医院信息系统等级保护测评实践

张益钊

（1 北京协和医院信息管理处 北京 100044
2 北京建筑大学经管学院 北京 100730）

朱卫国 孟晓阳

（北京协和医院信息管理处 北京 100044）

邱志刚 苏 博

（石化盈科信息技术有限责任公司 北京 100007）

宋 昭 王翔宇

（北京市电子产品质量检测中心 北京 100005）

〔摘要〕 从北京协和医院信息系统开展等级保护测评的实际出发，介绍信息系统定级情况以及测评的内容和流程，论述在具体工作中发现的普遍问题与风险分析办法，为信息安全相关工作提供借鉴。

〔关键词〕 等级保护；医院信息系统；测评
〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2015.10.003

Practice of Grade Protection Assessment on the Hospital Information System

ZHANG Yi－zhao, 1 Peking Union Medical College Hospital, Beijing100730, China, 2 School of Economics and Management, Beijing University of Civil Engineering and Architecture, Beijing100044, China; ZHU Wei－guo, MENG Xiao－yang, Peking Union Medical College Hospital, Beijing100730, China; QIU Zhi－gang, SU Bo, Petro－Cyberworks Information Technology Co. Ltd, Beijing100007, China; SONG Zhao, WANG Xiang－yu, Beijing Electronics Standard & Estimate Research Institute, Beijing100005, China

〔**Abstract**〕 Starting from the practices of grade protection assessment on the information system of Peking Union Medical College Hospital, the paper introduces the information system grade and assessment contents and processes, discusses common problems found in specific work and risk analysis approaches so as to provide a reference for work related to information security.

〔**Keywords**〕 Grade protection; Hospital information systems; Assessment

1 引言

我国的信息安全等级保护工作已经经过了 20 余年的探索和发展。1994 年，国务院颁布 147 号令——《中华人民共和国计算机信息系统安全保护条例》[1]，规定“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”。该条例明确了 3 个内容：一是确立等级保护是计算机信息系统安全保护的一项制度；二是出台配套的规章和技术标准；三是明确公安部的牵头地位。147 号令的颁布，标志着我国的信息安全等级保护工作正式拉开了序

〔修回日期〕 2015－10－20
〔作者简介〕 张益钊，网络工程师，北京建筑大学经管学院在读硕士研究生，发表论文 3 篇；通讯作者：朱卫国，常务副处长。

幕。2003 年 9 月 7 日，中共中央办公厅、国务院办公厅联合颁布《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发【2003】27 号）[2]，明确指出“实行信息安全等级保护”，这标志着等级保护已从计算机信息系统安全保护的一项制度提升到了国家信息安全保障一项基本制度。

2011 年 11 月 29 日，原卫生部办公厅颁布《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）[3]，提出了卫生行业要“做好信息安全等级保护工作”，并且明确了工作要求和工作原则，下达了定级备案、建设与整改、等级测评、宣传培训、监督检查 5 个阶段的工作任务，为卫生行业贯彻落实国家信息安全等级保护制度提供了指导意见。

2011 年 12 月 7 日，原卫生部办公厅颁布《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）[4]，规定了各阶段工作任务的时间节点，要求“卫生行业各单位要于 2012 年 5 月 30 日前完成本单位信息系统的定级备案工作”，并且“要于 2015 年 12 月 30 日前完成信息安全等级保护建设整改工作，通过等级测评。”

2012 年北京市卫生局发布《关于进一步加强北京市卫生行业信息安全等级保护工作的通知》（京卫办字【2012】26 号）[5]，复述了推进等级保护工作的具体内容要求，如工作目标、工作原则、工作机制、工作任务、工作要求等，提出了对于北京市卫生行业推进信息安全等级保护工作的时间细节要求，如 2015 年 10 月 30 日前完成测评工作。目前，北京市卫生行业各单位均在大力发展信息化建设，信息安全保障的需求也日益迫切，依据原卫生部和北京市卫生局发布的各项工作指导意见和通知，各单位在逐步完成各项工作任务。

依据原卫生部办公厅（卫办发【2011】85 号）颁布的《卫生行业信息安全等级保护工作的指导意见》，北京协和医院也对院内信息系统进行了统一梳理与归并，确定医院主要应用系统“医院门诊住院信息系统”为信息安全等级保护第 3 级系统，其他如“影像存储与传输系统”等辅助系统为第 2 级系统。本文主要从北京协和医院信息系统开展等级保护测评的实际工作出发，介绍信息系统定级情况以及测评的内容和流程，论述在具体工作中发现的普遍问题与风险分析办法，在各医院普遍开展等级保护工作的大背景下，为信息安全相关工作提供借鉴[6-8]。

