CAICT 中国信通院　腾讯安全　CHMIA 中国卫生信息与健康医疗大数据学会

# 数字医疗网络安全观测报告

## （2020年）

中国信息通信研究院安全研究所

腾讯科技（深圳）有限公司

卫生信息安全与新技术应用专业委员会

数据保护官（DPO）社群

2020年9月

# 版权声明

# 前　言

卫生健康事业关系着人民群众的生命安全和身体健康，习近平总书记曾深刻指出：在实现“两个一百年”奋斗目标的历史进程中，发展卫生健康事业始终处于基础性地位。近年来，人工智能、大数据、移动互联网等新技术在健康医疗领域加速应用和落地，尤其是在受到2020 年新冠肺炎疫情影响和刺激后，传统医疗服务快速向互联网医疗、智慧医院等新兴业态转换，行业数字化转型进程明显提速。与此同时，卫生健康领域的网络安全攻击和对抗也在不断升级演变，各类新型网络安全风险层出不穷，网络安全日益成为健康医疗行业发展过程中无法规避的重要问题。

为贯彻落实习近平总书记网络强国战略思想，促进健康医疗行业网络安全能力建设和发展，中国信息通信研究院（以下简称“中国信通院”）安全研究所联合卫生信息安全与新技术应用专业委员会、腾讯安全、数据保护官（DPO）社群等行业组织和产业头部企业组成研究团队，基于产业互联网安全实验室的技术能力，持续性地对卫生健康领域的各类机构开展公共互联网层面的安全观测扫描。并综合利用大数据、威胁情报等技术开展研究分析，结合近年来网络安全形势和政策变化趋势，总结形成本报告。

本报告沿用和升级了《2019 年健康医疗行业网络安全观测报告》的技术手段和分析维度，对于医疗机构在公共互联网上存在的资产脆弱性、安全漏洞问题、僵木蠕毒感染、网站篡改四类主要风险变化情况进行了趋势对比分析，并从互联网医院与非互联网医院、公立医院

与私立医院两个重要分类角度对风险特点进行了研究和解读。研究发现，健康医疗行业资产脆弱性和安全漏洞两类防御维度风险明显好转，体现出医疗机构网络安全意识和能力的较大幅度提升；而僵木蠕毒感染和网站篡改风险呈现上升趋势，表明行业面临的网络安全形势依旧十分严峻，针对卫生健康领域的安全攻击仍在持续升温。与此同时，互联网医院相比非互联网医院、公立医院相比私立医院承受着更为强烈的网络攻击，进而被恶意程序感染风险更高，需要重点关注。

本报告旨在通过全面和客观的行业安全态势研究，为健康医疗行业主管部门、医疗机构以及安全服务厂商提供工作思路和建议，共同促进卫生健康领域安全有序发展。限于编者能力和时间，本报告内容难免存在纰漏，恳请业界同仁批评指正。

# 目 录

# 图 目 录

# 一、健康医疗行业网络安全背景

## （一）网络安全形势发展变化情况

近年来，新一代信息技术蓬勃发展，网络空间日新月异，网络空间安全日益成为关系着国计民生的重要主题。习近平总书记指出，“没有网络安全，就没有国家安全”，将网络安全的重要性提升至国家战略层面。随着 2020 年新冠肺炎疫情在全球的暴发和蔓延，各国经济均受到不同程度的负面影响，国际局势日趋复杂，出于政治目的而发起的有组织的网络攻击持续高发。针对我国党政机关、关键信息基础设施运营者等重要单位的 DDoS 攻击、钓鱼邮件攻击呈现高发频发态势，特别是借助新冠肺炎疫情主题开展的网络钓鱼攻击，给我国政府机关和医疗机构带来了巨大的网络安全挑战，一定程度上影响着疫情防控工作的正常开展。

与此同时，新冠肺炎疫情的影响加速了我国企业和社会的数字化转型，互联网医疗、远程办公、线上买菜等新场景新应用得到快速推广和普及，人工智能、大数据、物联网等新一代信息技术逐步实现与场景的深度融合和广泛应用。然而，伴随新兴业态的热度突增和新技术的落地应用，安全漏洞、数据泄漏、网络钓鱼、勒索病毒等网络安全风险和威胁也日益凸显。据国家计算机网络应急技术处理协调中心（CNCERT）发布的《2019 年我国互联网网络安全态势综述》显示，软硬件安全漏洞数量和影响范围呈现逐年上涨趋势，相比 2018 年，2019 年的事件型漏洞和高危零日漏洞分别增长 227%和 47.5%，安全

