# 医院网络安全管理系统设计与防护机制构建研究

王晓华　叶瑞绵

武警黑龙江省总队医院信息科 黑龙江 哈尔滨 150076

【摘　要】：现代医院的发展态势多样，需要在常规参与公共卫生医疗服务的同时，加强自身建设，包括网络安全管理在内。本文以医院网络安全管理系统设计与防护机制构建要求为切入点，在此基础上分别就其设计方法、防护机制构建方法进行分析，包括总体设计框架、关键技术、不同技术的联动方法以及容灾模块建设等，为后续医院的网络安全管理工作提供参考，也服务其综合发展。

【关键词】：医院；网络安全管理；系统设计；防护机制构建

DOI:10.12417/2705-098X.26.08.077

## 前言

网络安全（Cyber Security）广义上是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受破坏、更改、泄露，系统可以连续可靠正常地运行。狭义上专指系统内的数据处于安全状态，本文取其狭义进行研究。就医院而言，其在日常工作中往往会产生海量信息，包括医院内部业务、财务、人事信息，也包括患者信息、药物信息，相关信息对医院管理和发展影响较大，需要保证信息安全[1]。同时《中华人民共和国网络安全法》、《网络数据安全管理条例》等文件的颁行，也要求各类组织重视网络安全管理。在此背景下，分析医院网络安全管理系统设计与防护机制构建方法，具有一定的现实意义。

## 1 医院网络安全管理系统设计与防护机制构建要求

### 1.1 全面性

医院网络安全管理系统设计与防护机制构建，首先应满足全面性要求。全面性是指该管理系统可以全面为医院各部门提供网络安全服务，也可以全面覆盖所有类别的保护对象，包括患者信息以及医院业务、财务信息等。从特点上看，当前医院面临的安全威胁多样，黑客攻击、病毒侵袭、恶意软件破坏以及网络灾害对医院各类信息、数据库的影响均带有相似性，可能无差别盗取数据、损坏数据库，故医院的网络安全管理系统应能够提供全面防护，应对已知风险和未知隐患。

### 1.2 实时性

实时性，是指医院网络安全管理系统设计与防护机制构建完成后，应能够实时为医院提供保护。与线下风险不同，网络层面的安全风险大多难以预知，可能因信息下载、终端新建链接，一瞬间实现破坏。如各类病毒，体积小、伪装性强，即便医院工作人员误操作、点击下载链接，病毒也可以在 1s 内快速侵入医院信息化工作系统内，直接盗窃信息或潜伏后造成长期破坏[2]。在组织网络安全管理系统设计与防护机制构建时，需要考虑该因素的影响，保持其实时作业能力。

### 1.3 开放性

从趋势上看，医院网络有关工作内容存在动态性，处于不断变化之中，如数据总量、处理方式、复用方法等，均在持续调整。同时，网络安全威胁也不是一成不变的，这意味着医院在组织网络安全管理系统设计与防护机制构建的过程中，也应考虑系统的开放性，使其拥有一定的可优化、可调整空间，以避免后续工作中可能出现的变化[3]。

### 1.4 鲁棒性

现代医院的工作内容多样，产生的网络信息也数目、类别也更多，任何环节出现问题，都可能波及医院信息化工作系统，这要求在保持系统全面、实时、开放的同时，通过技术性手段和管理性措施，使系统能够维持较高的工作稳定性。如系统在工作过程中出现突发事故、感染病毒或出现硬件大面积损坏情况，应能够通过维持数据安全，避免数据库崩溃、信息丢失等情况。此外，鲁棒性也关注系统设计的整体简明化，去除或减少非必要功能，减少建设和维护的复杂性，也削减系统出现 BUG、漏洞的几率[4]。

## 2 医院网络安全管理系统设计方法

### 2.1 总体框架

医院网络安全管理系统的总体框架设计，主要关注三个要素，一是关联主体，二是硬件系统，三是通信方式。

关联主体应包括三类，一是管理对象，即各类数据，二是服务者，包括医院内外需要使用网络信息的人员和组织，三是终端设备，即参与信息化工作，为信息化工作提供运作平台的设施。实际工作中，医院可根据自身情况进行上述三类主体的分析和选择，原则上应保证上述主体均可以通过实时化方式保持与医院管理中心的链接，能够实时接受服务、参与管理[5]。硬件系统主要关注性能优化，即便规模较小的县一级医院，需要处理的数据也较多、较复杂，故建议采用小型计算机群工作模式，设置 1 台主机+多台分机的机制，进行数据分析、挖掘、存储，计算机群建设可参考如下标准：

