疾控中心信息安全等级保护整改方案设计

庞延辉 罗 俊 肖 鹏

（武汉市疾病预防控制中心 武汉 430015）

〔摘要〕 介绍信息安全等级保护的目标、相关政策和实施流程，结合武汉市疾病预防控制中心网络、应用系统现状，按照安全等级保护的相关要求，测评发现存在的问题并设计出相应的技术整改方案，为下一步整改提供科学、合理的依据。

〔关键词〕 信息系统；安全等级保护；方案设计

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2018.08.009

Design of Rectification Scheme of Information Security Classified Protection of Center for Disease Prevention and Control

PANG Yan－hui, LUO Jun, XIAO Peng, Wuhan Center For Disease Prevention & Control, Wuhan 430015, China

〔**Abstract**〕 The paper introduces the objective, related policies and implementation procedure of information security classified protection. Combining with the status quo of the network and application system of Wuhan Center for Disease Prevention and Control, it assesses the existing problems that have been found according to relevant requirements for security classified protection, and puts forward corresponding technical rectification scheme to provide scientific and rational basis for the next step of rectification.

〔**Keywords**〕 Information system; Security classified protection; Scheme design

1 引言

近年来信息泄密、勒索病毒、伊朗核设施瘫痪事件等网络安全问题层出不穷，对人民生命、财产安全造成重大损失，网络安全成为舆论焦点。2017年6月1日《中华人民共和国网络安全法》实行，信息与网络安全上升到国家安全的战略高度，而信息安全等级保护制度（以下称“等保”）是我国信息安全保护的一项重要制度和方法[1]，开展信息安全等保工作是促进信息化发展、保障信息网络安全的重要措施。

随着武汉市疾病预防控制中心系统信息化的不断发展，传染病、艾滋病、慢性病、血吸虫病以及内部办公等重要业务均实现信息化，业务数据电子化，如果信息系统遭到破坏，重要数据泄露、丢失或者连续几小时无法访问将会对疾控中心业务和广大人民利益造成重大影响。根据《中华人民共和国网络安全法》和《“十三五”全面健康网络与信息完全规划》要求，做好网络信息安全等保工作，对促进我国卫生信息化建设的健康发展、维护社会秩序、公共利益和国家安全有重大意义[2]。本文通过测评手段分析现有信息系统在技术、管理等方面与等保要求存在的差距，提出整改方案，为疾控中心信息安全建设提供科学、合理的依据。

〔收稿日期〕 2018－03－08

〔作者简介〕 庞延辉，工程师；通讯作者：罗俊，副主任医师。

2 等级保护基本情况介绍

国务院在 1994 年颁布《中华人民共和国计算机信息系统安全保护条例》，指出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具体保护办法由公安部会同有关部门制定[3]。1999 年 9 月我国颁布《计算机信息系统安全保护等级划分准则》。2003 年中央办公厅、国务院办公厅颁布的《国家信息化领导小组关于加强信息安全保障工作的意见》中明确指出要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南[4]。2007 年 6 月公安部、国家密码管理局、国家保密局和国务院信息化工作办公室颁布《信息安全等级保护管理办法》，明确信息安全等级保护的详细要求。等保以信息系统为目标，针对信息系统的重要程度，即该信息系统遭到破坏后所造成影响的严重程度，对信息系统进行安全保护等级评定[5]。根据需求保证系统具备相应安全等级的防护能力，不同安全等级的信息系统具有不同等级的网络安全防护能力。等保提出相应的安全要求，根据实现方式的不同，基本安全要求分为基本管理和基本技术要求两类[6]，等级保护基本要求构架，见图 1。

