任　格. 基于等级保护的医院信息安全防护策略[J]. 中华医学图书情报杂志, 2018, 27(3): 61-64.

DOI: 10.3969/j.issn.1671-3982.2018.03.012

·信息组织与信息服务·

基于等级保护的医院信息安全防护策略

任　格

[摘要] 医院信息系统等级保护是医院信息安全防护的重要手段。通过分析医院信息化的特点及安全防护的难点, 基于等级保护的建设需求, 从技术、管理、运维、持续发展 4 方面讨论了具体安全防护策略, 建设了符合等级保护要求的医院信息安全防护体系, 使医院信息安全防护能够满足“互联网+”医疗新模式的发展需求。

[关键词] 等级保护; 医院; 信息安全; 策略

[中图分类号] R197.323　　[文献标志码] A　　[文章编号] 1671-3982(2018)03-0061-04

Hierarchical protection-based hospital information protection strategies

REN Ge

(Affiliated Beijing Tongren Hospital of Capital Medical University, Beijing 100730, China)

[**Abstract**] Hierarchical protection of hospital information system is an important measure to protect the hospital information security. The specific strategies of hospital information security protection were discussed in aspects of its technologies, management, operation and maintenance, and sustainable development according to the requirements of hierarchical hospital information system protection by analyzing the characteristics of hospital information system and the difficulties of its security protection. A hospital information security protection system that accords with the hierarchical protection requirements was developed in order to meet the needs of "Internet+" new medical mode.

[**Key words**] Hierarchical protection; Hospital; Information security; Strategy

随着信息技术及各类诊疗技术的快速发展, 远程医疗、移动医疗、医疗大数据分析、人工智能等已成为“互联网+”医疗创新模式的主要发展方向。我国多地正处于新医改的积极探索期, 医联体、医共体、专科联盟等新的医疗组织形态都离不开互联网和信息化平台, 这无疑给医院信息安全防护带来了更大挑战。一方面, 一旦医院信息系统出现故障, 将直接影响医院正常诊疗业务的开展, 对社会秩序和公共利益造成损害; 另一方面, 医院信息系统中存储着大量患者诊疗数据, 一旦发生数据泄露, 后果不堪设想。因此加强医院信息安全防护体系建设尤显重要。信息安全等级保护是我国信息安全保障的基本制度、基本方法和基本策略。贯彻落实国家信息安全等级保护制度, 满足医院信息安全等级保护要求, 开展等级保护建设相关工作势在必行。

[作者单位] 首都医科大学附属北京同仁医院, 北京　100730

[作者简介] 任　格(1982-), 男, 北京市人, 硕士, 工程师, 研究方向为医院信息化。

1　医院等级保护的具体要求

信息安全等级保护制度是我国社会信息化进程中提高信息安全防护能力, 维护国家安全和社会稳定, 推进各项建设顺利发展的一项基本制度。2011 年, 原卫生部发布了《关于全面开展卫生行业信息安全等级保护工作的通知》(卫办综函〔2011〕1126 号)。针对医疗卫生行业的信息系统, 原卫生部办公厅于 2011 年下发了《卫生行业信息安全等级保护工作的指导意见》(卫发办〔2011〕85 号), 规定三级甲等医院的核心业务信息系统信息安全等级保护定级不低于第三级, 并且要求 2015 年 12 月 30 日前完成信息安全等级保护建设整改工作并通过等级测

评[1-4]。同时信息系统安全保护等级纳入三级综合医院评审标准实施细则,作为评审三甲医院重要评分点。按照自主定级原则,一般情况下,HIS 系统定为三级信息系统,即 LIS 系统、PACS 系统、电子病历系统,外网网站等定为二级信息系统,但各信息系统的业务关联性较强。因此,按照等同保护原则,医院内网核心业务系统总体应按三级系统进行等级保护建设。

