的不断推进，医院信息系统（HIS）已广泛应用于医疗服务、护理管理、医学检验、医学影像、药品管理及医院运营等环节，信息化水平持续提升。电子病历、HIS、实验室信息系统（LIS）、医学影像存储与传输系统（PACS）以及互联网医院等业务平台实现了互联互通，在提高医疗服务效率和管理水平的同时，使医院网络环境日趋复杂。由于医院存储着大量患者隐私数据和重要医疗信息，且医疗业务具有连续性要求高、系统依赖性强等特点，一旦发生网络攻击、数据泄露或系统瘫痪，不仅会影响医院正常诊疗秩序，还可能危及患者生命安全[1]。因此，加强医院信息网络安全风险分析，建立科学完善的网络安全防护体系，已成为智慧医院建设的重要内容。

2 医院信息网络安全风险分析

医院信息网络安全风险呈现多源化与复杂化特征，主要体现在外部攻击、数据泄露、内部管理、医疗设备及云平台5个方面。（1）外部攻击风险。攻击者可通过漏洞扫描、弱口令攻击、SQL注入、Web攻击及勒索病毒传播等方式入侵医院系统。其中，勒索软件一旦攻击成功，可能导致HIS、EMR等核心业务系统瘫痪，造成严重业务中断与经济损失；APT攻击隐蔽性强、持续时间长，能够长期窃取患者信息和科研数据。（2）数据泄露风险。医院存储大量敏感医疗数据，一旦因数据库权限配置不当、接口访问控制不足、数据传输未加密、终端违规操作或云平台配置错误等问题导致泄露，将对医院声誉及合规性带来重大影响。（3）内部管理风险。部分医务人员安全意识不足，存在共享账号、弱口令及违规外接设备等行为；第三方运维人员若缺乏严格审批，也可能引发安全隐患。（4）医疗设备风险。CT与MRI等医疗设备因系统版本较低及厂商权限管理不足，易成为攻击入口。（5）云平台风险。互联网医院及云平台业务在身份认证和接口安全不足的情况下，可能导致数据泄露与业务中断，使医院网络安全风险由传统局域网逐步向云端和终端延伸[2]。

3 医院网络安全管理存在的问题

医院信息网络安全管理仍存在明显薄弱环节，主要

体现在体系建设、制度执行、技术监测及人员意识等方面。在体系建设方面，部分医院仍以传统边界防护为主，缺乏纵深防御与整体协同的安全理念，各类安全设备往往独立运行，未形成统一联动和集中管控机制，导致整体防护能力有限。在制度执行方面，虽然多数医院已建立较为完善的信息安全管理制度，但在实际执行过程中仍存在明显差距，尤其是在账号管理、权限审批、密码设置、数据备份及漏洞修复等关键环节，落实力度不足，制度要求与实际运行脱节现象较为普遍[3]。在技术监测方面，多数医院仍依赖人工巡检方式，缺乏安全态势感知和集中监测平台，难以及时识别异常访问、恶意流量及潜在攻击行为，导致安全事件发现滞后、响应效率较低。在人员意识等方面，医务人员普遍将工作重心放在临床业务，对网络安全重视不足，安全培训覆盖不够全面，对钓鱼邮件、恶意链接等常见攻击手段的识别能力较弱，容易成为网络攻击的突破口，从而进一步放大整体安全风险。

4　医院信息网络安全防护体系构建

4.1　构建网络纵深防御架构

医院信息网络安全应采用纵深防御理念，构建“边界安全—网络安全—主机安全—应用安全—数据安全”的五层防护体系，通过多层协同实现整体防护能力提升[4]。在边界层部署下一代防火墙、IDS/IPS 及 WAF 等安全设备，实现对外部攻击流量的识别与阻断，其防护有效率可表示为：

$$R=1-\frac{A_s}{A_t} \tag{1}$$

其中，A_s 为成功攻击数；A_t 为总攻击尝试数。在网络层通过分区分域管理，将办公网、医疗业务网、设备网及互联网访问区进行逻辑隔离，降低横向渗透风险。主机层面部署终端安全管理系统，实现病毒查杀、补丁更新及系统加固，提升单点设备安全性。在应用层强化身份认证、访问控制和日志审计，确保业务操作可追溯。数据层采用数据库加密、数据脱敏及异地备份机制，提高数据抗风险能力。