漏洞风险持续攀升，这些都给我们的新技术应用与新场景落地敲响了网络安全的警钟。

在数字医疗领域，数字化和智能化已经成为产业发展的大势所趋，网络安全问题成为产业转型过程中必须面对的重要挑战。当前，健康医疗机构一方面面临着以数据泄漏、勒索病毒为代表的传统网络安全威胁，另一方面也在探索着如何安全合规地开发利用健康医疗大数据。数字医疗领域的网络安全问题呈现多元化发展态势，网络安全与数字化发展更加紧密结合，如何在保障网络安全的前提下推动产业数字化转型发展，成为数字医疗领域共同面临的重大课题。

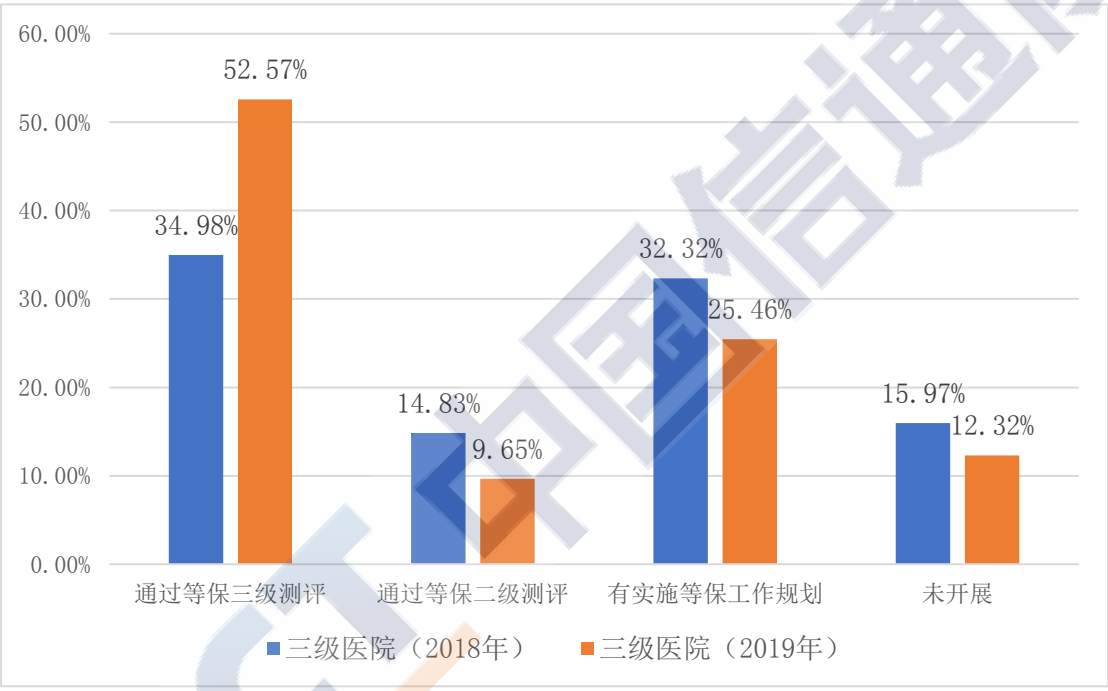
## （二）健康医疗行业安全政策研究

自 2017 年 6 月 1 日我国《网络安全法》实施以来，系列配套的法律法规和标准规范逐渐发布实施，形成相对完整的网络安全法律法规和标准体系。2019 年 5 月，公安部正式发布《信息安全技术 网络安全等级保护基本要求》等网络安全等级保护制度 2.0 相关的系列国家标准，针对新的安全形势提出了新的安全要求，标准覆盖度更加全面，安全防护能力有很大提升。2019 年 12 月，关键信息基础设施网络安全标准开展正式发布前试点，其在网络安全等级保护的基础上对卫生医疗等公共服务提出了更高的网络安全要求。2020 年 6 月，《关键信息基础设施安全保护条例》列入国务院 2020 年立法工作计划；同月，《数据安全法》和《个人信息保护法》列入全国人大常委会 2020 年度立法工作计划。7 月，《中华人民共和国数据安全法（草案）》（以下简称：《数据安全法（草案）》）面向社会公众征求意见，《数据安全