2 医院信息化特点及信息安全防护难点

医院信息化有以下突出特点:系统的可靠性高,诊疗业务要求多数应用系统 7×24 小时不间断运行,无论计划或非计划情况,网络间断时间应小于 2 小时;信息集成度高,所有信息需要集中使用,通过系统整合实现数据的共享和复用;异构系统多,系统复杂度高,而且系统间接口复杂,涉及厂家多[5];系统存储资料价值较高,如医院诊疗数据、患者隐私数据等;系统数据可作为诉讼证据,具有法律效力;核心网络与外网物理隔离。

以综合三甲医院为例,依据等级保护对三级信息系统的具体要求,涉及技术要点共 136 个,管理要点共 154 个[6],主要包括物理安全、网络安全、主机安全、应用安全、数据安全、管理制度、管理机构、人员安全、建设管理、运维管理等方面的不同层次[4]。其信息安全防护的突出难点表现如下。

一是医院内、外网物理隔离导致信息安全防护需增加跨网络防护策略。

二是区域边界的安全访问控制策略复杂,主要包括边界访问控制、边界完整性检测、边界入侵防范以及边界安全审计等方面。访问控制是对各类边界最基本的安全需求,对进出安全区域边界的数据信息进行控制,阻止非授权及越权访问。若边界完整性受损,则所有边界访问控制规则将失去效力。

三是多级安全域边界厘定[7-8]。一般而言,安全域的划分需将相同安全等级、相同安全需求的系统划入同一 VLAN 内,在 VLAN 的逻辑边界增设安全设备设计控制策略。进行等级保护建设后,医院内网应在终端和服务器之间建立安全访问路径,并根据具体业务工作流和数据处理的重要程度划分不同的子网,重要网段与子网间增设技术隔离策略。但依此方法进行信息系统分级保护后,处于不同安全域的系统间无疑会产生隔离壁垒,进而形成数据孤岛,这与患者实际就医的瀑布型业务流不符。因此,在保持原有信息系统业务顺畅运行的前提下,进行信息安全等级保护成为亟待解决的问题[9]。

3 医院信息安全防护策略

针对上述医院信息系统特点及信息安全防护难点,依据等级保护具体要求,各医院需制定合理的信息安全防护策略,以完成等级保护建设目标。

3.1 技术策略

3.1.1 物理安全

物理安全主要指中心机房的物理场所安全。中心机房是医院信息系统的核心区域,需根据室内各类设备的运行参数严格控制物理环境,主要包括远离用水设备,双路供电,须具备防雷、防火、防水、防潮、防静电、防电磁干扰的能力[10]。同时必须设有门禁,控制不同管理层级的工程师进出,防止外来人员非法出入。

3.1.2 网络安全

网络通信是医院信息化的基础,因其端点分散、覆盖面广而成为等级保护建设的重点。一般而言,等级保护建设是基于现有网络进行的,基础设施如网络布线、机房位置等相对固定,在此基础上的等级保护主要考虑网络的合理性、高效性、高可用性。合理的网络拓扑结构能够大幅提升网络的效率和安全性,拓扑优化工作重点为逻辑安全域的划分,拓扑优化往往能让等级保护工作达到事半功倍的效果。此外,在划分不同安全域后除需增设边界网络安全设备并制定合理的网络安全访问策略外,还需要消除网络通讯单点、配备必要冗余、设计负载均衡,保证网络的高可用性。

3.1.3 系统安全

系统安全策略重点包括身份认证策略、访问控制策略和分布式授权策略 3 方面。关于身份认证策略,医院信息系统在应用“用户名/密码”进行身份认证时,还应将 PC 的 IP 地址、MAC 地址与交换机的通讯端口进行绑定,以限制接入医院的内网用户;关于访问控制策略,医院信息系统的用户复杂,各角色的访问控制策略不但要考虑角色规则,而且要考虑时间、空间访问规则,即访问控制能够详细描述“什么人,在什么时间,在什么地点,基于什么规则,

