医院网络安全体系内信息系统管理技术实践探究

马 宁
黄石市公共卫生医疗救治中心 湖北 黄石 435000

摘 要：计算机信息系统管理技术构成网络安全防护的技术底座，覆盖身份认证、运维监控、数据保护与边界管控等多个层面。本文围绕访问控制与身份认证、系统运维监控与审计、数据保护与存储安全、网络边界与架构安全四个维度展开论述，剖析各模块的技术逻辑与管理要点。在此基础上，提出标准化运维、精细化管控与智能化升级等优化路径。

关键词：计算机信息系统管理技术；网络安全；访问控制；运维监控

引言：网络空间的攻击手段日趋复杂，单纯依赖单点防护已难以应对多维度的安全威胁。计算机信息系统管理技术将安全策略从"被动防御"转向"主动管控"，通过身份鉴别、行为审计、数据加密与架构隔离等手段，把安全要求嵌入系统运行的每一个环节。这些技术并非孤立存在，而是在访问控制、运维监控、数据管理与网络边界四个层面形成协同效应，为信息系统的持续安全运行提供了可操作的技术支撑。

1 访问控制与身份认证管理技术

1.1 用户身份标识与鉴别机制

用户身份标识是网络安全的逻辑起点，系统为每位访问者分配唯一编号，该编号在整个会话期间充当权限判定的锚点。鉴别机制在登录环节确认操作者与标识的归属关系，口令、生物特征与硬件令牌是三种主流手段[1]。单一口令因记忆负担轻而广泛采用，但泄露与暴力破解的风险始终存在，管理者在口令策略中引入长度与复杂度要求加以约束。生物特征鉴别凭借个体唯一性获得较高可信度，指纹与面部识别已在终端设备上大范围部署。

1.2 角色权限分配与管理

角色权限分配实现医护人员与系统操作权限的分离管理，管理员结合医院业务场景、岗位职能及信息安全等级，统一划分系统角色并为各角色匹配对应操作权限。普通医护人员仅具备诊疗数据查询、病历录入与业务提交权限；运维管理人员可开展系统参数调整、功能配置等操作；院内审计人员负责操作日志核查、统计报表导出等工作。随着岗位细分与人员变动，易出现角色权限交叉、范围重叠的问题，若各角色权限边界划分模糊，极易引发信息越权查看、违规操作等风险。医院需定期核对角色权限与实际岗位的适配情况，及时清理闲置冗余角色，降低院内数据安全隐患。所有权限调整操作必须履行院内审批流程，权限变更全程留痕、记录完整，满足医疗数据溯源与合规管理要求。

1.3 多因素认证集成策略

多因素认证将两种或以上不同类别的鉴别手段组合使用，显著提升身份验证的可靠程度。知识因子解决用户知道什么的问题，持有因子解决用户拥有什么的问题，固有因子解决用户是什么的问题，三种因子分别来自记忆、物理设备与人体特征。攻击者需要突破多个独立维度才能完成冒充，集成策略的关键在于因素组合的合理搭配。高安全场景要求三种因子全部参与验证，日常办公场景则可采用口令加动态令牌的双因素组合以平衡安全性与便捷度。认证触发条件可根据访问资源的敏感程度分级设定，敏感操作强制启用多因素认证，普通操作允许单一因子通过。

1.4 会话管理与会话隔离

会话管理对已通过认证的用户在系统内的活动进行持续跟踪与控制。每一次登录生成独立的会话标识，该标识关联着用户的权限集合与操作时间窗口。会话超时机制在用户长时间无操作后自动终止连接，防止未锁屏终端被他人利用。会话隔离要求不同用户或不同安全等级的操作在逻辑上相互独立，一个会话中的数据不会被另一个会话读取或篡改。并发会话数量的限制可防止单一账户被多处登录后产生权限叠加，异常地理位置或设备类型的会话接入会触发二次验证请求。

2 系统运维监控与审计管理技术

2.1 日志采集与集中管理

日志记录着医院信息系统的全量运行行为，人员登录、参数配置、数据访问、病历操作等行为均会生成日志。各类设备与业务系统日志分散存储，不利于医疗安全核查，需统一汇总至专用日志管理平台，按时间、设备、业务模块完成归档索引[2]。结合医疗行业规范区分日志类型，安全及诊疗相关日志设置更长留存周期，保障

事件溯源有据可依。同时对日志字段进行标准化规整，统一格式规范，保障检索功能正常使用，避免关键诊疗、操作信息缺失，全面支撑医院系统运维与医疗合规审计工作。

2.2 异常行为检测与告警

异常行为检测依赖于对用户操作序列与系统运行指标的持续分析，偏离正常基线的行为会被标记为可疑事件。检测引擎通过学习常规操作模式建立行为画像，当某一账户在非工作时间大量下载数据或频繁尝试越权操作时，引擎即刻生成告警并推送至运维人员终端。告警分级机制将事件按严重程度划分为不同等级，低级别告警进入队列等待人工确认，高级别告警则直接触发响应流程。误报率的控制是检测算法持续优化的方向，过多的无效告警会消耗运维精力并降低对真实威胁的敏感度。

