疾控信息系统网络安全防护实践

庞延辉 罗 俊 肖 鹏 章诗韵 舒成城

（武汉市疾病预防控制中心 武汉 430015）

〔摘要〕 分析疾控信息系统安全建设需求，从安全管理体系建设、安全运维措施、安全意识教育、信息系统全生命周期管理等方面详细阐述基于等级保护制度 2.0 的疾控信息系统网络安全防护实践。

〔关键词〕 等保 2.0；疾控信息系统；网络安全；实践

〔中图分类号〕R－058 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2022.04.013

Practice of Information System Network Security Protection in Center for Disease Control and Prevention *PANG Yanhui, LUO Jun, XIAO Peng, ZHANG Shiyun, SHU Chengcheng, Wuhan Center for Disease Control & Prevention, Wuhan 430015, China*

〔**Abstract**〕 The paper analyzes the requirements for the security construction of information systems of Center for Disease Control and Prevention (CDC), and expounds the network security protection practices based on the classified protection system 2.0 from the aspects of safety management system construction, safety operation and maintenance measures, safety awareness education, the whole life cycle management of information systems, etc.

〔**Keywords**〕 classified protection 2.0; information system of Center for Disease Control and Prevention (CDC); network security; practice

1 引言

1.1 研究背景

随着信息化发展，信息技术在疾控行业中得到充分应用。武汉市逐步建立起传染病、慢性病、健康危害因素及居民死亡原因上报等疾控信息系统，保存有大量敏感信息。近年来疾控、医院等卫生机构屡次发生勒索、入侵、数据泄露等安全事件[1]。如何加强网络安全防护已经成为信息化建设中的难题。2017 年《中华人民共和国网络安全法》和《网络安全等级保护基本要求（GB/T 22239－2019）》（等级保护制度 2.0）等系列标准相继出台实施[2－3]，成为我国各行各业开展网络安全防护工作的金标准，疾控网络安全建设必须以此为依据，提高网络安全防护能力。

1.2 等级保护制度 2.0 概述

2019 年 5 月 13 日等级保护制度 2.0 国家标准（以下简称等保 2.0）的发布标志着国家网络安全等级保护工作步入新时代。等保 2.0 在法律支撑、技术、工程应用层面都有较大创新，以“一个中心、三重防护”为中心的指导思想[4]，从安全管理体系和安全技术体系两方面建设网络安全防护框架[5]。等保 2.0 是推动新一代网络安全变革的驱动力[6]，可指导疾控行业新安全体系建设，应对外部高级威胁与内部业务安全问题，推动疾控信息系统网络安全水平全面提升。

〔修回日期〕 2021－08－08

〔作者简介〕 庞延辉，硕士，工程师，发表论文 8 篇。

2 疾控信息系统安全建设需求

2.1 安全管理体系

疾控中心横向隶属于本级卫生健康管理部门，纵向接收上级疾控中心的技术指导和工作要求，在网络安全上也受到辖区安全管理部门的监督。在信息化建设过程中，还涉及内部信息科、业务科室、采购部门等。根据等保 2.0 安全管理体系要求，需要做好制度、机构、人员、安全建设和安全运维管理 5 项工作内容。首先，亟需梳理各方关系，厘清网络安全责任边界，按照“谁建设谁负责、谁运营谁负责、谁使用谁负责”原则[7]，建立网络安全组织架构，明确信息部门工作范围和责任边界。其次，加强信息系统安全运维管理。最后，提高人员网络安全意识。

2.2 安全技术体系

由于疾控中心业务范围涉及较广、需求多样，经长时间发展形成较多孤立的信息系统。另外为满足业务系统需求，逐渐接入了卫生专网、政务内网、财务专网、视频会议专线，具有复杂的网络结构和互联网暴露点多的特点，增加了网络安全防护难度。依据等保 2.0 安全技术体系要求，需要做好安全物理环境、通信网络、区域边界、计算环境和安全管理中心 5 方面工作。根据疾控中心实际情况，一方面，厘清内部信息资产；另一方面，划清网络安全边界，加强区域防护；最后，加强信息系统全生命周期信息安全管理。对此，本次实践从安全管理和安全技术两方面入手，对疾控中心原有安全架构查漏补缺，形成符合等保 2.0 的 3 级信息系统安全体系。

3 安全管理体系建设

3.1 组织架构

3.1.1 *总体架构* 网络安全管理是一项复杂的工程，其管理对象包括人、物和网络空间，除了技术实现，单位管理层的参与和重视至关重要。因此以单位党委书记作为网络安全第一责任人，强化网络安全责任制，在组织架构上划分为管理层和运行层。