做了什么事”，最终设计出受时间、空间、规则三维约束的角色访问控制策略；关于分布式授权策略，设置树状权限管理机构对医院的信息资源进行分布式管理和统计，确定层级权限管理负责人节点，各分布式部门的责任人节点拥有下层节点的约束管理能力，每层负责人节点负责授权管理下层的权限策略，依次层级递推。

3.1.4　数据安全

数据是医院的核心资源和重要财富。数据安全等级保护建设要求医院应制定详细的备份策略，特别应建立健全高效的备份恢复机制，一般采用“近-远-离-异”与“热冷”结合的数据安全保障策略。近线备份采用实时备份，目的是实现数据的快速恢复；远线数据备份采用全备份加增量备份，形成基于时间节点的完整备份数据集；离线冷备份解决人为非逻辑错误的数据恢复；异地备份解决不可抗力的数据恢复。

3.1.5　应用安全

系统整合后的用户同步是等级保护在应用安全方面关注的主要问题。目前，进行系统整合并建立统一用户管理系统（UUMS）是解决该问题的通行做法。UUMS 采用建立专属用户数据库的方式统一存储全部应用系统的用户信息，应用系统通过 UUMS 管理用户并对用户授权，以此实现统一存储、分布授权。认证策略是指通过“与”“或”“非”的布尔逻辑组合实现的认证方式，最终定义为认证方式和认证规则。医院具体应用通常采用“用户名/密码 and IP 地址”认证的方式。

3.2　管理策略

医院信息系统的安全防护和安全管理是一个整体，在等级保护中都占有重要地位，不容忽视。就目前的医院信息系统等级保护现状而言，管理策略主要考虑强化信息安全意识[11]、加大安全管理投入和人员规范化培训 3 方面。

3.2.1　强化信息安全意识

信息安全意识是人们头脑中建立起来的“信息化工作必须安全”的观念，即人们在信息化工作中对各种有可能对信息本身或信息所处的介质造成损害的外在条件的一种戒备和警觉的心理状态。医院全体人员需不断强化信息安全防护意识，提升信息安全防护的敏感性，以防微杜渐。

3.2.2　加大安全管理投入

虽然目前医院信息化投入相较之前已有明显改善，但投入的大部分资金主要用于网络、系统维护和新项目的建设，对安全防护并未设立专项经费，即使有安全专项经费投入，因其投入效果没有新建项目收效明显而往往得不到重视。

3.2.3　人员规范化培训

医院信息安全等级保护是一项长期的系统工程，需要专门的人才队伍，但目前医院信息科人员对信息安全等级保护知之甚少。因此需要专门对相关工作人员进行培训，提高等级保护专业技能，从而提高医院信息安全整体水平。

3.3　运维策略

随着信息技术的不断发展，医院信息化程度不断提升，系统复杂性不断提高，传统的运维管理模式存在潜在的安全隐患。医院网络应用系统的健康运行需进行相应的事前管理以及透明化的运维动态监控，如安全事件的处置已从事中、事后的应对前移至事前的预警和预防，以提升医院整体系统的安全运维能力。

3.4　持续发展策略

持续推进医院安全体系建设是医院信息化发展的重要保障。只有从体系上发挥其作用，才能保证医院信息系统长期处于较高的安全水平和稳定的安全状态。这既能满足三级安全等级保护的具体要求，又能建立立体、纵深的医院安全保障防御体系。同时医院信息安全防护还需强调常态化，制定全面的规章制度，培育安全信息防护人才，为信息安全防护工作常态化提供支撑[9]。“互联网+医疗”使医疗行为不再局限于医院，移动医疗、网络医院等新型诊疗模式将随着政策和技术的落实逐渐常态化，同时要求信息安全防护新模式常态化。此外，在医院人才评价中往往只注重信息科人员的创新能力，而忽视系统的安全无事故运行，因此将系统安全运行纳入人员和科室的评优体系是落实信息安全制度的有效办法。