2 信息系统定级情况以及测评内容和流程

2.1 内容

在定级过程中，北京协和医院组织各方专家充分调研了系统现状，依据系统现状填写《信息系统安全等级保护备案表》，撰写《信息系统安全等级保护定级报告》，充分论证了系统的安全需求，确定了系统信息安全保护等级；依据指导意见的要求，如期完成了主要系统定级备案的工作，取得了《信息系统安全等级保护备案证明》[9-11]。同时，为配合国家等级保护政策的推进，符合国家等级保护的相关标准要求，北京协和医院进一步提高了信息系统的信息安全保障能力和防护水平，委托北京市推荐的测评机构——北京市电子产品质量检测中心（京字 008 号）进行等级保护测评，对医院门诊住院信息系统的安全状态做出判断，给出目标系统在安全技术和安全管理方面与相应安全等级保护基本要求之间的差距。测评结论作为院方进一步完善系统安全保护措施的依据。

2.2 流程

2015 年 4 月 2 日召开项目启动会，等级测评工作正式开始。2015 年 4－5 月对医院门诊住院信息系统进行了现场安全管理核查和安全技术测评、物理安全测评、安全管理测评。根据现场测评结果提出了差距分析和整改建议，于 2015 年 7－8 月对整改结果进行了复测，2015 年 9 月根据复测结果进行了单元测评结果汇总和整体测评分析，对不符合项进行了风险分析，得出测评结论，最终形成测评报告，确保依据北京市卫生局要求，在 2015 年 10 月 30 日前完成测评工作[12]。本次测评流程，见图 1。

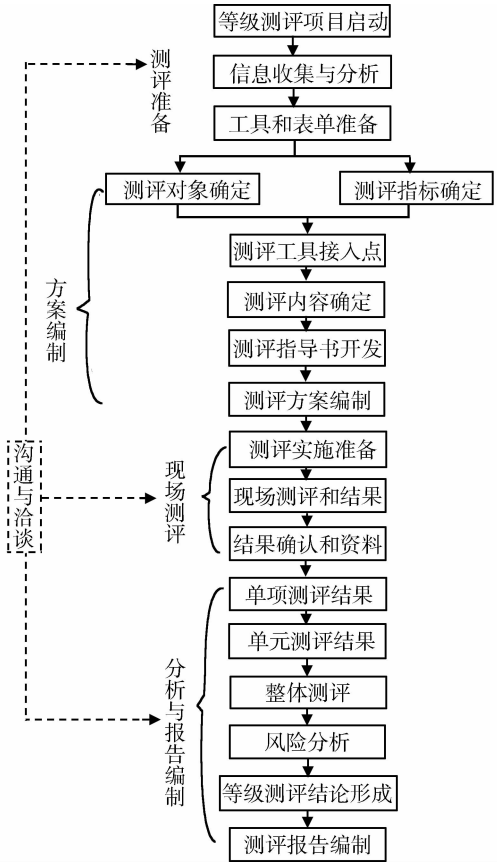

图 1 等级测评基本工作流程

3 测评结果分析

3.1 网络安全层面

3.1.1 *访问控制* 访问控制（G3）中要求：“应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级”。一般信息系统，如医院信息系统、门诊系统或住院系统等均可以通过防火墙，设置为限制从系统外部访问内部的 IP 地址，但未达到端口级，在网络内部并未进行访问限制，应该对防火墙进行细化配置予以整改弥补，如限于现实情况不能立刻整改的，可通过对现行规则进行梳理，确保所有访问来源可信，提出后续整改计划，于一定期限内进行整改。

3.1.2 *过滤信息内容* 访问控制（G3）中要求：“应对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制”。如果自查时发现所属的信息系统，如医院信息系统、门诊系统或住院系统等达不到该项要求，可采用防火墙进行细化配置予以整改弥补，如无该类设备的，可通过内网部署入侵检测设备进行部分弥补，降低风险。

3.1.3 *保护审计记录* 在安全审计（G3）要求中明确提出：“应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等，保存时间不少于半年”。一般而言多数信息系统，如医院信息系统、影像存储与传输系统等可能达不到该项保存时间要求，未部署网络设备的日志审计系统，安全审计纪录缺失，可采用对网络设备的审计日志（Syslog）外发的方式对审计纪录进行保护，予以整改弥补。