3.1.2 *管理层* 在管理层面成立网络信息安全领导小组，由中心领导和中层干部组成。中心党委书记担任小组组长，分管领导为直接负责人，科长为成员。领导小组职责是制定中心网络安全目标和管理制度、评审与监察网络安全事件。

3.1.3 *运行层* 领导小组下设办公室在中心信息科，具体承担领导小组的日常管理工作，依据“谁建设谁负责、谁运营谁负责、谁使用谁负责”原则，贯彻落实上级网络工作的部署和要求；负责统筹、协调本单位网络安全事件应急工作，配合上级主管部门和辖区网络安全管理部门做好网络安全相关应急处置工作；保障应用系统安全，推进信息系统全生命周期安全管理，信息技术基础设施安全基线检查，督促相关科室及厂商完成安全整改等。后勤部门负责信息系统及相关硬件设备采购、电力供应和消防设备维护等。系统建设部门承担信息系统安全主体责任，负责软件部分安全整改。同时中心与上级主管部门、各类供应商、业界专家及安全组织等外联单位保持合作伙伴关系，建立合作内容、联系方式列表，开展常态化沟通协作。

3.2 安全运维

3.2.1 *安全巡检* 网络安全是不断变化和发展的动态过程，使用任何一种功能强大、体系健壮的技术产品都不可能一劳永逸地解决网络安全威胁问题，需要根据外部安全态势和安全通告不断完善内部安全措施。日常安全巡检是信息系统常态化运行中保障网络安全的重要手段，其目的是确保信息系统网络安全一直处于等保基线水平上。在实践中采取“日周月季”巡检措施。日巡检：每日进行机房物理安全巡查，包括门禁状态、空调温湿度、不间断电源（Uninterruptible Power Supply，UPS）以及各种网络设备服务器指示灯是否正常等；周巡检：收集态势感知平台和日志审计数据，对本周内网络攻击行为进行分析总结，采取漏洞修复、口令修改、IP 封堵等措施，降低安全风险；月报告：对终端电脑、服务器、虚拟机、安全设备、数据库等做

全面安全检查，形成月度运维报告，分析存在的安全问题，提出整改意见，列出整改计划；季度漏扫：每季度定期对信息系统进行安全漏洞扫描和人工渗透，形成“季度安全渗透测试及巡检报告”，涉及信息系统有安全漏洞的，由信息科督促责任部门及时整改，按时提交整改报告并将整改结果纳入季度绩效考核。

3.2.2 安全应急处置 目前安全应急处置主要来自于外部通报和内部自查。其中外部通报是指市网信办、市网安部门、上级主管部门等第 3 方监管机构下发的安全通报，由网络安全员负责进行深入分析，评估影响范围，按时完成系统加固并提交整改报告；内部自查是指在日常安全巡检或收到态势感知的安全警告，发现系统有被黑客入侵的迹象，网络安全员对该情况进行深入分析，如果确认系统被攻击，则立即启动“信息系统安全应急预案”，果断采取阻断措施，同时评估影响范围，进行攻击溯源，形成网络安全事件报告，按预案流程逐级上报。

3.2.3 重保服务 重大事件安全保障服务简称为“重保服务”，是为解决人员经验技术不足及配置缺陷等问题，由第 3 方专业安全公司提供协助，处理特殊时期（如各级护网行动、重大节假日及活动期间）信息系统安全工作中出现的故障、安全事件以及安全管理方面的问题，保障业务系统完整性、保密性，使业务系统高效持续运行。通过事前发现与预防、事中处理与恢复、保障后评估与总结 3 个阶段，全面了解系统安全现状，实现详细资产梳理、漏洞检测加固、全量的网站监控、专业人员值守、问题总结实时整改等工作。

3.3 安全意识教育

3.3.1 安全培训 网络安全意识教育是保障网络安全的重要环节，在等保 2.0 中明确指出应对各类人员进行安全意识教育。疾控机构中参与信息系统流程的人员较多，将培训对象分为业务人员和信息技术人员，由信息科统一组织、定期开展，采取线上、线下或两者相结合的培训形式。针对业务人员进行普及性安全意识教育，结合当前国内外网络安全形势、安全事件案例等告知相关安全责任和惩戒措施，加深被培训者的印象，针对信息技术人员进行网络安全基础知识和岗位技能培训，加强政策宣贯和制度学习。