法（草案）》中指出“工业、电信、自然资源、卫生健康、教育、国防科技工业、金融业等行业主管部门承担本行业、本领域数据安全监管职责。”

作为数字医疗领域主管部门，国家卫生健康委员会近年来相继颁布一系列部门规章和规范性文件，推动健康医疗行业网络安全水平提升。2018 年 4 月，国家卫生健康委发布《关于印发全国医院信息化建设标准与规范（试行）的通知》，对二级及以上医院的数据中心安全、终端安全、网络安全及容灾备份提出要求。2018 年 9 月，国家卫生健康委发布《国家健康医疗大数据标准、安全和服务管理办法（试行）》，明确责任单位应当落实网络安全等级保护制度要求，对健康医疗大数据中心、相关信息系统开展定级、备案、测评等工作。同月，国家卫生健康委发布了《关于印发互联网诊疗管理办法（试行）等三个文件的通知》，明确要求互联网诊疗及互联网医院信息系统实施第三级信息安全等级保护，并向监管部门开放数据接口，支持实时监管。2019 年 3 月，国家卫生健康委发布了《关于落实卫生健康行业网络信息与数据安全责任的通知》，明确卫生健康领域网络信息与数据安全的职责分工和主体责任，推动建立和落实网络安全的工作领导责任制及相关方责任，严格执行网络信息与数据安全的责任追究制。2020 年 6 月，国家卫生健康委发布《关于做好信息化支撑常态化疫情防控工作的通知》中，强调要强化网络安全工作，切实保障个人信息和网络安全，落实网络安全责任，加大网络安全投入，加强网络安全防护和保障能力，组织网络安全宣传教育和培训。

随着国家级网络安全法律法规和标准规范的不断出台，以及健康医疗行业网络安全相关政策的相继发布，健康医疗机构及其从业人员网络安全意识不断增强，行业整体网络安全建设水平迈上新的台阶。以医疗机构网络安全等级保护实施情况为例，2019 年我国三级及以上医疗机构通过等保三级测评比例相比 2018 年显著提升，通过等保三级测评比例由 34.98%上升为 52.57%，具体数据如图 1 所示。




数据来源：中国医院协会信息专业委员会（CHIMA）

图 1 我国三级及以上医疗机构等级保护工作开展情况图

## （三）公共互联网的安全观测结果

为助力健康医疗行业更好地掌握和评估当前细分机构类别和地域的安全状况，研究团队基于中国信通院安全研究所产业互联网安全实验室技术能力，对医疗机构在公共互联网上的数字资产展开全方位实时安全观测扫描与量化评估，旨在为医疗机构了解自身与行业安全基线的差距提供支撑，为健康医疗行业加强安全建设、管理、运维等提供工作思路。

## 1．观测范围分布情况

本次观测行动通过公共互联网发起，共涉及健康医疗行业的15946 家相关单位，相比 2019 年新增 607 家单位。观测范围从职能划分上看，覆盖疾病预防控制中心（以下简称“疾控中心”）549 家，卫生监督所（以下简称“监督所”）332 家，卫生健康委员会（以下简称“卫健委”）432 家，医学会 170 家，公立医院 4531 家，私立医院 9933 家。结合《2019 年我国卫生健康事业发展统计公报》数据可知，本次观测公立医院和私立医院的覆盖率分别达 37.9%和 44.2%。观测总量较之 2019 年的 15339 家增长 3.9%，新增观测单位主要是公立医院和私立医院。观测范围按职能分布如图 2 所示。