4.2　建立数据全生命周期安全管理机制

医院应构建覆盖数据“采集—传输—存储—使用—共享—归档—销毁”的全生命周期安全管理体系，实现数据安全闭环管理。针对患者敏感数据，应实施分类分级保护策略，根据数据重要等级设置差异化访问权限与保护强度。在采集环节，规范数据源接入和采集权限，确保数据来源合法合规；在传输环节，采用加密通信协议，防止数据被窃取或篡改；在存储环节，核心数据库采用透明加密技术，并结合实时备份与异地灾备机制，提高数据可恢复能力，其数据完整性可表示为：

$$D=\frac{S+B}{S+L} \tag{2}$$

其中，S 为安全数据量；B 为备份数据量；L 为丢失数据量。在数据传输环节，采用加密通信协议，防止数据在传输过程中被窃取或篡改；在使用和共享环节，加强数据访问控制与审批机制，并通过日志审计实现全流程追溯；在数据归档和销毁环节，采用规范化脱敏及安全擦除技术，防止数据残留风险。

4.3　完善身份认证与访问控制机制

医院应建立统一身份认证平台，实现多业务系统的单点登录和集中管理，从源头解决多账号管理混乱问题。在核心业务系统中引入多因素认证机制（如密码+动态验证码+设备绑定），提高身份认证安全性，其认证强度可表示为：

$$I=\sum(w_i\times f_i) \tag{3}$$

其中，w_i 为认证因子权重；f_i 为认证通过因子。同时，医院应坚持最小权限原则，根据医生、护士、药师、行政人员及第三方运维人员的职责差异，进行精细化权限分配，避免权限过度集中。对于高敏感操作（如数据导出、系统配置修改等），应设置二次审批机制；远程运维方面，加强审批流程管理，对所有远程登录行为进行录像审计与日志记录，确保操作可追溯、可审计、可追责。

4.4　建立智能安全运营体系

医院应建设统一安全运营中心（SOC），整合防火墙、入侵检测、终端防护、数据库审计及漏洞扫描等安全数据，实现集中监控和统一分析。通过引入人工智能与大数据分析技术，对异常登录、异常流量及异常数据访问行为进行智能识别和预测：

$$P=\sigma\left(\sum w_i x_i+b\right) \tag{4}$$

其中，P 为威胁概率；x_i 为安全特征指标。在此基础上，构建安全事件分级响应机制，按照“监测—预警—处置—恢复—复盘”的闭环流程进行管理，实现安全事件全流程管控。同时，通过建立安全知识库与威胁情报共享机制，提高对新型攻击手段的识别能力。

4.5　强化网络安全管理与人员培训

医院网络安全管理不仅依赖技术体系，也需要制度与人员协同保障。首先，应建立完善的网络安全责任体系，明确医院管理层、信息部门、临床科室及第三方运维单位的职责边界，形成分级负责、协同联动的管理机制。其次，应定期开展网络安全教育培训，增强医务人员在密码管理、数据保护、邮件安全及终端使用规范等方面的安全意识，促进安全要求落实到日常操作。为衡量人员安全管理和培训效果，采用人员安全行为合规率作为评价指标：