3.3.2 管理制度 做好网络安全管理应制定网络安全工作总体方针、安全策略和各种管理制度。由信息科制定和发布，定期对安全管理制度合理性和适应性进行论证和审定，针对存在的不足进行修订。围绕信息系统全生命周期制定相关制度，包括“信息化项目管理制度”“网络安全管理制度”“信息系统运维管理制度”“网络安全意识教育和培训制度”“网络安全责任追究制度”“信息系统安全应急预案”等。严格按照制度内容落实网络安全工作，通过日常网络安全防护实践不断完善管理制度，形成良好循环。

3.3.3 安全通告 安全通告是指通过互联网或第 3 方安全服务公司及时获取最新的安全漏洞态势、前沿安全技术，及时了解最新的重大安全事件，提升网络安全管理员技术能力，为单位内部进行安全预警，提前做好安全漏洞补丁修复。在实践中采取购买服务形式，由第 3 方每月提供一期安全态势报告，内容包括紧急安全事件通告、安全漏洞通告、安全预警通告和安全建议。在出现高危漏洞和突发重要事件时将提供相应安全通告。

3.4 信息系统全生命周期管理

针对信息系统，严格落实“同步规划、同步建设、同步使用”的 3 同步原则[8]。首先，在信息系统规划阶段要进行安全方案讨论，明确用户对象、保护等级、所属安全区域、安全措施；其次，在实施阶段填写“服务器资源申请表”，明确系统网络拓扑图，设置安全措施（杀毒软件、EDR、主机防火墙、网络防火墙安全策略、WAF、数据库审计、日志审计、数据备份、堡垒机、VPN 等），上线前在绕开安全设备防护下进行安全漏洞扫描，整改完成后才允许上线运行；最后，同步运行，做好常态化系统运行网络安全监督检查整改。同时在信息系统停止使用后，要收回服务器资源和网络安全配置，做到信息系统的全生命周期管理。

4 安全技术体系建设

4.1 信息资产梳理

网络安全遵循“木桶原理”，防护工作质量取决于最短板[9]。因此全面梳理信息资产是做好网络安全的首要工作，将资产整理成表形成网络拓扑图和资产清单。信息资产包括服务器、虚拟机、存储、安全设备、软件信息系统等，不同资产的记录字段有所差异。

4.2 安全区域规划（图 1）

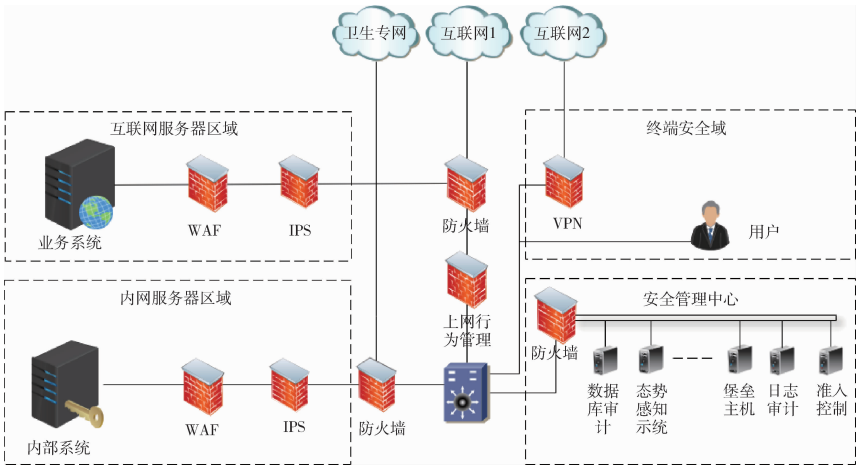

图 1 安全区域规划构架

4.2.1 概述 等保 2.0 提出“一个中心，三重防御”的重要思想：一个中心指“安全管理中心”，三重防御是指“安全计算环境、安全区域边界、安全网络通信”[10]。中心参考网络安全等级保护安全技术设计框架，将网络划分为 4 个安全区域：外网服务器安全域、内网服务器安全域、终端安全域和安全管理中心。各安全域所使用资源相对独立，域间通过安全设备相互通信，域内通过虚拟局域网（Virtual Local Area Network，VLAN）进行逻辑隔离或者终端检测响应平台（Endpoint Detection and Response，EDR）进行微隔离[11]。

4.2.2 外网服务器安全域 该区域采用虚拟化技术构建虚拟计算资源池，部署供互联网用户访问的业务信息系统。域内各虚拟机均安装企业版杀毒软件，利用 EDR 进行服务器间的微隔离，控制服务器间横向访问，根据最小访问权限原则仅开放虚拟机之间必要的访问端口。

4.2.3 内网服务器安全域 该区域同样采用虚拟化技术构建计算资源池，部署仅供内部员工或医疗卫生单位用户访问的业务信息系统，用户只能通过局域网或卫生专网访问业务系统。安全策略与外网服务器区域一致，通过防火墙与其他区域进行逻辑隔离。

