浅谈医院三级等保与网络安全设备的协同构建

张伟强

中国中元国际工程有限公司，北京 100089

DOI: 10.61369/ME.2024070026

摘　　要： 随着医疗行业与信息技术的深度融合，医院信息化程度不断提高。从电子病历系统、医院信息系统（HIS）到远程医疗、智慧医疗等应用的普及，大量医疗数据产生、存储和传输，如患者的个人信息、诊疗记录、药品信息等。但医院网络环境日趋复杂，面临诸多安全威胁，像黑客攻击、恶意软件入侵、数据泄露等。本文以某三甲医院信息机房及网络安全设备建设为例，探讨如何保障医院网络安全。

关 键 词： 信息机房建设；三级等保；网络安全

A Brief Discussion on the Collaborative Construction of the Third-level Information Security Protection for Hospitals and Network Security Devices

Zhang Weiqiang

China IPPR International Engineering Co., Ltd. Beijing 100089

Abstract: With the deep integration of the medical industry and information technology, the informatization level of hospitals has been continuously increasing. From the popularization of applications such as the electronic medical record system, the Hospital Information System (HIS), telemedicine, and smart healthcare, a large amount of medical data is generated, stored, and transmitted, including patients' personal information, diagnosis and treatment records, drug information, and so on. However, the network environment in hospitals is becoming increasingly complex, and it faces numerous security threats, such as hacker attacks, malicious software intrusions, and data breaches. Taking the construction of the information computer room and network security equipment of a certain Class-A tertiary hospital as an example, this paper explores how to ensure the network security of hospitals. eimer's disease-related pathological changes in the brain, thereby exacerbating cognitive impairment.

Keywords: construction of information computer room; third-level information security protection; network security

引言

随着 “健康中国 2030” 战略的推进与人工智能、物联网技术的深度应用，医疗行业正经历从传统诊疗模式向 “智慧医疗” 的跨越式变革。电子病历系统、医院信息系统（HIS）、医学影像信息系统（PACS）等核心业务系统的普及，以及远程手术、互联网医院等创新场景的落地，使医疗数据呈现爆发式增长 。医院之间的信息共享和业务协同也日益紧密，通过区域医疗信息平台，实现了患者信息的互联互通，促进了医疗资源的合理配置。然而，医疗行业信息化程度的提高也带来了网络安全挑战[1]。医院网络系统中存储着大量患者的个人信息、诊疗记录、健康档案等敏感数据，这些数据不仅关乎患者的隐私和权益，还涉及医疗服务的安全和质量。因此，加强医院网络安全建设，保障医疗信息系统的安全稳定运行，已成为医疗行业信息化发展的重要任务。网络安全等级保护制度作为我国网络安全领域的基本制度，为医院网络安全建设提供了重要的指导和规范。其中，三级等保是针对重要信息系统的安全保护标准，要求医院在技术和管理层面采取严格的安全措施，以确保信息系统的安全性和可靠性。本文从项目概况、等保概念、信息机房建设、网络系统设计及安全管理等方面来阐述。

一、项目概况

本项目为三级甲等综合医院，包括医疗综合楼、科研教学楼、感染楼、发热门诊等，规划总建筑面积约22万平方米，住院床位数1200床。信息机房位于科研教学楼，面积为320平方米，灾备机房位于医疗综合楼，面积为100平方米。本项目内、外网采用双核心双汇聚单接入的三层结构网络体系，网络传输采用万兆主干、千兆桌面的网络传输方式。医院的信息管理系统（HIS）、医学影像系统（PACS）、临床信息系统（CIS）、放射信息系统（RIS）等医院信息系统、各类资产管理系统、智慧医

疗、候诊呼叫信号系统、护理呼应信号系统等接入内网。

二、等保概述

达到三级保护级别的信息系统，需构建系统化的安全防护体系。该体系应依据统一的安全策略进行规划与部署，从而抵御来自外部专业攻击团队的恶意侵袭。这些攻击者往往具备充足的资源与技术能力，攻击手段更为复杂和隐蔽。同时，系统还须具备应对严重自然灾害等不可抗力因素的能力，以及防范其他同等级别危害的威胁。在安全监测与响应方面，三级保护对象需建立有效的安全监测机制，能够实时感知并识别各类攻击行为。一旦发生安全事件，系统应迅速启动应急响应流程，采取有效措施进行处置。此外，系统应具备完善的灾备与恢复机制，在遭受安全威胁导致系统受损后，能够快速恢复核心功能和大部分业务，将损失控制在最小范围内，保障信息系统的持续稳定运行。