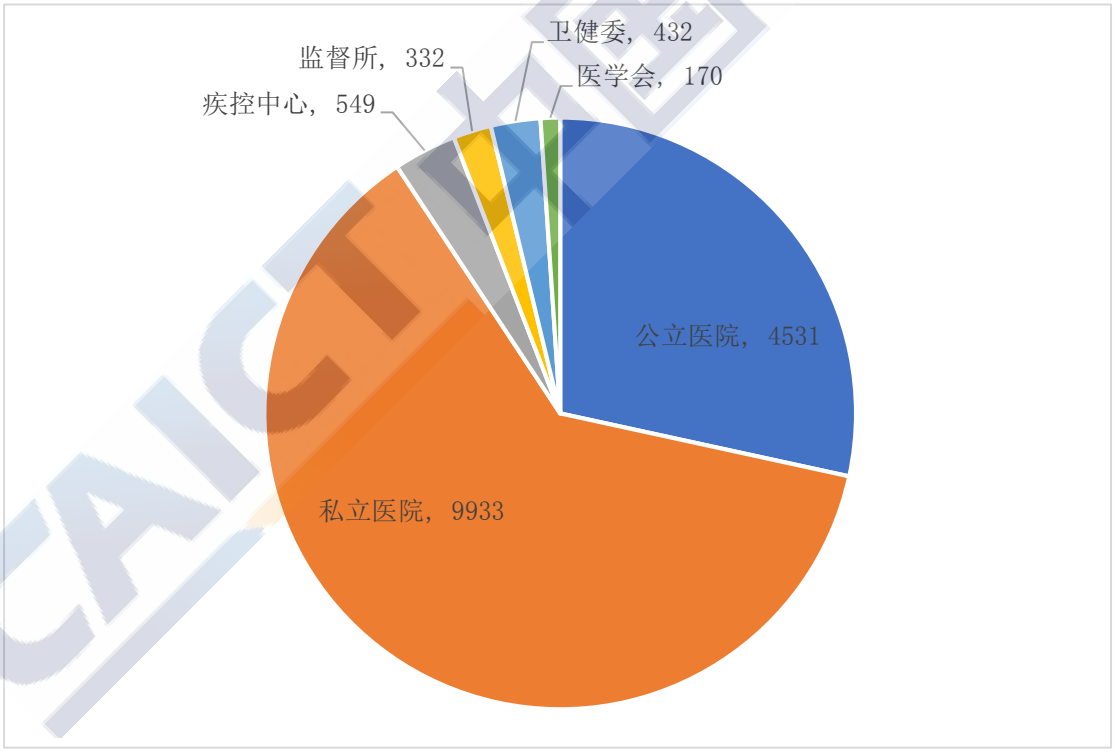



图 2 公共互联网安全观测范围-以职能划分的分布图

观测范围从地域划分上看，覆盖了全国除港、澳、台以外所有的 31 个省、自治区和直辖市。其中单位分布数量较多省份的分别是山东、四川、广东、江苏、河南、浙江，与 2019 年排名前六的省份完