表 1 计算机群一般参考参数

| 设备 | 台数(台) | 虚拟内存(GB) | 显存(GB) | 存储空间(GB) |
|---|---|---|---|---|
| 主机 | 1~2 | 32 | 16 | 4096 |
| 分机 | 5~10 | 8~16 | 4~8 | 512 |

大型医院可以适当调整计算机群的建设参数，进一步优化其作业能力。通信方式方面，从稳定性角度出发，主张采用有线形式提升各主体的关联效果，为优化通信灵活性，则主张添加无线链接接口，确保各主体可以在办公室环境之外与网络安全管理系统保持关联。

### 2.2 关键技术

按照上文所述的设计要求，应在医院网络安全管理系统中采用以物联网、区块链为核心的工作技术，此外常规应用各类计算机技术、网络技术、通信技术等提供辅助。

物联网技术的应用，关注借助可扩展的实时通信系统，完成各类关联主体的实时化互动，其设计并不复杂，在当前技术支持下可以有序开展。然而考虑到医院的工作部门较多、信息资源较复杂，还应以区块链技术提供管理层面的支持。区块链模式下，医院可以根据信息管理的具体要求设置多个工作中心，独立完成数据管理，但接受物联网中心的集中控制。如医院的门诊部、住院部等，均可独立形成数据工作分中心，分中心只处理各自工作有关的数据，相互之间互通但不存在管理层面的隶属关系[6]。安全管理工作也各自独立根据实际情况开展，当医院内外各部门需要使用数据、查看资料时，可通过相互联通的网络发出请求，由对应部门响应，再根据管理规定提供或拒绝服务，避免信息安全问题。此模式下，区块链技术降低了医院集中处理信息的麻烦，分摊了工作压力，也能保证信息安全管理的独立性。

### 2.3 授权模式

从安全角度出发，应加强医院网络安全管理系统的授权管理，只允许获取授权的人员、组织访问有关物联网和区块链中心，以面向工作人员的授权为例。医院可收集目标人员（授权对象）的信息，并录入数据库，默认人员 A 的个人面部信息采集结果如下：

[24G；08；88H；QE；-9H]（人员 A 的个人面部标准信息）

相关信息采集完成后，将其输入计算机，并保持计算机与物联网的实时关联，人员 A 提出访问申请时，实时对其个人信息进行采集，通常实时信息与标准面部信息应是完全相同或高度相似的，在光线略有不同、A 表情存在变化时，其面部实时信息可能与标准信息稍有差异：

[24G；08；87H；QE；-9H]（人员 A 的个人面部实时信息）

由系统进行对比，人员 A 的个人面部实时信息与标准信息高度相似，认定为同一工作人员（A），可允许访问数据库，查看、调取数据或进行管理操作。授权机制可以直接提升医院网络安全管理系统的工作能力，避免非法人员闯入导致破坏。

## 3 医院网络安全管理系统防护机制构建方法

### 3.1 多技术联动

医院网络安全管理系统防护机制的构建，主要关注不同技术的联动，弥补单一技术防护能力不足、缺乏实时性和全面性的问题。按照上文所述设计方式和要求，主张采用智能防火墙、实时防护软件、节点防护并行的方式，为医院信息安全工作提供服务。

智能防火墙主要布置在医院内部以太网和公共网络之间，利用智能防火墙对各类外来数据包、程序等进行分析，当外来者身份合法且不存在安全风险时，予以放行；当外来者存在安全风险时，予以拦截或粉碎；当外来者身份可疑，但不确定是否存在安全威胁时，予以拦截、记录，提示工作人员进行处理。实时防护软件主要负责对计算机进行防护，当防火墙无法拦截、辨识部分危险因素，且该因素已经进入医院工作网络的情况下，由实时防护软件进行分析和清扫，避免其造成破坏。此外，实时防护软件也可以对计算机软件自带漏洞进行检索，主动完成上报和修复，减少内部软件功能异常导致的信息安全风险[7]。

节点防护模式主要面向计算机以及其他终端工作设备内数据库提供防护，与防火墙、实时软件防护不同，节点防护一般作为医院网络安全管理系统的最后防护手段，可以采用加密模式提供安全保障。如医院内财务数据库，记录了医院财务信息，在加密模式下，可以随机选取 1000 个以上参数并进行打乱，形成原始资源池。工作人员访问财务数据库时，资源池按照某一固定逻辑进行处理，形成由三个以上参数组成的随机密钥，要求访问者同时掌握原始资源池信息以及加密逻辑，才能完成访问，可以直接提升数据库信息安全性，与其他工作技术联动保证医院网络安全管理系统工作能力[8]。

