山东省卫生健康行业网络安全调查与分析*

徐东海[1]　屈晓晖[2]　刘志国[3]　李　勇[4]　成世良[5]　包国峰[6]

（[1]山东健康医疗大数据管理中心　济南 250000　[2]国家卫生健康委统计信息中心　北京 100044
[3]东营市第二人民医院　东营 257000　[4]北方健康医疗大数据科技有限公司　济南 250000
[5]广饶县人民医院　东营 257300　[6]山东第一医科大学附属省立医院　济南 250000）

〔摘要〕　**目的/意义** 调查分析山东省卫生健康行业网络安全现状，精确定位行业网络安全短板，提升风险管理决策能力。**方法/过程** 以问卷方式采集数据，从医疗机构等级和地域分布两个维度进行网络安全差距分析。**结果/结论** 针对当前山东省基层医疗卫生机构信息化建设管理和技术防护层面的问题，提出卫生健康行业网络安全治理具体措施。

〔关键词〕　卫生健康；网络安全；数据安全；安全治理；差距分析
〔中图分类号〕R－058　　〔文献标识码〕A　　〔DOI〕10.3969/j.issn.1673－6036.2023.11.008

Investigation and Analysis of Network Security of Health Industry in Shandong Province

XU Donghai[1], *QU Xiaohui*[2], *LIU Zhiguo*[3], *LI Yong*[4], *CHENG Shiliang*[5], *BAO Guofeng*[6]
[1]*Shandong Health and Medical Big Data Management Center, Jinan 250000, China*; [2]*Statistical Information Center of the National Health Commission, Beijing 100044, China*; [3]*The Second People's Hospital of Dongying, Dongying 257000, China*; [4]*North Health Medical Big Data Technology Co. Ltd., Jinan 250000, China*; [5]*The People's Hospital of Guangrao County, Dongying 257300, China*; [6]*Provincial Hospital Affiliated to Shandong First Medical University, Jinan 250000, China*

〔**Abstract**〕　**Purpose/Significance** To investigate and analyze the current situation of health industry network security in Shandong province, to pinpoint the network security weaknesses, and to improve the decision－making capacity of risk management. **Method/Process** Based on the data collected by questionnaires, the gap analysis of network security is conducted from the two dimensions of the level and regional distribution of medical institutions. **Result/Conclusion** In view of the problems faced by the informatization construction of primary medical and health institutions at the management level and the technical protection level, the specific solutions to the network security governance of health industry are put forward.

〔**Keywords**〕　health industry; network security; data security; security governance; gap analysis

1　引言

自2016年《网络安全法》[1]颁布以来，各行业纷纷出台适用于本行业的网络安全规章制度。近年来，随着《关于促进和规范健康医疗大数据应用发展的指导意见》《关于促进“互联网＋医疗健康”发展的意见》[2]《关于深入推进“互联网＋医疗健

〔修回日期〕　2023－05－08
〔作者简介〕　徐东海，高级工程师，发表论文10余篇；通信作者：屈晓晖，副研究员。
〔基金项目〕　山东省软科学研究计划项目（项目编号：2020RKB01483）。

康”“五个一”服务行动的通知》等政策文件的出台，以及大数据、人工智能等新兴技术的发展，健康医疗数据应用、“互联网 + 医疗健康”和智慧医疗迎来蓬勃发展。与此同时，各类新技术、新应用的出现为卫生健康行业数据治理带来更多挑战。为应对新兴技术应用带来的安全风险，本文通过定量化风险评估和差距分析，协助医疗行业快速找到安全短板，提升风险管理决策能力。

2 资料与方法

2.1 数据来源

采用山东省卫生健康委员会 2022 年 11 月在全省开展的卫生健康领域健康医疗大数据安全治理调研数据。

2.2 研究区域和数据描述

参与本次调研的机构共 248 家，覆盖山东省 16 个地市。按照地域分布情况分为 6 类，即鲁北地区、鲁东地区、鲁南地区、鲁中地区、鲁西北地区、鲁西南地区。其中，鲁北地区包含滨州市和东营市；鲁东地区包含青岛市、烟台市和威海市；鲁南地区包括济宁市、枣庄市、临沂市和日照市；鲁中地区包括济南市、淄博市、潍坊市和泰安市；鲁西北地区包括德州市和聊城市；鲁西南地区为菏泽市。将组织机构分为 5 类，分别是各地市卫生健康委员会（局）、三级医疗卫生机构、二级医疗卫生机构、一级医疗卫生机构、其他类型医疗卫生机构。