三、机房建设要求

1.本项目机房设置在科研教学楼三层，避开强电场及强磁场（如变配电室）、强震动源（如空调机房）、强噪声源（如柴发机房）、易发生火灾、水灾等区域。

2.机房出入口设置人脸识别门禁系统，可以控制、鉴别和记录进出信息机房的人员。

3.机房门口处设置入侵报警系统。

4.机房内设置视频监控系统，视频监控主机及存储设备设置在信息机房值班室内。

5.机房设置火灾自动报警消防系统，对机房划分区域进行管理，区域和区域之间设置隔离防火措施；设置漏水检测仪器，对机房进行漏水检测和报警。

6.机房设置温湿度传感器及空调自控系统，使机房温湿度变化在设备运行的范围内。

7.本项目设置2套 UPS，提供30的备用电力供应，满足设备在市电断电情况下的正常运行要求。

四、网络安全设备设计

网络安全是医院三级等保的关键环节。应有详细网络拓扑图，清晰展示网络架构和设备连接关系，便于网络管理和故障排查。核心交换机、防火墙、路由器等网络设备的配置必须符合要求，进行 Vlan划分，有效防止网络风暴和非法访问；配置 QoS 流量控制方案，根据业务需求合理分配网络带宽，确保关键业务的网络性能 ；配备访问控制策略，对网络访问进行精细控制，只允许合法的访问流量通过，防止非法访问和攻击。重要网络设备和服务器应进行 IP/MAC 绑定，确保设备身份的唯一性和网络访问的安全性。配备网络审计设备，对网络活动进行全面记录和审计，以便及时发现和追溯安全事件；部署入侵检测或防御设备，实时监测网络流量，及时发现并阻止入侵行为。交换机与防火墙需建立严格的身份鉴别体系[3]。设备应采用强身份认证机制，设置具有唯一性的用户名，并要求配置复杂度高的密码，通过设置密码长度、大小写字母、数字与特殊字符组合等要求，提升密码破解难度。同时，为强化账户安全，需制定完善的登录访问失败处理策略，当出现多次无效登录尝试时，系统将自动触发账户锁定机制，暂停该账户的登录权限，并在锁定期间采取审计记录等措施，有效抵御暴力破解攻击，切实保障网络设备的访问安全。网络链路、核心网络设备和安全设备需要提供冗余性设计，当主链路或设备出现故障时，备用链路或设备能够自动切换，确保网络的连通性和可用性[4]。

服务器主机安全直接关系到医院信息系统的稳定运行。服务器的自身配置应符合严格要求，强化身份鉴别机制，采用多种身份验证方式；完善访问控制机制，根据用户角色和业务需求，对服务器资源进行细粒度的访问控制；建立安全审计机制，对服务器的操作进行全面审计，记录操作行为和事件，便于事后追溯和分析；安装防病毒软件，实时监控和查杀病毒，防止病毒感染服务器，确保系统安全。应用服务器和数据库服务器应配置多台使其具有冗余性，采用双机热备或集群部署等方式，提高服务器的可用性和可靠性，当一台服务器出现故障时，保证另一台服务器能够立即接管业务，确保系统不间断运行。在服务器与关键网络设备部署上线前，必须开展系统性的安全检测工作[5]。借助专业的漏洞扫描工具，对设备进行全维度的安全评估，重点排查 Windows 操作系统、数据库管理系统、各类系统软件及其开放端口存在的安全隐患。针对检测发现的中高级别漏洞，需建立严格的修复机制，确保在设备上线前完成漏洞修补，从而有效提升系统的安全防护水平，降低遭受外部攻击的可能性。此外，为强化安全事件的溯源与分析能力，应配置独立的日志管理服务器，对主机系统与数据库产生的审计日志进行集中存储与管理。通过规范化的日志收集与存储策略，确保日志数据的完整性与准确性，为后续的安全审计与事件分析提供可靠依据 ，便于统一管理和分析[6]。

应用安全关乎医院信息系统的业务功能正常实现和数据安全。应用自身的功能应符合等保要求，加强身份鉴别机制，确保用户身份的真实性和合法性；完善审计日志功能，记录应用操作的详细信息，便于审计和追溯；采用通信和存储加密技术，对重要的数据在传输和存储过程中进行加密，以防止数据被窃取和篡改。应用处应考虑部署网页防篡改设备，实时监测网页内容，防止网页被非法篡改，确保医院对外发布信息的真实性和完整性[7]。

在医院三级等保体系架构中，数据安全保障处于核心地位。为防范数据丢失风险，需构建完善的数据备份体系。一方面，建立本地数据备份机制，每日定时将关键业务数据同步至院内信息机房，确保数据在本地存储环境中的冗余性和可用性；另一方面，针对医疗核心数据，需进一步实施异地备份策略。通过加密传输通道与安全通信协议，将核心数据实时或定期传输至异地备份站点，形成跨地域的数据存储副本。这种双备份架构能够有效抵御自然灾害、硬件故障等极端情况对数据的毁灭性破坏，确保