2.3 运维操作审计追踪

运维操作审计追踪要求对所有管理行为进行全程记录，操作者身份、操作时间、操作对象与执行结果均被写入不可篡改的审计日志。审计追踪的价值在于事后还原操作链条，当系统出现配置异常或数据泄露时，审计记录能够快速定位责任人与操作路径。操作回放功能支持按时间顺序重现运维人员的每一步指令，为事故分析提供直观依据。审计日志的存储应独立于被审计系统，防止攻击者在入侵后清除审计痕迹。

2.4 配置基线管理与变更控制

配置基线管理为每一台设备与每一项服务设定标准配置模板，运维人员在部署或修复后需将实际配置与基线进行比对，偏差超过允许范围的配置会被自动标记。变更控制流程要求任何配置修改在执行前经过申请与审批，变更内容、执行人与执行时间被完整记录。回滚机制为变更失败提供了退路，当新配置导致服务异常时，运维人员可在短时间内将配置恢复至变更前的状态。基线的更新需跟随业务需求与安全标准的变化定期迭代，过时的基线模板反而会成为管理盲区。

2.5 补丁分发与漏洞修复流程管理

补丁分发流程从漏洞信息获取开始，经过风险评估与兼容性测试后进入分阶段推送环节。高危漏洞的补丁在测试通过后应在最短时间内覆盖全部受影响设备，中低危漏洞则可纳入常规维护窗口统一处理。分发过程中需监控每台设备的补丁安装状态，安装失败的设备会被自动列入重试队列。修复流程管理要求在补丁部署后进行验证扫描，确认漏洞已被有效封堵方可关闭工单，避免补丁安装不完整带来的二次暴露风险。

3 数据保护与存储安全管理技术

3.1 数据分级分类管理

数据分级分类是存储安全管理的起点，不同敏感程度的数据需要匹配不同的防护等级。分级依据数据泄露后可能造成的损失程度进行划分，从公开信息到内部资料再到高度机密数据，逐级递增的安全要求贯穿存储、访问与传输全过程[3]。分类维度则按照业务属性与数据类型进行区分，用户个人信息、财务记录与系统配置参数各归属于不同的管理类别。分级分类方案一旦确立，便成为后续加密策略、备份周期与访问权限设定的决策依据，数据管理员依据分类标签执行差异化的保护动作，避免对所有数据采用同一种防护力度带来的资源错配。

3.2 加密存储与密钥管理

加密存储将明文数据经过算法变换后写入存储介质，即便存储设备被物理获取，攻击者也无法直接读取数据内容。对称加密算法适用于大批量数据的快速加密，非对称加密算法则在密钥交换与数字签名场景中发挥作用，两种算法在实际部署中往往配合使用。密钥管理的复杂度不亚于加密算法本身，密钥的生成、分发、存储、轮换与销毁均需纳入统一管理流程。密钥与加密数据分开存放是基本要求，硬件安全模块为密钥提供了独立于操作系统的存储空间，降低了密钥被内存扫描或进程窃取的可能性。

3.3 数据备份与恢复调度

数据备份与恢复是医院医疗数据安全的重要保障。结合诊疗数据特性，采用全量、增量、差异三类备份模式，兼顾数据完整度、存储成本与备份效率。医院需定期开展数据恢复演练，检验备份文件可用性，避免突发故障时数据无法正常还原。为应对机房故障等风险，实行备份数据异地存储，主备站点间通过加密链路传输数据，严防患者诊疗信息、病历资料在传输中泄露、窃取。整套调度机制可有效抵御数据丢失风险，保障医院业务连续运转与医疗数据合规留存。

3.4 数据传输通道安全管理

数据在网络中流转时面临截获与篡改的双重威胁，传输通道的安全管理旨在为数据流动构建可信路径。传输层安全协议为端到端通信提供了加密隧道，数据在离开发送端前即被封装，到达接收端后才解密还原，中间节点无法获取明文内容。通道管理还涉及对传输路径的持续监控，异常路由跳转或非授权中间代理的出现会被视为潜在的中间人攻击信号。虚拟专用网络技术为跨公网的数据传输增加了一层隔离，内部数据在专用隧道中传输，与公网流量物理分离，有效降低了被嗅探的概率。