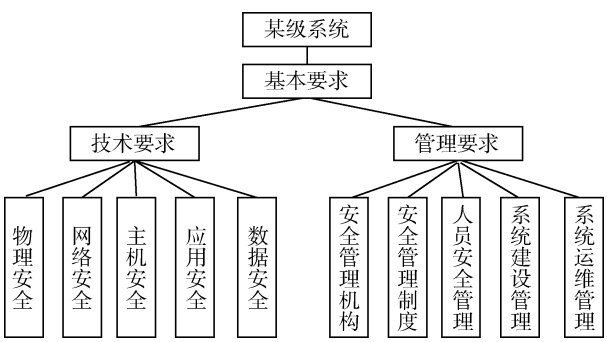

图 1 等级保护基本要求构架

3 实施流程

信息系统安全等级评测流程可以分为 4 个阶段、8 个步骤[7]，见图 2。信息系统资产识别主要内容是成立项目组，对疾控信息系统进行全面摸底调研，掌握总体情况；信息系统登记备案指针对疾控信息系统业务特点，依据等级保护定级指南向当地省公安厅进行定级备案；信息系统风险分析指依据对应的保护等级，开展风险评估工作；信息系统差距分析指依据现场评估结果和相关标准对信息系统的安全保护情况进行差距分析；安全整改方案设计指依据相关标准确定安全保护策略，制定安全建设整改方案；预测评方案编制指依据相关评测标准编制信息系统安全等级评测方案；实施安全建设整改指依据相关标准实施安全建设整改（包括技术和管理层面的整改）；等保评测[8]是由有等级评测资质的第 3 方机构依据相关标准对整改后的信息系统进行安全等级测评，通过后将对信息系统颁发相应的等级证书，若不符合测评要求将重新进行安全整改，直到通过测评为止。

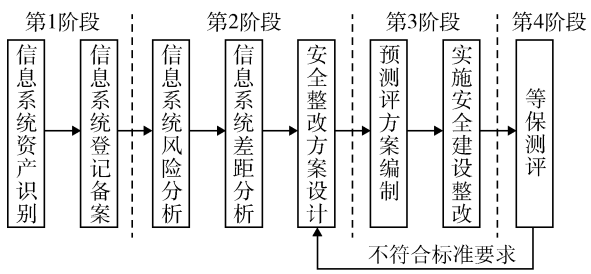

图 2 等级保护实施流程

4 信息化现状

武汉市疾控中心信息化经过十几年的建设，逐步建成几十个信息系统，主要包括 12320 呼叫系统、美沙酮社区维持治疗系统、65 岁以上老人体检系统、死因登记信息管理系统、肿瘤登记信息管理系统、内部办公自动化系统、计划免疫信息管理系统、财务预算信息系统等。2014 年完成信息网络系统、安全系统及配套基础设施改造。网络系统架构设计划分为服务器区，卫生专网区，虚拟专用网（Virtual Private Network，VPN）区，财务专网区以及用户接入区，网络拓扑结构，见图 3。目前存在的主要问题有：（1）各业务系统直接对互联网提供访问服务，信息安全控制措施不能够保障业务系统安全、独立运行。（2）服务器及设备物理、逻辑摆