2.3 方法描述

采用调查问卷方式采集数据，按照医疗机构的等级与地域分布，分别从网络与数据安全管理能力、技术防护两个方面进行差距分析。其中网络与数据安全管理能力方面主要涵盖 17 项指标，技术防护方面涵盖 36 项指标。差距分析基于调查问卷中各指标的填报数据，进而比较分析。

3 研究结果

3.1 按机构等级进行差距分析

3.1.1 管理能力差距分析（表 1）

表 1 医疗机构管理能力差距分析

机构类型	机构数（家）	网络安全管理职能部门建设完善的机构数及占比［n（%）］	信息化领导小组建设完善的机构数及占比［n（%）］	应急处置机制建设完善的机构数及占比［n（%）］	尚未开展新技术应用的机构数及占比［n（%）］
各地市卫生健康委员会（局）	20	18（90）	15（75）	14（70）	6（30）
三级医疗卫生机构	81	77（95）	75（93）	69（85）	30（37）
二级医疗卫生机构	107	89（83）	81（76）	73（68）	62（58）
一级医疗卫生机构	21	13（62）	13（62）	12（57）	11（52）
其他类型医疗卫生机构	19	14（74）	14（74）	13（68）	12（63）

3.1.2 技术防护差距分析 各级医疗卫生机构技术防护能力参差不齐，其中各地市卫生健康委员会（局）在拒绝服务攻击、数据脱敏系统和主机安全探针等技术防护方面较其他机构更加完善；三级医疗卫生机构在数据库审计、运维审计堡垒机、日志审计与分析等技术防护方面建设更加突出，占比均超过 80%；一级医疗卫生机构在上网行为管理、邮件安全和数据库防火墙等技术防护方面优于另外 4 类机构，占比均在 70% 以上。各级机构在对脆弱性评估与管理、安全基线与配置管理等技术防护方面关注较为欠缺，均未达到 40%，见表 2。防火墙、防病毒和数据备份与恢复等技术防护方面建设较完善，且不同等级机构之间相差不大。

表2　医疗机构技术防护能力差距分析

机构类型	采用率最高（大于90%）的网络安全防护设备及措施	采用率中等（50%～90%）的网络安全防护设备及措施	采用率最低（小于50%）的网络安全防护设备及措施
各地市卫生健康委员会（局）	防病毒网关设备、防火墙和入侵检测与防御	网络安全审计、网络准入等16种技术	数据库防火墙、数据加密系统、安全基线与配置管理等7种技术
三级医疗卫生机构	防火墙设备、入侵检测与防御、数据备份与恢复	运维审计、数据库审计、网络安全审计等22种技术	威胁分析与管理、硬件认证和邮件安全等11种技术防护措施
二级医疗卫生机构	防火墙设备、防病毒、数据备份与恢复	入侵检测与防御、网络隔离和单向导入等27种技术	数字证书、安全管理平台和主机安全探针等16种技术防护措施
一级医疗卫生机构	防病毒设备	防火墙和上网行为管理	数据加密系统、硬件认证和主机安全探针等15种技术
其他类型医疗卫生机构	邮件安全设备	终端安全管理和防病毒	Web应用安全扫描、网络安全审计、威胁分析与管理等16种技术防护措施

3.2　按机构地域进行差距分析

3.2.1　管理能力差距分析　鲁北、鲁东、鲁南等6个地区在成立领导小组方面做得比较好，各地区之间差距较小。在网络安全管理职能部门建设层面，鲁北和鲁西北地区相较其他地区做得比较好，鲁东、鲁南、鲁中和鲁西南地区管理水平差距不大。在应急处置机制方面，各地区水平差异较大，相比之下，鲁北、鲁东、鲁南、鲁西北等地区管理能力较强，见表3。

表3　各地域医疗机构管理能力差距分析

地区	机构数（家）	网络安全管理职能部门建设完善的机构数及占比［n（%）］	信息化领导小组建设完善的机构数及占比［n（%）］	应急处置机制建设完善的机构数及占比［n（%）］	尚未开展新技术应用的机构数及占比［n（%）］
鲁北	22	20（91）	15（68）	13（59）	18（82）
鲁东	74	60（81）	60（81）	45（61）	61（82）
鲁南	76	65（86）	59（78）	58（76）	46（61）
鲁中	44	38（86）	36（82）	33（75）	25（57）
鲁西北	24	23（96）	22（92）	22（92）	7（29）
鲁西南	8	6（75）	6（75）	6（75）	4（50）