4　结语

在云计算、移动互联网、大数据、物联网、AI 等一系列新技术的驱动下，医疗行业正在经历一个快

速发展的时代[12]。一场“互联网+医疗”浪潮汹涌袭来,医院信息化建设的信息安全问题被摆到了信息化发展的重要位置,医院信息化面临新发展机遇的同时,其信息安全防护也面临新的挑战。信息安全等级保护建设可大幅提升医院信息系统安全水平,医院应通过建立制度、加大扶持、加强监管、培育人才等具体措施切实保障“互联网+医疗”新环境下的等级保护工作圆满完成。

【参考文献】

[1] 王 波. 基于等级保护的医院信息网络平台安全体系设计与实现[J]. 医学信息学杂志,2014,35(7): 30-32,45.

[2] 张益钊,朱卫国,孟晓阳,等. 医院信息系统等级保护测评实践[J]. 医学信息学杂志,2015,36(10): 14-18.

[3] 韩作为. 医院信息安全等级保护三级建设流程与要点[J]. 中国数字医学,2013,8(9):33-35.

[4] 邹陆曦,胡广禄,孙 玲. 三甲医院信息安全等级保护的实施及应用[J]. 中国数字医学,2015,10(2): 84-86.

[5] 辛均益,陈启岳,王宏宇. 关于医院重要信息系统信息安全等级保护工作的探讨[J]. 信息网络安全,2013(10):31-33.

[6] 蔡 颐. 三甲医院信息安全建设策略研究[J]. 海峡科学,2016(4):18-21.

[7] 曹利峰,陈性元,杜学绘,等. 多级安全网络区域边界访问控制模型研究[J]. 计算机工程与应用,2011,47(32):118-122.

[8] 王 俊. 基于等级保护的医院网络区域边界安全研究[J]. 中国数字医学,2013,8(3):96-98.

[9] 卢欣然,金 轶,徐 平,等. 浅论三级甲等医院信息安全等级保护管理体系建设[J]. 中国医疗器械信息,2014,20(6):55-58.

[10] 甄晓红. 三甲专科医院信息等级保护三级安全策略[C]//郑州:中华医学会第二十一次全国医学信息学术会议,2015:343-345.

[11] 徐冬兰. 医院网络中的安全风险与防范措施[J]. 网络安全技术与应用,2017(5):125,127.

[12] 朱圣才,徐 御,金铭彦,等. 基于等级保护策略的云计算安全风险评估[J]. 计算机安全,2013(5):39-42.

[收稿日期:2018-02-25]

[本文编辑:刘 娜]

(上接第 43 页)

[8] Shibata N, Kajikawa Y, Sakata I. Extracting the commercialization gap between science and technology: case study of a solar cell[J]. Technological Forecasting & Social Change, 2010, 77(7): 1147-1155.

[9] 黄鲁成,王静静,李 欣,等. 基于论文和专利的钙钛矿太阳能电池的技术机会分析[J]. 情报学报,2016,35(7):686-695.

[10] 亢川博,王 伟,张世玉,等. 国内外医学信息学研究现状的可视化分析[J]. 中华医学图书情报杂志,2016,25(8):24-30.

[11] 梅策香,柳 钰,曾利霞. 可穿戴设备在人体健康监测中的应用与发展现状[J]. 电子世界,2016(19):8-10.

[12] 石用伍. 可穿戴医疗设备的研究进展[J]. 医疗装备,2018,31(5):193-195.

[13] 迎 九,金 旺. 可穿戴设备中的传感器应用需求及趋势[J]. 电子产品世界,2017,24(6):21-24.

[14] 芮婷婷. 我国用户移动医疗服务使用意愿研究:以可穿戴设备为例[D]. 成都:西南交通大学,2016.

[收稿日期:2018-01-15]

[本文编辑:黄思敏]