$$C=\frac{C_a}{C_t} \tag{5}$$

其中，C_a 为合规行为次数；C_t 为总行为次数。最后，应结合医院实际开展网络攻防演练与应急演练，模拟勒索病毒攻击、数据泄露及系统中断等场景，检验应急预案的

有效性。

5 实践应用与效果分析

5.1 实践环境

为验证本文体系的实际应用效果，选取某三级专科医院作为实践对象。该医院编制床位约600张，信息化程度较高，已部署HIS、EMR、LIS、PACS、互联网医院、移动护理及医学检验等50余套核心业务系统，形成覆盖诊疗、管理和服务的综合信息平台。同时，医院终端设备规模较大，约1 200台各类计算机终端接入业务网络，另有约200余台医疗设备实现联网运行，网络环境复杂且业务依赖性强。在原有运行体系中，医院主要依赖防火墙及基础杀毒软件进行安全防护，存在明显短板，如网络边界防护能力单一、终端安全策略分散、日志数据缺乏集中分析能力等问题，导致整体安全态势感知能力不足。针对上述问题，医院进一步构建以网络分区、零信任访问控制、终端安全防护、数据库审计及SOC为核心的综合防护体系，并配套完善数据备份机制、漏洞管理流程、应急响应机制及人员安全培训体系，通过持续化安全治理不断提升整体网络安全防护水平与风险应对能力。

5.2 实施效果分析

在新建网络安全防护体系上线运行6个月后，医院对整体网络安全运行情况进行了系统性评估和数据统计分析。从结果来看，各项关键安全指标均得到明显改善。在漏洞管理方面，高危漏洞平均修复时间显著缩短，安全响应效率明显提升；在恶意攻击防护方面，病毒及木马感染事件数量大幅下降，系统整体稳定性得到增强；在访问控制方面，非法访问行为的拦截能力明显提高，有效降低了潜在入侵风险；在应急响应方面，安全事件平均处理时间显著缩短，整体处置流程更加高效；在数据安全方面，数据备份成功率提升至较高水平，进一步增强了系统容灾与恢复能力；在人员管理方面，医务人员网络安全培训覆盖率实现全面提升，安全意识明显增强。

6 结束语

随着智慧医院、互联网医院及人工智能医疗的快速发展，医院信息网络安全已成为保障医疗服务连续性、患者隐私安全和数据资产价值的重要基础。本文围绕医院信息网络安全面临的主要风险，分析了外部攻击、数据泄露、内部管理、医疗设备及云平台等方面存在的问题，并提出了涵盖网络架构、数据安全、身份认证、安全运营及人员管理的综合防护体系。实践结果表明，该体系能够有效提升医院网络安全防护能力与应急响应水平。

未来，医院应进一步融合零信任架构、人工智能安全分析、威胁情报共享及智能安全运营等新技术，持续完善网络安全治理体系，实现医院信息网络安全由被动防御向主动防护、由单点建设向体系化运营的转变，为智慧医院高质量发展提供更加坚实、安全、可靠的信息化保障。

参考文献：

[1] 贾志明.医院信息化进程中的网络安全防护策略研究与应用[C]//2025智慧设计与建造经验交流会论文集，2025：1-3.

[2] 孟亚，周志洪，李述胜，等.智慧医院零信任信息安全防护体系研究[C]//西湖论剑·网络安全大会论文集，2022：29-32.

[3] 汪兆来.线上线下一体化医疗服务模式下医院网络安全管理研究[J].中国医疗设备，2025，40(6)：93-99.

[4] 刘鹏，王璐，卫飞飞."互联网+"模式下的医院网络安全系统建设[C]//2017四川省卫生信息学会年会论文集，2017：249-252.

作者简介：

张雅雯(1998—)，本科，助理工程师，研究方向：医院信息网络安全。

(上接第179页)

及思考[J].法制博览，2015(4)：141-142+149.

[2] 刘峰.公路交通智能化建设发展趋势分析与探讨[J].工程建设与设计，2019(17)：52-54.

[3] 李焕贞.多模态传感器融合在智能视频监控中的应用[J].家庭影院技术，2023(20)：11-13.

[4] 尹乐贤.智能交通技术在交通安全管理中的应用[J].科技风，2017(15)：9-10.

作者简介：

吴霖(1994—)，本科，工程师，研究方向：科技创新管理、科技研发及成果转化。

龚林(1993—)，本科，助理工程师，研究方向：数字化建设、智慧交通建设及运营。