全一致，前六省单位数量占观测单位总数比例达 40%，具体分布情况如图 3 所示。

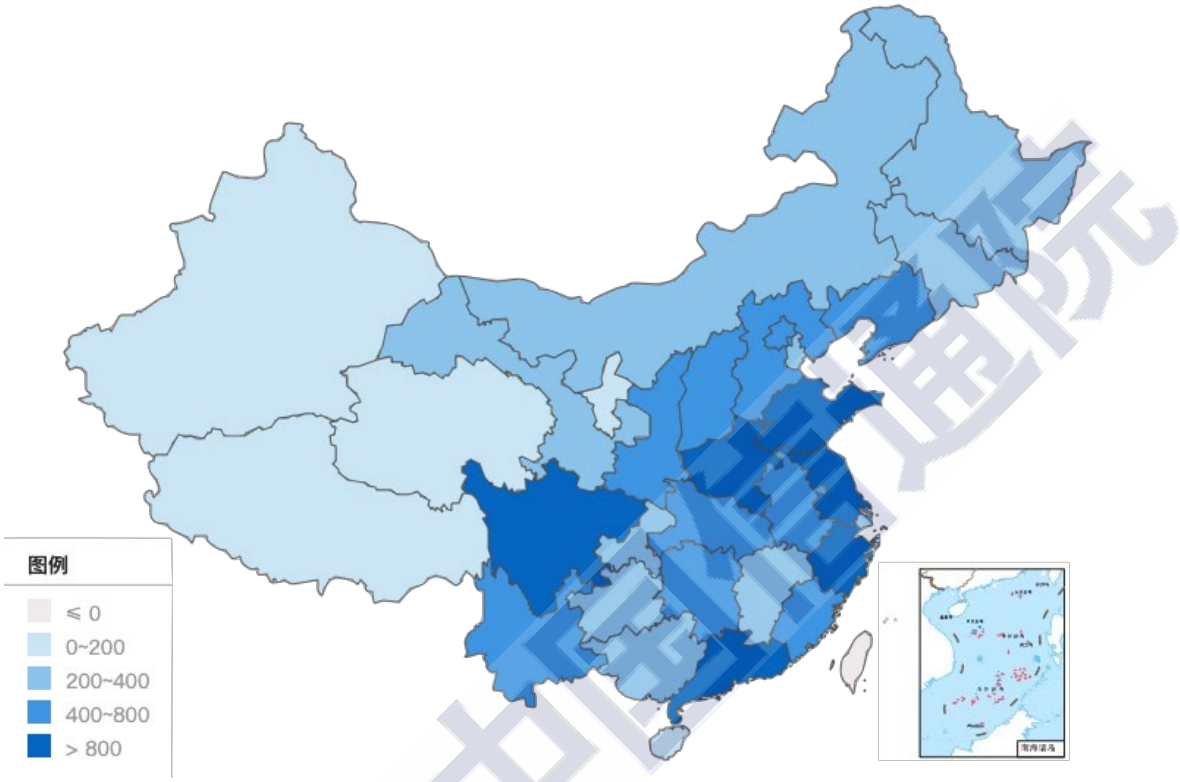



图 3 观测范围-以地域划分的分布图

## 2. 观测结果评估情况

经过持续性的公共互联网安全观测，本报告研究团队综合运用大数据、人工智能、威胁实时感知等技术和能力，全方位、多维度地梳理了健康医疗行业的网络安全现状及风险变化趋势，并采用风险量化的方法对观测结果进行了评估。本报告的风险分级沿用《2019 年健康医疗行业网络安全观测报告》中的分级标准，分别为重大风险（0-500 分）、较大风险（500-800 分）、一般风险（800-900 分）和低风险（900-1000 分），具体网络安全风险分级请见附录 A。分数越高，网络安全风险越低；分数越低，网络安全风险越高。

本次观测健康医疗行业整体评分为 842 分，总体行业处于“一般

风险”的风险级别，具备了基础的安全防护能力，但仍存在较多的网络安全风险及可以被利用的安全隐患。行业整体安全评分相较 2019 年有一定提升，表明行业整体在公共互联网方面安全防护意识加强，安全防护技术和手段有了一定程度提升。各省份风险量化评估结果分布如图 4 所示。