在本地数据中心遭遇重大事故时，仍可凭借异地备份数据快速恢复业务系统运行，保障医疗服务的连续性与数据完整性[8]。

五、安全管理

在管理层面，安全管理制度是保障医院信息系统安全的重要环节。应制定全面、详细的安全管理制度，涵盖网络安全、数据安全、人员安全等各个方面。明确安全管理目标、职责分工、操作流程和应急处理机制等，确保安全管理工作有章可循。例如，制定数据访问权限管理制度，规定不同人员对患者数据的访问级别和权限，防止数据泄露；建立安全事件报告和处理制度，明确安全事件的报告流程和处理方法，确保安全事件能够得到及时有效地处理[9]。

医院应设立专门的安全管理机构，负责统筹协调医院信息系统的安全管理工作。明确机构内各岗位的职责和权限，确保安全管理工作的有效实施。例如，设置安全管理员岗位，负责日常的安全管理工作，如安全设备的配置和维护、安全事件的监测和处理等；设立安全审计员岗位，负责对安全管理工作进行审计和监督，确保安全管理制度的执行。

人员安全管理是防止内部安全风险的关键。加强对医院员工的安全意识培训，提高员工对网络安全的认识和重视程度，使其了解网络安全的重要性和相关法律法规。培训内容包括网络安全基础知识、安全操作规程、数据保护意识等，通过案例分析、模拟演练等方式，增强员工的安全意识和应急处理能力。建立人员访问权限管理制度，根据员工的工作职能和需求，分配最小化的访问权限，定期对员工的访问权限进行审查和更新，防止权限滥用和数据泄露。对涉及敏感信息的人员进行背景审查和定期考核，确保人员的可靠性和安全性[10]。

系统建设管理贯穿于医院信息系统建设的全过程。在系统规划阶段，应充分考虑网络安全因素，将安全需求纳入系统设计方案，确保系统在建设之初就具备良好的安全性能。在系统开发阶段，遵循安全开发规范，采用安全的开发技术和工具，对代码进行安全审查和漏洞检测，防止因开发过程中的安全漏洞导致系统安全风险。在系统验收阶段，严格按照等保标准进行验收，对系统的安全功能和性能进行全面测试，确保系统符合三级等保要求 。

系统运维管理是保障医院信息系统长期安全稳定运行的重要环节。建立系统运维管理制度，明确系统运维的流程和要求，包括系统的日常维护、故障处理、升级更新等。定期对系统进行安全检查和评估，及时发现并修复安全漏洞。建立系统应急响应机制，制定应急预案，定期进行应急演练，确保在发生安全事件时，能够迅速、有效地进行应急处理，降低安全事件的影响。对系统运维过程中的操作进行详细记录，便于追溯和审计。

六、总结

随着医疗信息化的加速推进与网络安全形势的深刻变革，医院网络安全呈现多维度发展趋势，同时也面临诸多挑战。云计算、大数据、人工智能、物联网等新兴技术在医疗领域的深度融合，使得医院网络安全环境日益复杂：云计算在实现系统弹性扩展的同时，带来数据云端存储安全与服务提供商信任风险；大数据应用丰富了医疗决策依据，但也加剧了患者数据泄漏风险；人工智能虽提升了诊疗效率，但其算法漏洞可能导致诊断失误；物联网实现医疗设备互联互通，却带来设备身份认证与数据传输安全隐患。为此，医院需强化新兴技术安全风险研究，创新安全防护技术与管理模式，需要持续关注网络安全态势，及时调整网络安全防护策略，以应对不断变化的安全威胁。

参考文献

[1] 中华人民共和国国家市场监督管理总局，中国国家标准化管理委员会 . GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求 [S]. 2019.

[2] 中华人民共和国国家市场监督管理总局，中国国家标准化管理委员会 . GB/T 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求 [S]. 2019.

[3] 刘建伟，王育民。网络安全：技术与实践（第 2 版）[M]. 北京：清华大学出版社，2011.

[4] 纪爱民. 计算机安全的思想与方法（第 3 版）[M]. 北京：电子工业出版社，2015.

[5] 中华人民共和国住房和城乡建设部. 智能建筑设计标准：GB 50314-2015 [S]. 北京：中国计划出版社，2015.

[6] 住房和城乡建设部. 火灾自动报警系统设计规范：GB 50116-2013 [S]. 北京：中国计划出版社，2013.

[7] 住房和城乡建设部. 消防设施通用规范：GB 55036-2022 [S]. 北京：中国建筑出版传媒有限公司，2022.

[8] 中华人民共和国住房和城乡建设部，国家市场监督管理总局。综合医院建筑设计标准：GB 51039-2014 [S]. 北京：中国计划出版社，2014.

[9] 中华人民共和国住房和城乡建设部 . 安全防范工程技术标准：GB 50348-2018 [S]. 北京：中国计划出版社，2018.

[10] 住房和城乡建设部，国家市场监督管理总局。建筑电气与智能化通用规范：GB 55024-2022 [S]. 北京：中国建筑出版传媒有限公司，2022.