3.2.2　技术防护差距分析　整体来看，各地域之间对于不同防护手段的部署程度有差异。防火墙、入侵检测与防御、防病毒网关、数据备份与恢复、日志分析与审计等，各地域部署程度均比较成熟且差异较小；在数据库脱敏系统、数据库加密系统、数据泄露防护、文件管理与加密等方面，各地域部署的防护能力普遍偏低，有待加强；而在网络隔离和单向导入、防病毒网关、网络安全审计、虚拟专用网络（virtual private network，VPN）、抗拒绝服务攻击等方面，各地域之间部署防护程度差异较大，见表4。

表 4　各地域医疗机构技术能力差距分析

地区	采用率最高（大于90%）的网络安全防护设备及措施	采用率中等（50% ~90%）的网络安全防护设备及措施	采用率最低（小于50%）的网络安全防护设备及措施
鲁北	防火墙、防病毒、Web 应用防火墙	防病毒网关、数据库审计、数据备份等 14 种技术	网络安全探针、数据加密系统、威胁分析与管理等 9 种技术
鲁东	防病毒网关、数据备份与恢复、防火墙	入侵检测与防御、网络安全审计等 17 种技术	Web 应用安全扫描、数据库防火墙、安全管理平台等 16 种技术防护措施
鲁南	防火墙、防病毒、数据备份与恢复	网络隔离、运维审计等 17 种技术	网页防篡改、Web 应用安全扫描、硬件认证等 15 种技术
鲁中	防火墙与防病毒、数据备份与恢复、入侵检测与防御	网络隔离、运维审计等 17 种技术	数据库防火墙、威胁分析与管理、数字证书等 12 种技术
鲁西北	防火墙、入侵检测与防御、防病毒	数据备份与恢复、网络隔离与单向导入等 15 种技术	安全管理平台、网页防篡改、数据加密系统等 14 种技术
鲁西南	防火墙、入侵检测与防御、防病毒、数据备份与恢复	网络隔离与单向导入、网络安全审计、数据库审计、运维审计堡垒机等 12 种技术	抗拒绝服务攻击、Web 应用安全扫描、数字证书等 14 种技术

3.3　结果分析

248 家机构的网络安全管理制度体系建设和技术防护体系建设都比较完善。约 60% 的单位在数据安全方面符合管理要求，其余单位在管理层面和技术防护层面仍存在一些问题。在管理层面，部分机构信息安全建设、运维工作缺乏，安全管理技术力量有待加强，40% 的单位在等级保护建设、数据分类分级标准制定及实施方面相对欠缺，50% 的单位在数据销毁方面未实现监管。在技术防护层面，40% 的机构在数据加密、数据脱敏、数据防泄露、威胁分析与管理等方面比较欠缺，目前仅靠防火墙、防病毒软件等产品的简单堆砌，不能有效抵御安全风险。总之，分析本次调研数据可以看出，目前山东省基层医疗卫生机构的信息化建设水平参差不齐，大多数基层医疗卫生机构信息化建设较《医疗卫生机构网络安全管理办法》的要求还有很大距离，当前基层医疗卫生机构信息化建设仍面临巨大挑战。

4　问题与讨论

4.1　问题分析

4.1.1　人员安全管理薄弱　医院管理层对信息化建设及网络安全工作不够重视，未配备足够的专业技术与管理人员，甚至有些等级较低的机构未设置专职岗位，导致医院信息系统安全隐患与漏洞问题无法及时发现与处理。

4.1.2　终端防护能力匮乏　大数据和云计算技术改变了数据存储方式，打破了数据访问边界，医院也开始对外共享数据资源，传统基于物理边界的安全防护已不适用，终端防护能力匮乏引起的病毒威胁、工作效率低下问题日益突显。

4.1.3　安全事件监测能力欠缺　各机构虽在制度规范上趋于完善，但部分机构仍存在制度落实不到位、应急响应不及时、缺乏高端网络安全人才的现象。这极易造成医疗行业信息安全短板效应突出、顶层设计不足、统筹力度不够等问题。

4.1.4　协同联动处置能力不足　卫生健康信息化建设的各个业务系统如果按照条线进行建设和管理，各自为政的建设模式会导致信息烟囱和孤岛的形成，医疗资源无法实现充分整合及利用，信息难以共享，业务服务不能协同。

4.1.5　数据安全防护能力薄弱　自 2021 年《数据安全法》颁布后，医疗行业对数据安全的关注度大幅提升，但在本次调研中发现，大部分机构在此方面的建设能力相对薄弱，使用数据安全关键技术的组织机构占比较低，缺乏数据安全技术的投入，整体防护面建设能力较薄弱。

