基于三级等保标准的医院信息安全体系建设实践

魏 勤 刘艳亭 郭敬鹏 李功靖 孙 琳 刘 荻 冯国斌 张 振

（首都医科大学附属北京同仁医院 北京 100730）

王 青

（中国医学科学院医学信息研究所 北京 100020）

〔摘要〕 以首都医科大学附属北京同仁医院为例，介绍基于三级等保标准的医院信息安全体系建设项目实施过程，包括调研、制定方案和工作计划、实施、三级等保测评与项目验收，阐述项目技术亮点及下一步工作，指出该项目有助于提升医院整体信息安全管理水平。

〔关键词〕 信息安全；三级等保；医院

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2019.02.009

Practice of Building Hospital Information Security System on the Basis of Level－3 Rank Protection Standard *WEI Qin, LIU Yanting, GUO Jingpeng, LI Gongjing, SUN Lin, LIU Di, FENG Guobin, ZHANG Zhen, Beijing Tongren Hospital, Capital Medical University, Beijing 100730, China; WANG Qing, Institute of Medical Information, Chinese Academy of Medical Sciences, Beijing 100020, China*

〔**Abstract**〕 The paper, by taking Beijing Tongren Hospital, Capital Medical University as an example, introduces the project implementation process of building hospital information security system on the basis of level－3 rank protection standard, including investigation and survey, preparation of proposal and work schedule, implementation, measurement and project evaluation of level－3 rank protection. It also elaborates on technical highlights of the project and the next steps in the process, points out that the project can facilitate the improvement of overall information security management of the hospital.

〔**Keywords**〕 information security; level－3 rank protection; hospital

1 引言

信息系统及网络设施的安全性直接关系到医院医疗工作的正常运行，一旦网络瘫痪或数据丢失将会给医院带来巨大灾难和损失。医院信息系统涉及大量经营和患者医疗等私密信息，这类信息的泄露和传播将会给医院、社会和患者带来风险[1]。为此国家和行业主管部门相继发布相关法律法规，主要包括原卫生部办公厅《关于开展全国卫生行业信息安全等级保护工作的通知》（卫办综函［2011］1126 号），《卫生行业信息安全等级保护工作的指导意见》（卫办发［2011］85 号），原北京市卫生局《关于进一步加强北京市卫生行业信息安全等级保

〔收稿日期〕 2019－01－09

〔作者简介〕 魏勤，高级工程师，发表论文3 篇；通讯作者：王青，编审，发表论文40 余篇。

护工作的通知》（京卫办字［2012］26 号）以及2017 年6 月1 日开始实施的《中华人民共和国网络安全法》，2018 年6 月30 日公安部发布的《网络安全等级保护条例（征求意见稿）》等。近年来医疗行业信息化建设发展迅速，投入不断增加，基础设施水平提升明显，标准化建设意识提高，系统建设、信息互联互通水平及新技术应用都有很大的拓展[2]。

首都医科大学附属北京同仁医院是北京市属的一所三级甲等医院，分为东西南3 个院区。医院采用内外网逻辑隔离的网络架构，在机房面积、服务器台数、存储容量、终端数量等基础设施建设方面，以及信息化投入、应用系统覆盖面、互联互通水平等信息化建设方面都处于全国三甲医院的中等水平。目前将医院信息系统（Hospital Information System，HIS）定级为等保三级系统，检验信息系统（Laboratory Information System，LIS）、医学影像存储与传输系统（Pictures Archiving and Communication System，PACS）和门户网站定级为等保二级系统。近几年完成部分信息安全建设工作，取得一定成果，但面对日益严重的信息安全问题，亟需建立符合等保要求且相对完整、协调高效的信息安全管理体系。

2 基于三级等保标准的医院信息安全体系建设项目实施

2.1 概述

获批国家资金且完成测评、监理、集成、供货等公司的招标工作后，于2017 年12 月12 日正式启动项目。项目组制定明确的3 个层次的目标，即2018 年通过三级等保测评，合规、较好地完成项目验收，整体提升医院信息安全管理水平。

2.2 调研阶段

项目启动后的第1 项工作是测评公司做差异度分析，梳理出155 条整改内容，见表1。在物理、网络、主机、应用、数据安全等技术方面以及安全管理机构、安全管理制度、人员安全管理、系统建设管理、系统运维管理等管理方面与三级等保标准的要求存在较大差距。