### 3.2 重点防护

医院内的各类信息、数据类别多样，部分数据的价值较高，也有部分数据的价值偏低，如果采用统一的工作方法组织管理，可能导致低价值信息消耗、占用过多管理资源的情况。

未来医院可以根据当前内部管理情况、大数据资源等，对内部数据进行分类，根据其重要性分为三个类别，提供不同的管理服务：

形成时间少于 1 年，牵涉到医院财务、患者资料等关键内容的信息，作为第一类信息，均按照防火墙+防护软件+节点防护的标准组织安全管理；

形成时间 1~3 年，牵涉到医院管理、一般会议纪要有关的资源，作为第二类资源，在条件允许的情况下提供防火墙+防

护软件+节点防护，如果管理资源紧张，可不组织节点防护；

形成时间超过 3 年，与药物存量、工作人员招聘配置等有关的低价值数据作为第三类资源，在条件允许的情况下提供防火墙+防护软件+节点防护，如果管理资源紧张，可不组织节点防护实时软件防护。

所有数据均以 1 年为间隔进行一次归类调整，结合其重要性组织管理，有重点、有针对性的完成数据保护工作。

### 3.3 容灾模块建设

各类网络灾害的影响不可预知，且往往在短时间内造成巨大破坏，实际工作中，医院网络安全管理系统的防护机制构建也应考虑该问题，建设完善的容灾模块，该模块建设主要关注两个方面措施，一是自动备份，二是便携式备份。

各医院可以在常规组织智能防火墙、实时防护软件、节点防护并行防护的基础上，建设独立备份系统，该系统不强调功能复杂化，以存储容量较大的计算机为主。日常工作中，备份系统不启动、不参与工作，医院每个工作日的结束阶段，启动备份系统对当日生成的各类数据进行拷贝和迁移，完成备份后中断与工作系统的链接，重新进入待机状态。在此基础上，考虑到计算机系统即便不存在直接链接，仍可能在大范围网络灾害来临时遭受破坏，医院可以建设便携式备份机制，选取大容量便携式存储器，每周或每个月，对医院内的各类关键数据进行拷贝和迁移，即便常规工作系统和独立备份系统均因为网络灾难损害，医院仍可以利用便携式设备中的数据重建数据库。便携式设备除保证容量外，也要求选取专人进行设备的维护、保管，严格避免丢失和损坏等情况，同时定期进行设备检查和更新，必要时更换新设备。

## 4 结论

综上所述，医院网络安全管理系统设计与防护机制构建对其运营、管理作用突出，需要在实际工作中予以关注。从要求上看，该系统的设计、防护机制建设需要保证全面性、实时性、开放性和鲁棒性，以匹配实际工作需要。从设计上看，系统框架应简明易维护，以物联网技术为中心，实现各要素的实时关联。防护机制构建方面，主要关注不同技术的联动，并对部分重点环节进行分析，提供高质量的安全保障，最后还应借助备份机制提升容灾能力，全面改善医院网络安全管理工作水平。

## 参考文献：

[1] 陈明.基于自适应微隔离的互联网医院安全防护设计[J].数字通信世界,2025,(10):104-106.

[2] 孔维强.提高医院计算机网络安全管理工作有效性的方法探讨[J].中国宽带,2025,21(11):61-63.

[3] 魏杨杨.基于智慧医疗的医院网络安全管理系统设计[J].无线互联科技,2025,22(14):71-74.

[4] 金煜林.医院信息化建设中计算机网络安全管理及其维护探讨[J].信息与电脑,2025,37(12):75-77.

[5] 王斌,刘兴淮.网络信息安全背景下桌面管理系统在医院信息化运维终端安全管理中的应用——以 H 市 Y 医院为例[J].网络安全技术与应用,2025,(06):117-120.

[6] 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(06):93-99.

[7] 张黎,赵孙锋,潘娇,等.基于“互联网+”的军队医院网络安全管理研究[J].网络安全技术与应用,2024,(12):131-133.

[8] 彭如飞.5G 背景下智慧医院网络安全管理面临的挑战分析和对策研究[J].网络安全技术与应用,2024,(06):111-113.