放比较混乱，不利于管理及控制，存在安全隐患。（3）技术类的安全控制措施不够，不能满足安全等级保护 3 级要求。

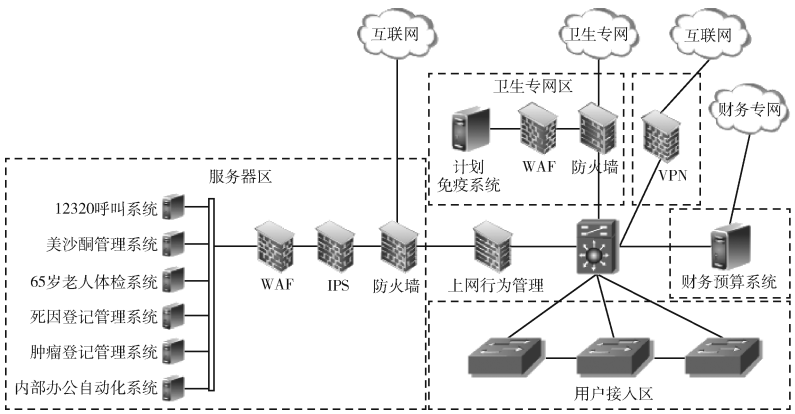

图 3 网络拓扑结构

5 等级保护整改方案设计

5.1 系统分析和定级

系统定级是信息系统开展信息安全等保工作的第 1 个环节，也是后续等级测评和网络安全整改的前提条件。信息系统定级由两个因素决定：一是系统安全服务等级；二是业务信息安全等级。主要考量业务信息系统在受到破坏时的客体以及对客体造成的受损程度，根据《信息系统安全保护等级定级指南》在两者中取等级较高的为信息系统的安全级别[9]，见表 1。武汉市疾控中心的计划免疫信息管理系统为全市适龄儿童提供疫苗接种的信息管理，内容包含有家庭住址、电话、身份证号、姓名、性别、接种针次等，涉及全市几十万儿童家庭信息。美沙酮社区维持治疗信息管理系统是国家根据当前禁毒防艾的工作要求提出并逐步推进的针对海洛因等阿片类药物依赖者的一种替代治疗模式的信息系统，包含患者姓名、地址、联系方式、身份证号、敏感用药情况等隐私信息。以上两个业务信息系统受到破坏后会严重影响社会秩序，而信息泄露则会严重损坏公众利益，按信息系统安全等级保护定级指南的规定，确定计划免疫信息管理系统和美沙酮社区维持治疗信息管理系统安全保护等级为第 3 级。

表 1 信息系统定级

受到破坏时所侵害客体	对客体造成的侵害程度		
	一般	严重	特别严重
公民、法人和其他组织的合法权益	第 1 级	第 2 级	第 2 级
社会秩序和公共利益	第 2 级	第 3 级	第 4 级
国家安全	第 3 级	第 4 级	第 5 级

5.2 安全整改方案设计

5.2.1 概述 依据 GB1759 – 1999 等系列安全等级保护 3 级相关标准，对原有的网络体系结构进行安全整改，加强区域边界安全保护，将相关技术要求落实到网络安全区域边界、运行环境、管理中心和通信 4 个部分。构建成 1 个中心、3 重安全保障体系的防护体系，整改后的网络拓扑结构，见图 4。

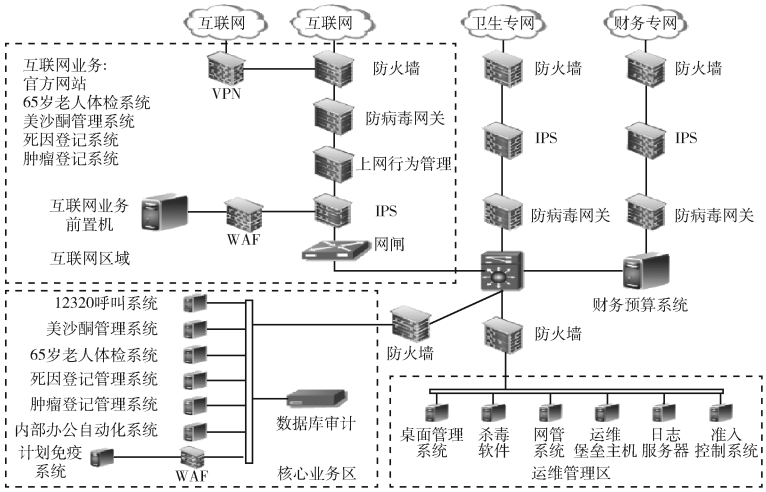

图4 整改后的网络拓扑结构

5.2.2 安全运行环境 发现终端用户或是服务器中存在的不安全特性，对现有操作系统进行有针对性的网络安全加固，如在信息系统中实现安全访问控制、身份认证、安全审计等安全防护。

5.2.3 安全区域边界 根据不同的业务功能、出口划分为5 大安全区域。(1) 核心业务区。主要存放业务信息系统和数据库，对外通过防火墙进行逻辑隔离，直接接入内网核心交换机。服务器按照不同信息系统的安全保护等级划分到不同虚拟局域网(Virtual Local Area Network，VLAN) 进行逻辑隔离，进行有效的访问控制，只允许高级访问低级系统，不允许低级访问高级系统。(2) 运维管理区。从功能、重要级别角度考虑，建立专门的安全运维中心，承担保障网络运行、安全、维护的工作。包括桌面管理系统、杀毒软件、网管系统、运维堡垒主机、日志服务器、准入控制系统等安全设备或软件，通过防火墙与内网进行逻辑隔离。(3) 互联网区域。主要提供互联网出口和对外业务访问，属于高风险区域，利用网闸设备与内网进行物理隔离。对外提供服务的信息系统(如官方网站、65 岁以上老人体检系统、美沙酮社区维持治疗信息管理系统、死因登记管理系统、肿瘤病历报告管理系统等) 在互联网区域采用前置机的形式，通过应用防火墙(Web Application Firewall，WAF)，入侵防火系统(Intrusion Prevention System，IPS)，防病毒网关等安全措施保证业务系统的安全。(4) 卫生专网和财务专网区域。在边界部署 IPS、防火墙和防病毒网关与内网进行安全逻辑隔离。(5) 用户接入区。部署网络准入控制管理系统通过身份认证等手段确认接入终端的合法性，一旦发现非法终端立即采用技术手段中断其网络访问权限，拒绝其接入网络。通过对非法接入的管理可以有效阻止内部员工在工作时间访问非信任网络资源，防止由于访问非法网络资源而导致信息泄露或引入其他的网络安全威胁。