表1 155 条整改建议危机值分布

评测分析分类	高危	中危	低危	总计
管理安全	10	25	35	70
安全管理机构	1	2	8	11
人员安全管理	2	2	5	9
系统建设管理	2	8	–	18
系统运维管理	5	13	–	32
数据安全及备份恢复	1	2	2	5
网络安全	9	7	4	20
物理安全	2	4	10	16
应用安全	2	12	5	19
主机安全	6	8	11	25
合计	30	58	67	155

2.3 制定方案和工作计划阶段

对照等级保护法规的相关要求，根据测评公司给出的整改建议，结合医院网络、系统和管理的实际情况，先后7 次组织相关人员召开方案讨论会，3 次外请专家论证。在充分研讨的基础上制定针对性强、务实可行的项目建设方案和详细的工作计划。项目建设方案总体架构，见图1。

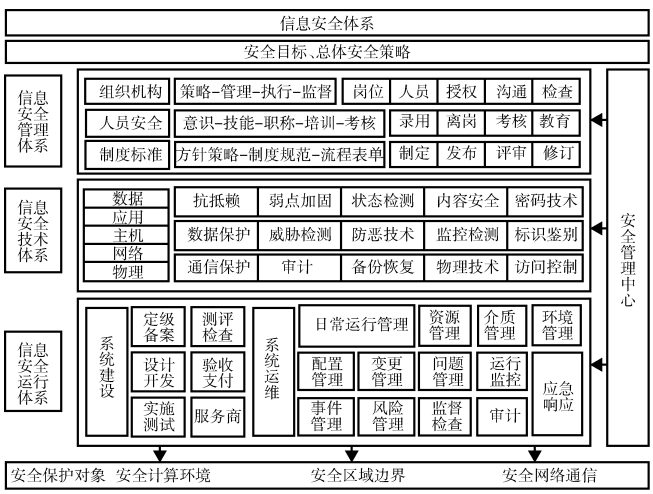

图1 项目建设方案总体架构

2.4 实施阶段

2.4.1 部署设备与系统 按照部署方案和工作计划进行 45 套安全设备和 907 台终端系统的安装调试，以及设备的配置与策略的部署。最终完成网络审计、防火墙、入侵检测系统（Intrusion Detection System，IDS）、应用防火墙（Web Application Firewall，WAF）、漏洞扫描、日志审计、防病毒软件等设备和系统的部署，以及集成与策略的优化。（1）服务器操作系统安全优化方面。实现安全加固软件和人工安全加固相结合，关闭无用的服务，进行漏洞扫描、身份认证、安全审计、访问控制、资源控制、备份等。（2）数据库系统安全优化方面。通过人工加固方式将操作系统和数据库帐号分开管理，采用最小授权原则、制定口令策略、数据库审计、对权限较敏感的存储过程加密管理，对远程数据库调用进行地址限制、备份等。（3）应用系统安全优化方面。定期进行漏洞扫描，实施应用系统安全加固，加强身份认证机制及用户权限和访问控制，应用安全审计，通信安全加密传输，加强资源控制，部署 Web 防火墙实现应用安全防护。（4）数据备份及恢复方面。定期进行数据备份，编制灾难恢复计划，开展灾难演练。（5）防病毒、终端管理、日志审计方面。部署杀毒软件实现主机层面病毒防御，终端安全管理系统实现终端安全检测，安管监控平台进行整体化系统化的监管。在这个阶段，调整机房设备，完成部分设备的腾挪搬迁；3 区 HIS 统一后将南区停用的设备下架，为解决旧系统的退卡退费问题专门研发程序；针对物理环境和应用系统需要整改的问题，院领导批准追加相应经费；HIS 供应商配合完成应用系统的改造；漏水与入侵监测、门禁系统等工作也得到了相关单位的全力配合。

2.4.2 梳理规章制度及文档 信息安全建设必须坚持“技术与管理并重，三分技术 + 七分管理”的原则[3]。三级等保标准要求建立信息安全管理组织机构，制定明确的安全策略、管理制度和工作流程。为此制定和修订 25 项管理制度，建立制度的审核与修订机制；与关键岗位、合作公司的相关人员签订保密协议，明确相应的责任和具体保密内容；信息系统操作权限实行分级管理，采用身份鉴别机制对用户访问权限进行控制；通过在中层干部会的宣教以及在内网上组织全院职工答题等多种方式在全院范围做好信息安全教育和培训工作，在院内网上答题的员工多达 2 600 余人。制度与文档建设情况，见图 2。