4.2.4 终端安全域 终端是指局域网内有线用户、无线用户和 VPN 虚拟终端。中心办公区域全部覆盖无线网络，为规范管理无线用户，将其分为内网用户和游客两类。其中内网用户仅指内部员工，可访问内部业务系统，需要安装准入控制系统进行登记，实施杀毒软件、主机强口令的安全检测，通过后给予放行；有线用户管理同无线内网用户；VPN 虚拟终端是指用户在互联网环境以 VPN 方式访问内部资源，将严格控制访问权限。系统运维人员以 VPN 方式访问堡垒机，开展系统维护工作。

4.3 安全管理中心

等保 2.0 将安全管理中心从管理层面提升到技术层面，独立出来进行要求，包括系统管理、审计管理、安全管理、集中管控等功能[12]，从被动防御转变为主动防御、动态防御。该区域功能主要通过安全设备实现，包括防火墙、网络管理平台、日志审计、数据库审计、数据备份、VPN 设备、准入控制系统、EDR、安全网闸、堡垒机、态势感知平台

等，以实现权限集中管控、日志集中审计、安全事件集中监控响应、安全策略的统一管理、漏洞补丁的统一更新等。

5 结语

通过上述网络安全加固措施，大幅提升疾控信息系统安全防护能力，顺利通过网络安全 3 级等保测评，有效保障网络安全。等级保护 2.0 为各行各业提供了一个网络安全建设基线[13]，但网络安全是个动态防护过程[14]，重点是建立一套监测、整改加固、应急事件处置的日常管理机制。在本实践中较为创新的是设置“日周月季”的巡检措施和完善的应急处置流程，将网络安全工作常态化，做到早发现、早处置。网络安全需要从技术与管理的角度对当前存在的安全隐患进行全面分析，保证疾控信息系统安全稳定运行，为疾控工作提供可靠支撑。

参考文献

1 中国政府网. 中国疾控中心回应艾滋病感染者疑遭电话诈骗——已报请公安部门立案侦查 [EB/OL]. [2016 - 07 - 17]. http://www.gov.cn/xinwen/2016 - 07/17/content_ 5092288.htm.

2 瞿朗, 左秀然, 杨国良. 疫情期间医院网络安全风险及防范措施 [J]. 中国数字医学, 2020, 15 (5): 92 - 95.

3 吴军, 沈晓融, 陶沁, 等. 基层疾控机构信息网络安全建设探讨 [J]. 中国卫生信息管理杂志, 2019, 16 (1): 26 - 28.

4 鞠鑫. 市级卫生计生信息中心安全建设的探索与实践 [J]. 中国卫生信息管理杂志, 2018, 15 (3): 254 - 257.

5 孟晓阳, 王辰超, 朱卫国. 医院网络安全防护策略实践与探讨 [J]. 中国卫生信息管理杂志, 2020, 17 (3): 290 - 295.

6 吴前兵, 刘静, 程西雅. 医院信息安全建设探索 [J]. 医学信息学杂志, 2020, 41 (8): 57 - 61.

7 李先锋, 曹亮, 刘熠斐, 等. 等保 2.0 对医院信息安全管理的新要求探讨 [J]. 江苏卫生事业管理, 2020, 31 (3): 344 - 347.

8 胡建平, 郝惠英, 何祺, 等. 卫生健康行业网络安全态势感知平台建设探讨 [J]. 中国卫生信息管理杂志, 2019, 16 (1): 4 - 8.

9 黄家平, 鲁茜. 医院信息网络安全体系构建 [J]. 医学信息学杂志, 2019, 40 (11): 45 - 47.

10 戴丽金, 张丽娜, 巫立华, 等. 福建地震信息系统等级保护应用实践 [J]. 网络安全技术与应用, 2020 (10): 156 - 157.

11 陈强, 马家奇, 王松旺. 省级疾病预防控制中心信息化建设与信息安全评估 [J]. 中国卫生信息管理杂志, 2019, 16 (1): 22 - 25.

12 刘军. 省级疾控机构信息化建设中的信息安全问题与对策 [J]. 医疗卫生装备, 2015, 36 (4): 120 - 122.

13 王晓丽, 丁月红, 陆昊. 等保 2.0 要求下医疗网络安全建设与管理研究 [J]. 中国数字医学, 2020, 15 (12): 5 - 9.

14 冯国斌, 刘艳亭, 郭敬鹏, 等. 基于网络安全等级保护制度 2.0 标准的医院态势感知平台建设实践 [J]. 中国数字医学, 2020, 15 (11): 135 - 138.