3.1.4 *边界完整性检查* 边界完整性检查（S3）中要求：“应能够对内部网络用户私自联到外部网络的行为进行检查，准确定位并对其进行有效阻断”。一般而言大多数信息系统达不到该项要求，可采用网络交换设备进行设置的方式，予以整改弥补。

3.1.5 *恶意代码防范* 恶意代码防范（G3）中要求：“应在与外单位和互联网连接的网络边界处对恶意代码进行检测和清除”。部分信息系统达不到该项要求，可采用具备恶意代码查杀清除功能的网络安全设备，予以整改弥补。

3.1.6 *管理员登录地址限制* 网络设备防护（G3）中要求：“应对网络设备的管理员登录地址进行限制”。一般医院类机构并未对管理员登录地址进行限制，可采用对网络设备进行设置的方式，予以整改弥补，对不具备该项设置的网络设备，可通过具备访问控制功能的设备如防火墙等进行设置。

3.1.7 *身份鉴别* 网络设备防护（G3）中要求：“主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别”。医院信息系统、影像存储与传输系统等在上线初期达不到该项要求，在传统的用户名/口令方式之外还可采用网络设备支持的如数字证书等身份鉴别方式对网络设备进行设置，予以整改弥补，对不具备该项设置的网络设备，建议对可登录网络设备的终端设备进行加强认证，如限定登录范围或采用安全计算机等，确保所有访问来源可信。

3.2 主机安全层面

3.2.1 启用登录失败处理功能 身份鉴别（S3）中要求："应启用登录失败处理功能，可采取结束会话、限制登录间隔、限制非法登录次数和自动退出等措施"。医疗机构的主机大多为默认配置，不能达到该项要求，应对会话内主机登录次数进行配置，防止非法猜解密码等攻击行为。

3.2.2 组合的鉴别技术 身份鉴别（S3）中还要求："宜采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别，如以密钥证书、动态口令卡、生物特征等作为身份鉴别信息"。大部分医院信息部门已有的现代化支付系统前置主机仅采用用户名/口令一种鉴别方式，不能达到该项要求，在传统的用户名/口令方式之外还可采用主机操作系统支持的如数字证书等身份鉴别方式对主机进行设置，予以整改弥补，还可对可登录主机的终端设备加强认证，如限定登录范围或采用安全计算机等，确保所有访问来源可信。

3.2.3 操作系统和数据库系统权限分离 访问控制（S3）中要求："应实现操作系统和数据库系统特权用户的权限分离"。部分卫生行业单位主机管理员同时兼管数据库，或有名义上的 A、B 岗设置，现实中主机与数据库的管理权限并未分离，对于人员条件许可的，应将该权限真正分离，因卫生行业单位内部人员管理措施与管理制度等较为完善，所存在的风险较低。

3.2.4 安全审计内容保护 安全审计（G3）中要求："审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用、账号的分配、创建与变更、审计策略的调整、审计系统功能的关闭与启动等系统内重要的安全相关事件"。主机大多为默认配置，不能达到该项要求，较多卫生行业单位未部署主机的日志审计系统，安全审计纪录缺失，可采用对主机的审计日志外发的方式对审计纪录进行保护，予以整改弥补。

3.2.5 病毒监控中心 恶意代码防范（G3）中要求："应建立病毒监控中心，对网络内计算机感染病毒的情况进行监控"。一般情况下医院信息部门因人员和资源有限未建立病毒监控中心，不能对网络内计算机感染病毒的情况进行监控，应采用提供该机制的防病毒设施，予以整改弥补。

3.3 应用安全层面

身份鉴别（S3）中要求："应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用"，还要求"应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，根据安全策略配置相关参数"。在上线的应用中没有用户鉴别信息复杂度检查功能，仅仅采用不超过 6 位数字的口令进行身份鉴别，部分卫生行业单位部署的新终端通过智能卡、数字证书关联使用者身份的鉴别措施予以弥补，因卫生行业单位内部监控措施与管理制度等也较为完善，所存在的风险较低。

4 安全管理测评结果分析及风险控制

4.1 安全管理测评结果分析

安全管理制度体系在信息安全保障工作中也是相当重要的，借助本次等级保护测评工作，北京协和医院对安全管理制度体系也进行了一次梳理。从测评的结果来看，在安全管理制度方面还是较为完善的，建立了由安全管理总体策略、安全管理分项制度到安全管理工作实施记录表格构成的多层次的体系结构，并且由专门人员进行制度的管理、记录的收集与存档，确保安全管理工作的开展有制度约束和规范，并且能够进行记录和回顾[13]。通过等级保护测评，对于安全管理制度体系的建设有了更系统的认识，从安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理 5 大方面对管理制度进行了梳理与改善，对于应急预案的定期培训与演练等方面的工作都有了更高的重视程度，在之后安全管理工作的执行过程中，进行不断审视和完善。