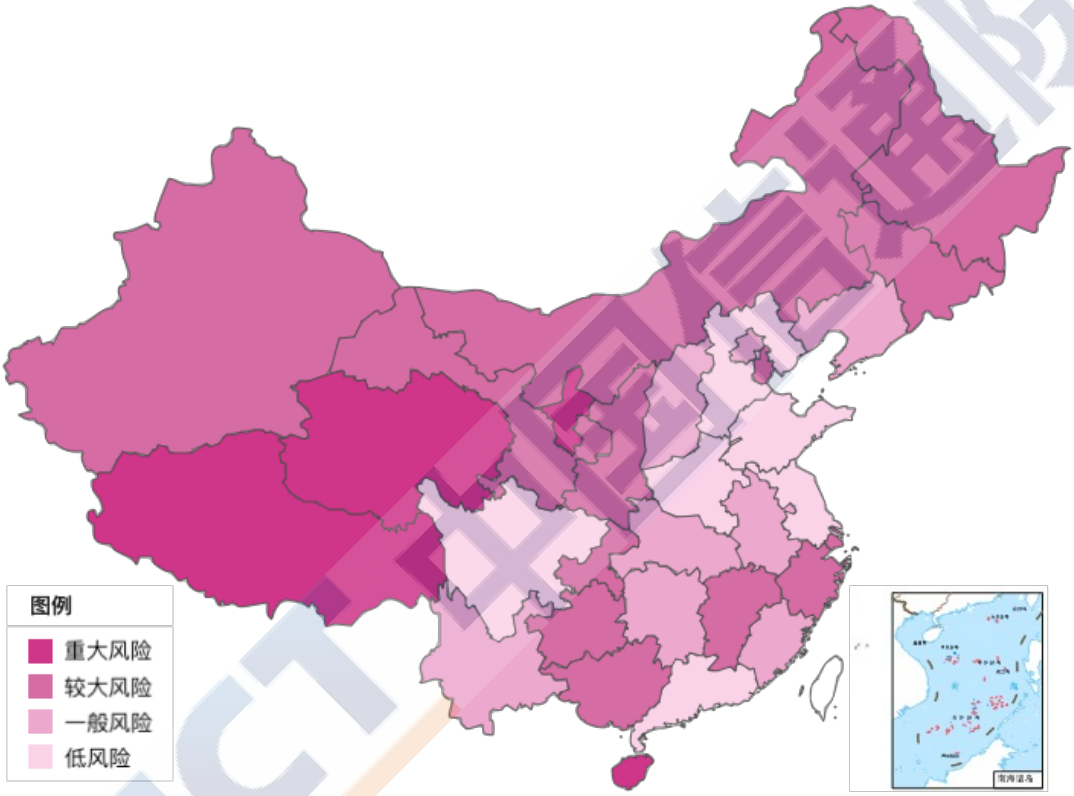



图 4 各省份风险评估结果分布图

风险级别为“低风险”的省份有：山东省、四川省、广东省、江苏省、河南省、河北省；

风险级别为“一般风险”的省份有：北京市、辽宁省、安徽省、山西省、福建省、云南省、湖南省、湖北省；

风险级别为“较大风险”的省份有：上海市、重庆市、天津市、浙江省、吉林省、黑龙江省、内蒙古自治区、新疆维吾尔族自治区、甘肃省、江西省、广西壮族自治区、贵州省、陕西省；

风险级别为“重大风险”的省份有：海南省、西藏自治区、宁夏回族自治区、青海省。

## 二、公共互联网的安全风险分析

当前，伴随着产业互联网逐步进入发展深水区，医疗数据与应用服务由内网向公网、云融合转型升级的速度也在不断加快。新基建背景下，互联网医疗或将迎来井喷式发展。医疗上云在极大提升优质医疗资源利用率，推动民生改善的同时，也会导致医疗业务和数据的暴露面大幅增多，进而使健康医疗行业面临更为严峻的安全形势。

2019 年以来，加拿大某医疗机构 270 万个医疗录音文件遭黑客公开、印度 1250 万份孕妇医疗记录被公开泄露，以及我国新冠肺炎抗疫用户数据和实验资料遭黑客窃取并暗网售卖等大型医疗网络安全事件的相继爆发，反映出健康医疗行业面临的巨大网络安全威胁。根据 Ponemon Institute 数据显示，医疗数据泄露的平均成本为每条记录 380 美元，是全球全行业平均数据泄露成本的 2.5 倍。而医疗机构因服务器遭勒索病毒攻击导致系统瘫痪，影响患者就医等事件的发生，也进一步表明，医疗行业在公共互联网环境下所受的威胁冲击不仅影响着行业业务和数据资产的安全，还可能透过医疗应用服务对大众生活产生影响，触及人民群众生命安全的保护面。

安全漏洞、僵木蠕毒、网站篡改等层出不穷且花样百出的渗透攻击，仍是医疗行业公共互联网安全面临的主要威胁。不管是从健康医疗行业升级发展的角度，还是从夯实人民群众生命安全堡垒的角度，全面提升健康医疗行业在数字化时代的安全防护能力和防护水平已成为行业共识。对健康医疗行业在公共互联网环境下的安全风险进行的全面透析则，成为升级医疗行业风险防御能力，打造适配安全解决

方案的基础所在。

## （一）资产脆弱性问题现状及趋势对比分析

健康医疗数据具备高真实度、完整度和私密性等特性，其与医疗业务开展有着不可分割的关系，也是医疗上云后的核心数字资产。随着医疗机构信息化程度的不断提升，数字资产体量和价值日益加码，随之而来的是黑产的网络攻击持续升级。然而，健康医疗行业网络安全防护体系仍相对薄弱，系统漏洞无法及时修复、补丁更新延迟等现象大量存在。根据中国医院协会《2018-2019 年度中国医院信息化状况调查报告》结果显示，目前我国大多数医院的网络安全防护设备较为缺乏，绝大多数医院仅采用防火墙保障网络安全，对网闸、防侵入、防毒墙等设备的应用率均小于 50%。换言之，攻守能力失衡，使得用以衡量医疗数字资产安全隐患的资产脆弱性问题仍处于较高水平。从某种程度上来讲，医疗的网络安全战场本质上是一个数据战场。因此，资产脆弱性作为攻击产生的入口，成为本次观测评估的首要问题。

本次观测关于资产脆弱性的评估着重集中在敏感服务及高危端口直接暴露在公共互联网和具有公开漏洞的低版本服务两大方面。结果显示，在本次观测的 15946 家医疗单位中，共有 8145 家单位存有资产脆弱性风险，占比达 51.07%。资产脆弱性问题相比 2019 年的 62.14%有所下降，一定程度上体现出行业资产脆弱性问题的态势好转，但该问题在医疗单位中仍然普遍存在，需要进一步关注和推动解决。夯实资产原生屏障，提升资产自身“免疫力”仍是健康医疗信息化提升安全水平的首要挑战。