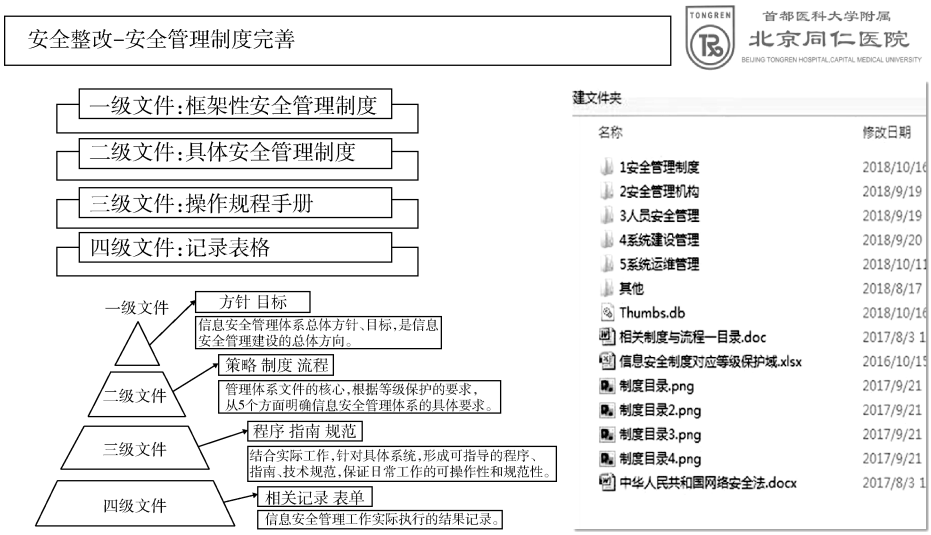

图 2 制度与文档建设

2.5 三级等保测评与项目验收

2018 年 10 月 15 日专业测评公司连续 5 天在医院开展现场测评，等保测评通过后于 2018 年 10 月底召开验收准备会，外请 5 位专家做技术把关。2018 年 11 月在监理公司监督下组织院外专家分别进

行项目的初验和终验，顺利通过项目验收。2018 年 12 月通过国家财政资金使用情况的财务审计专项检查。项目整个过程由监理公司全程监理，共召开项目例会 27 次，每周完成工作周报。项目文档齐全，包括市公安局定级备案表、预测评报告（差异度分析报告）、招标合同、中标通知、需求调研报告、设计方案、施工图纸、实施方案、设备安装调试报告、测试报告、试运行报告、总结报告、制度文档（电子版）、测评公司出具的信息系统安全等级测评报告、项目初验和终验专家意见、监理文档集等。

3 技术亮点

3.1 发现网络综合威胁

目前安全建设的难点是以往信息化建设与安全相对独立，重硬件轻软件，重网络轻数据。信息安全建设缺乏统一规划，管理和安全运维分割，没有完整和统一的平台。为此部署网络综合威胁发现平台及运维管理平台有助于信息安全整体的综合研判。

3.2 提升医院对威胁预测能力

引入威胁情报和高级持续性威胁（Advanced Persistent Threat，APT）发现手段来进行安全建设和全面布防，以威胁情报与实际网络中信息分析对比，打通攻击定位、溯源与阻断多个工作环节，从源头上解决安全问题。从安全整体架构设计时就兼顾检测发现、响应、预测与处置的防御过程，建立以检测发现为起始、形成闭环的协同防御安全体系。

3.3 建立网络威胁感知平台

通过快速搜索技术提升数据查找能力；基于大数据挖掘分析的恶意代码智能检测技术提升检测恶意代码的能力；基于轻量级沙箱的未知漏洞攻击检测技术提升检测未知漏洞的能力。同时为高效处理信息安全问题，提高运维能力，将核心关键设备进行联动处置优化，将部署在不同位置的关键设备日志信息统一发送到感知平台，进行综合安全分析。

3.4 生物识别双因素认证

在系统登录认证环节引入生物识别技术。通过动态的授权和生物识别实现人、权限、系统的统一。使用者可利用手机添加指纹或人脸识别等方式获得自身登录权限，做到动态授权管理和单点登录，保障业务系统的安全访问。