4.2 测评过程中的风险控制

经过测评发现的安全问题，对于医院来说都是

需要做好保密工作的，一旦问题被泄露，则会给医院信息系统带来不可估量的安全风险，因此，在测评过程中进行好风险控制对于开展信息安全等级保护工作也是必须重视的。首先在测评机构的选择上，北京协和医院选择了由公安部门认可的具有等级保护测评资质的测评单位来实施测评工作，参与测评工作的工程师均为公安部门认可的具有测评工程师资质的人员。在测评工作开始前，与测评机构签署了服务合同与保密协议，明确了责任和义务，确保测评机构开展测评工作的范围均在授权范围内。在进行漏洞扫描、渗透测试前，由扫描和测试的实施人员告知被测评单位实施的风险，配合部门做好必要的备份后方可实施，在实施的过程中做好系统监控工作。此外，还要求测评机构的测试人员应在扫描和测试开始前主动介绍测评工具的功能和风险，确认测评工具的版本和授权状态，在测试人员获得授权后方可实施测试工作，测试完成后，立即关闭由于测试开放的相应端口。为确保测评机构对全部测评结果、文档的保密，多次考察测评机构的独立的、保密的测评数据的处理系统，确保医院的信息系统安全问题不会被泄露。在测评的全过程中，特别重视等级保护测评工作中的风险控制，确保测评工作确实提高信息系统的安全防护能力的同时，未给信息系统带来更多的安全风险。

5 结语

综合测评分析和安全整改的结果，北京协和医院门诊住院信息系统等级测评结果中存在“部分符合”项，但不会导致信息系统面临高等级安全风险，故该系统测评结论为：基本符合。近年来，随着医院信息化建设突飞猛进的发展，新技术、新架构、新观念、新管理模式和新系统不断涌现，大幅提高了医院各方面工作的效率，同时也增加了系统复杂度，而相应的信息安全保障需求和难度也随之大幅提升，这就需要卫生行业的各单位与各信息安全服务机构、测评机构进行深度合作和不断探索，尝试建立适合卫生行业自身发展需要的卫生行业信息系统信息安全标准（建议可参考北京市卫生行业基础设施建设指南和规范 2008 版）。随着新技术的不断发展和完善，应团队协作，合作共赢，切实确保信息系统安全保障和测评工作，能够与正在不断发展和完善的新一代医院信息系统相匹配。

参考文献

1 国务院. 中华人民共和国计算机信息系统安全保护条例（147 号令）[S]. 1994.

2 中央办公厅、国务院办公厅. 国家信息化领导小组关于加强信息安全保障工作的意见（中办发【2003】27 号）[S]. 2003.

3 卫生部办公厅. 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）[S]. 2011.

4 卫生部办公厅. 卫生行业信息安全等级保护工作的指导意见（卫办综函【2011】1126 号）[S]. 2011.

5 北京市卫生局. 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护工作的通知（京卫办字【2012】26 号）[S]. 2012.

6 屠正伟. 三级信息系统等级保护常见问题的整改建议[J]. 电力信息化, 2011,（3）: 65 - 68.

7 高朝勤. 信息系统等级保护中的多级安全技术研究[D]. 北京：北京工业大学, 2012.

8 齐剑雄. 基于信息系统等级保护下安全巡检系统的研究与设计[D]. 北京：北京邮电大学, 2012.

9 刘嘉. 基于综合判定分析的信息系统安全检验技术研究[D]. 北京：北京邮电大学, 2011.

10 胡皓. 面向等级保护的主机安全测评系统的设计与实现[D]. 北京：中国科学院大学工程管理与信息技术学院, 2013.

11 方勤. 基于《信息安全技术信息系统安全保护等级定级指南》的定级量化模型研究及实践[D]. 重庆：重庆大学, 2008.

12 孟晓阳, 郭杰峰. 使用 IT 运行监控系统保障医院信息系统的高可用性[J]. 医学信息学杂志, 2015, 36（2）: 23 - 26.

13 肖革新, 马家奇, 周立平, 等. 公共卫生信息系统安全等级保护建设相关问题思考[J]. 医学信息学杂志, 2012, 33（2）: 2 - 8.