5.2.4 安全通信 当用户需要跨区域访问时，根据3 级等保标准要求，需要对业务数据在传输过程中进行防护，主要分为以下3 个方面：(1) 业务上报单位与服务器间通信。通过部署天融信 VPN 安全设备构建安全隧道，为通信双方建立安全通道，实施数据传输机密性和完整性保护。美沙酮社区维持治疗系统各门诊点通过 IPSEC VPN 客户端连接到服务器，对于免疫规划信息管理系统采用卫生专网为主、VPN 隧道为辅的安全通信策略，为全市接种点与市级计免平台间信息的安全传输提供身份鉴别、加密和完整性保护及控制等安全机制。(2) 内网各部门员工间的相互通信。通过划分 VLAN 进行逻辑隔离，规定哪些部门可以访问哪些服务器，提高网络效率。(3) 内部用户与互联网间的通信。通过部署深信服上网行为管理设备，对内网用户访问互联网时进行资源访问控制和带宽使用优先级，合理阻止非业务网络应用，有效管理与利用互联网资源。

5.2.5 安全管理 信息安全等级保护3级的信息系统应建立信息安全管理中心，用于监控和记录信息系统中比较重要的网络设备、服务器等信息以及所有业务系统和系统用户的网络安全状况。部署企业版杀毒软件、桌面管理系统、网管系统、运维堡垒主机、日志服务器、准入控制系统等，完成通信线路、网络设备、主机、应用系统和系统用户等监控和警告，形成相关数据报表。

6 结语

本文主要从等保技术要求的角度阐述对疾控中心原有网络结构的改造，但要完成安全等保评审工作还应从制度、人员、运维等全方位实施和落实[10]。通过信息安全等保工作的开展，优化信息安全资源配置，保障重要疾控业务信息系统安全，促进网络安全与业务信息化协同发展，在疾控信息化建设过程中同步建设网络信息安全对推动疾控业务信息化可持续发展具有深远意义。

参考文献

1 中华人民共和国国家质量监督检验检疫总局，中国国家标准化管理委员会. 信息系统安全等级保护基本要求（GB/T 22239－2008）［S］. 2008.

2 中华人民共和国国家质量监督检验检疫总局，中国国家标准化管理委员会. 信息系统安全等级保护测评过程指南（GB/T 28449－2012）［S］. 2012.

3 蔡海岩. 采供血机构信息安全等级保护建设方案与实践［J］. 计算机光盘软件与应用，2014，(11)：165－166.

4 李洪民. 浅谈网络安全等级保护信息建设方案［J］. 现代工业经济和信息化，2016，6（13）：85－87.

5 蔡雨蒙，朱一新，刘云，等. 医疗卫生行业信息安全等级保护探讨［J］. 医学信息学杂志，2014，35（9）：12－15.

6 鞠鑫，戴春林，沈婷. 苏州市卫生信息中心信息安全等级保护建设实践与应用［J］. 中国数字医学，2015，10（2）：77－80.

7 郑见立，李亚子. 信息系统等级保护与分级保护实施对比分析［J］. 医学信息学杂志，2015，36（10）：25－29，33.

8 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.

9 肖勇，沈绍武，田双桂，等. 中医药项目预算监控平台信息安全等级保护实践［J］. 医学信息学杂志，2014，35（9）：7－11.

10 王磊，魏晓艳，郎爽，等. 医院信息安全等级保护三级评测的应用与实践［J］. 中国数字医学，2015，10（2）：81－83.