3.5 业务行为安全网关及监测方案

安全行为、内部操作安全也是信息安全管理重要的组成部分，需要对正常的安全行为进行建模，对安全模型之外的风险操作进行分析处置。如异常异地登录、非常规时间访问、超频工作、权限跨越等。为此引入业务行为安全网关，通过策略制定和建模全面分析医疗安全以及内部操作风险。在此基础上在行为监测平台上进行综合监测，将威胁情报、行为管理、网络综合感知平台、终端安全等相关信息进行关联、定位和确认。这项尝试真正地将人、技术、管理结合为一体，也使整个方案体现出协同联动和统一处置的建设思想。

4 下一步工作

4.1 挖掘设备使用的潜能

进一步发挥已安装部署设备的作用。如数据库审计，不能只用于防统方的管理和基础的监控，还需要不断地丰富和完善数据库监控内容和策略，使其发挥更大的作用。

4.2 加强技术培训和人才培养

在项目实施过程中集成、供货、设备厂商等合作单位承担很多工作。接下来将对信息中心人员进行分工和深度培训，这样网络、服务器、安管监控平台、终端等各领域的相关技术工作都有专人负责协调，提高运维水平和效率，信息中心人员也有未来技术提高的空间。

4.3 完善和落实各项规章制度

规章制度建设是信息安全管理重要的组成部

分，需建立长效机制并不断地增补和修订。而最关键的是将已建立的规章制度落实到实际工作中。计划按照信息技术基础构架库（Information Technology Infrastructure Library，ITIL）的理念和方法，部署信息中心运维管理系统作为相关管理制度落实的工具。通过制度建立、工作落实、检查修订、总结提升这样常态化的循环工作机制不断提升管理效率和水平。

5 结语

在为期10 个月的项目建设过程中体会最深的有两点：一是必须重视项目管理。需在综合分析和整体设计的基础上确定明确的项目和范围，细化项目的成本、变更、时间管理，严格把控项目的风险和质量。二是应特别重视相关方的合作与协同。该项目涉及16 个院内外单位，通过项目例会来建立和固化项目各方的沟通机制，共同讨论工作计划、遇到的问题及解决方案，增强相互之间的理解与协同，提高工作效率。在团队的共同努力下，项目通过三级等保测评，完成项目验收，实现医院信息安全管理整体的提升。

参考文献

1 王晖. 医疗卫生行业信息安全等级保护实施指南［M］. 石家庄：河北出版传媒集团，2014.

2 王才有，汤学军，董方杰，等. 全国三级医院信息化情况调查研究［J］. 中国卫生信息管理杂志，2016，13（4）：342－347.

3 唐江波. 基于医院信息安全等级保护的整改实践［J］. 中国数字医学，2018，13（11）：83－86.

4 汤斌，黄玉成. 三级等保下医院信息系统安全优化方案实践［J］. 中国医疗设备，2018，33（9）：136－140.

（上接第6 页）

12 Mechael P N. The Case for MHealth in Developing Countries［J］. Innovations，2009，4（1）：103－118.

13 Ivatury G，Moore J，Bloch A. A Doctor in Your Pocket：health hotlines in developing countries［J］. Innovations，2009，4（1）：119－153.

14 Ćubić I，Markota I，Benc I. Application of Session Initiation Protocol in Mobile Health Systems［C］. Opatija，Croatia：2010 Proceedings of the 33rd International Convention，IEEE，2010：367－371.

15 Chatterjee S，Chakraborty S，Sarker S，et al. Examining the Success Factors for Mobile Work in Healthcare：a deductive study［J］. Decision Support Systems，2009，46（3）：620－633.

16 Kahn J G，Yang J S，Kahn J S. "Mobile" Health Needs and Opportunities in Developing Countries［J］. Health Affairs，2010，29（2）：252－258.

17 Qiang C Z，Yamamichi M，Hausman V，et al. Mobile Applications for the Health Sector［M］. Washington：World Bank，2011.

18 Akter S，D'Ambra J，Ray P，et al. Modelling the Impact of mHealth Service Quality on Satisfaction，Continuance and Quality of Life［J］. Behaviour & Information Technology，2013，32（12）：1225－1241.

19 Ramanathan N，Swendeman D，Comulada W S，et al. Identifying Preferences for Mobile Health Applications for Self－monitoring and Self－management：focus group findings from HIV－positive persons and young mothers［J］. International Journal of Medical Informatics，2013，82（4）：e38－e46.

20 Hamine S，Gerth－Guyette E，Faulx D，et al. Impact of mHealth Chronic Disease Management on Treatment Adherence and Patient Outcomes：a systematic review［J］. Journal of Medical Internet Research，2015，17（2）：e52，1－15.