3.5 敏感数据访问控制策略

敏感数据的访问控制在身份认证与权限管理的基础上叠加了更为严格的约束条件。访问策略采用"默认拒绝"逻辑，未被明确授权的用户与应用均被排除在敏感数据之外。动态脱敏技术在数据展示环节对敏感字段进行部分遮蔽，运维人员在查看数据库记录时仅能看到经过处理的内容，完整数据只在经过额外审批后才可调取。访问行为被完整记录并纳入审计范围，对敏感数据的每一次读取、导出与修改都生成独立的审计条目，异常访问模式会被检测引擎捕获并触发告警。

4 网络边界与系统架构安全管理技术

4.1 防火墙策略配置与维护

防火墙部署在网络边界充当流量筛选的第一道闸门，策略配置的精细程度直接决定了网络防护的实际纵深。策略编写遵循最小化开放原则，仅允许业务所必需的端口与协议通过，默认拒绝所有未被明确许可的连接请求[4]。规则条目按照优先级从高到低排列，高优先级规则优先匹配，避免因规则顺序不当导致宽松策略覆盖了严格策略。策略维护是一项持续性工作，随着业务上线与下线，过时的规则若不及时清理，便会在防火墙中形成隐性通道。定期审计策略的命中率与冗余度，将长期无流量命中的规则标记为待删除项，可有效收缩攻击面。

4.2 网络分区与隔离管理

结合医院业务场景划分多个网络安全域，核心诊疗业务区、医疗数据存储区、办公网络区相互隔离。办公网络禁止直接访问数据库服务器，可有效避免终端异常引发的横向入侵，守护患者病历、诊疗数据安全。依托虚拟局域网、访问控制列表，在不同层级落实访问限制。各分区边界布设监测设备，对跨区域数据流量深度检测，一旦发现异常协议、非法端口访问行为立即拦截，全方位筑牢医院网络安全防线。

4.3 入侵检测与防御系统部署

入侵检测与防御系统承担着对网络流量与主机行为进行深度分析的任务，部署位置的选择决定了检测覆盖的广度。网络侧部署的探测器可捕获来自外部的扫描与攻击行为，主机侧部署的代理则关注内部异常操作与提权尝试。检测引擎依赖特征库与行为分析两种技术路线，特征库匹配已知攻击模式，行为分析则通过偏离正常基线的操作触发告警。防御模式在检测到攻击后可自动生成阻断规则，将恶意流量在到达目标前即被丢弃，缩短了从发现到处置的响应时间。

4.4 终端安全接入管理

终端安全接入管理要求所有接入网络的设备在获得访问权限前完成安全状态核查。设备接入时需提交身份凭证，接入控制系统验证身份后还会扫描终端的补丁版本、杀毒软件状态与系统配置合规性，不满足安全基线的设备被引导至修复区域而非直接接入生产网络。网络准入控制将合规终端与非合规终端隔离在不同的网络段中，非合规设备仅能访问补丁服务器与修复资源，待安全状态达标后方可迁入正常网络。接入日志完整记录每一台设备的入网时间、身份信息与安全状态，为事后追溯提供了可靠依据。

4.5 虚拟化环境安全隔离策略

虚拟化环境中多个虚拟机共享同一物理硬件，隔离策略的失效将导致一台虚拟机的安全事件波及整台宿主机。安全隔离从计算、存储与网络三个维度分别施加约束，计算隔离通过虚拟化管理层的权限控制防止虚拟机逃逸，存储隔离为每台虚拟机分配独立的虚拟磁盘空间，网络隔离则利用虚拟交换机将不同安全等级的虚拟机划分至独立的虚拟网络中。虚拟机之间的流量须经虚拟防火墙逐一检查，未经授权的跨虚拟机通信将被直接阻断[5]。

结束语

计算机信息系统管理技术在网络安全领域发挥着不可替代的支撑作用，访问控制构筑身份防线，运维监控提供持续感知能力，数据保护守住信息资产底线，边界管控则为系统架构划定安全范围。四个维度相互嵌套、协同运行，任何一个环节的缺失都会导致防护体系出现短板。将标准化流程、精细化管控与智能化手段融入日常管理实践，可有效提升网络安全的整体防护水平，为信息系统的稳定运行提供坚实保障。

参考文献

[1]宋宪余.计算机信息系统管理技术在网络安全中的应用[J].中国高新科技,2024(5):50-52.

[2]齐雪.浅谈计算机信息管理技术在网络安全中的应用[J].中国新通信,2023,25(1):91-93.

[3]付青燕.计算机信息管理技术与计算机网络安全应用[J].消费电子,2025(10):167-169.

[4]田华锋.加密技术在计算机信息系统中的应用研究[J].中国管理信息化,2023(2):175-177.

[5]胥林.信息系统的网络安全技术及实施方法分析[J].网络安全技术与应用,2023(10):26-27.