4.2　解决措施

4.2.1　优化管理机制，强化落实安全管理责任　网

络安全管理制度建设可以最大化地发挥安全系统效能，串联预防、保障、监控、应急全流程，从根本上提升网络安全能力。在此基础上，首先要考虑加强机房安全建设、完善网络安全架构等基础防护，为持续安全建设奠定良好基础。

4.2.2 加强网络安全培训，提升网络安全能力 定期对现有人员开展网络安全培训，动员和组织广大干部职工积极参与，正确认识和使用网络，自觉抵制有害、低俗信息，提高网络安全防范能力[3]，远离网络陷阱、钓鱼事件，确保公众信息及财产安全。

4.2.3 加强数据保护，开展分类分级，关注安全审计 建立数据分级分类指南，注重数据脱敏保护，从业务需求出发对重要数据进行备份，定期检查备份数据的有效性，使用加密系统保护传输和存储数据，达到数据保护与数据价值释放的双重目标。对重要用户及行为进行审计，并将审计日志实时备份至日志服务器，以便在事件发生后进行溯源，快速修复系统，发挥预防和惩戒的作用。

4.2.4 积极利用新技术，解决新问题 在健康医疗大数据利用层面，医疗卫生机构的强诉求是数据不出本地，可利用联邦学习、安全多方计算等安全技术手段实现“数据可用不可见”。

4.2.5 加强网络边界感知能力，提升安全防护意识 现阶段医疗体系的网络边界已经被重新定义，其安全防护措施和手段也应同步更新和提升。如何对各种设施有效实施准入机制以及部署管理措施是面临的主要问题之一[4]。

4.2.6 定期开展资产梳理，减少互联网暴露面 定期采用主动扫描方式，使用网络风险资产监测分析系统，识别联网的资产，获取端口、协议，对网络风险资产进行全面、准确的梳理[5]。通过快速、轻量级漏洞专扫及概念验证（proof of concept，PoC）主动发现网络资产存在的安全漏洞、弱口令等可被攻击者利用的安全风险，准确定位风险优先级，快速有效地解决潜在威胁。

4.2.7 加强威胁情报共享，提升威胁分析能力 基于集中智能化“网络威胁情报云共享平台”，在行业分布式部署威胁情报联防阻断系统，实时汇聚、加工、分析和共享“正向攻击、反向外联”网络威胁情报数据，利用旁路阻断、点对点可信认证、畸形数据包检测、全流量审计、多维度攻击画像等核心技术，发挥云端专家监测分析优势。一点监测、全网阻断，有效落实网络安全防护“关口前移，防患于未然”的要求[6]。

4.2.8 建立安全运营管理中心 建立安全运营管理中心，进一步加强医疗卫生机构的安全防护水平，形成具有主动防御和协同运营能力的医疗卫生机构间的安全运营合作机制。将防病毒系统、桌面准入系统、堡垒机、数据库审计、日志审计、态势感知、运维管理平台等进行统一管理、监控、审计、综合分析[7]。

5 结语

山东省卫生健康行业网络安全治理具有典型代表性，可为各机构提升网络安全保障能力提供参考。卫生健康行业的网络和数据安全治理，对强化卫生健康领域网络和数据安全管理，消除网络和数据安全重大隐患，确保全省乃至全国卫生健康行业网络和数据安全建设工作的有序开展具有重要意义。

参考文献

1 中华人民共和国网络安全法［EB/OL］.［2022－11－07］. http://www.zyhc.gov.cn/ztzl/lszt/gjwlaqxcz/202209/t20220920_76569748.html? isMobile=true.

2 国务院办公厅. 关于促进“互联网＋医疗健康”发展的意见［EB/OL］.［2022－04－25］. http://www.gov.cn/zhengce/content/2018－04/28/content_5286645.htm.

3 唐春芳. “互联网＋”时代下网络信息安全现状及对策［J］. 中国集体经济，2022（21）：3－4.

4 李雁，贺嘉，郑袁平，等. 互联网时代条件下计算机网络数据安全管理措施［J］. 网络安全技术与应用，2021（8）：173－175.

5 胡贞华，陈雪花. 数据治理中安全保障措施的探究［J］. 网络安全技术与应用，2022（6）：55－56.

6 赛迪智库. 我国数据安全治理情况分析［J］. 软件和集成电路，2022（6）：84－90.

7 胡国华. 数据安全治理实践探索［J］. 信息安全研究，2021（10）：915－921.