## 1. 高危端口与敏感服务暴露风险大幅下降，数据服务威胁仍占主导

作为 Web 应用的入口，端口承担着“安全守门者”的角色，其安全性直接关乎敏感数据、服务器命令及权限的正确执行。本次观测数据显示，共有约 4000 家医疗单位涉及高危端口风险，与 2019 年的 7000 家单位相比，下降了 42.85%。高危端口开放带来的安全风险大幅下降，相应安全防护水平普遍有所提升。就开放高危端口类别来看，现存代表数据库的 3306 端口风险的单位数目仅为 2019 年的一半，而存有严重远程连接漏洞风险的 3389 端口风险由 2019 年的 1860 家下降为当前的 492 家，具体数据如图 5 所示。可见，医疗单位在高危端口及敏感服务暴露风险方面有了较大改进，相应防护意识和防护能力有所增强。

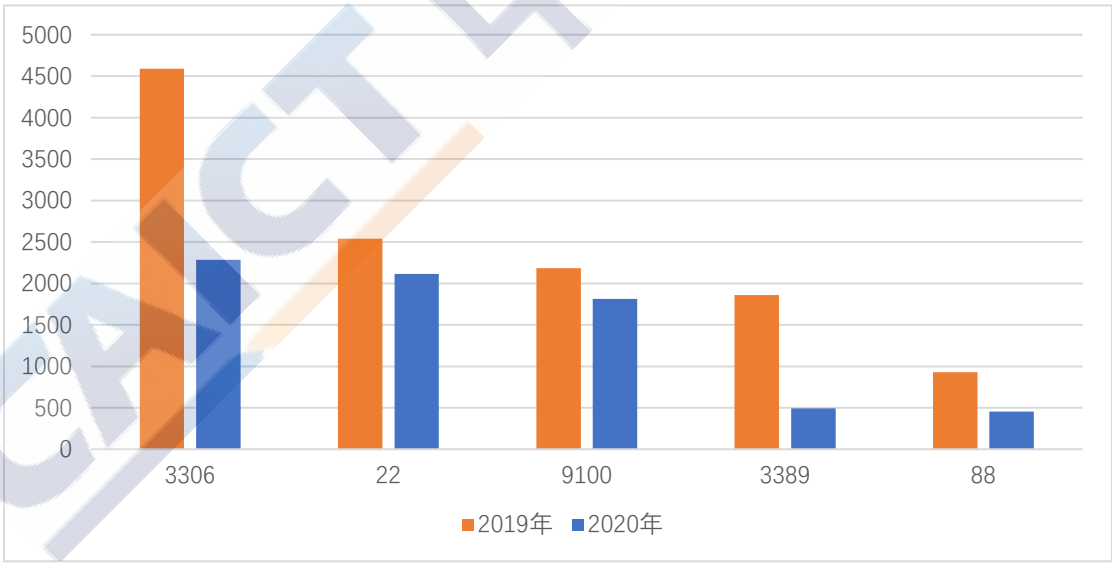



图 5 存有高危端口风险单位数对比图

健康医疗服务涉及大量敏感个人信息，包括患者姓名、手机号、身份证号、家庭住址、网络 ID 等个人身份信息以及挂号记录、检查检验报告、住院记录、体检报告、缴费记录等就医诊断信息，呈现出

高敏感性的特点。而这些服务与公共互联网侧的远程登录、数据库、FTP、打印机等服务的嫁接，可能带来更大的安全隐患。例如敏感服务端口被攻破可能成为攻击者实施进一步攻击的跳板，进而导致大面积的医疗数据泄露，直接影响医疗机构业务连续性，甚至给患者带来足以危及生命安全的严重损失。本次观测数据显示，2020 年度的敏感服务威胁主要来源于 FTP、MySQL、ssh、jetdirect、ms-wbt-server 等五项服务，具体数据如图 6 所示。其中，虽然威胁数量较之 2019 年有较大幅度下降，但仍有近半数医疗机构存在以 FTP、MySQL 为代表的数据服务暴露隐患，数据服务暴露问题仍然是医疗机构面临的主要资产脆弱性问题。

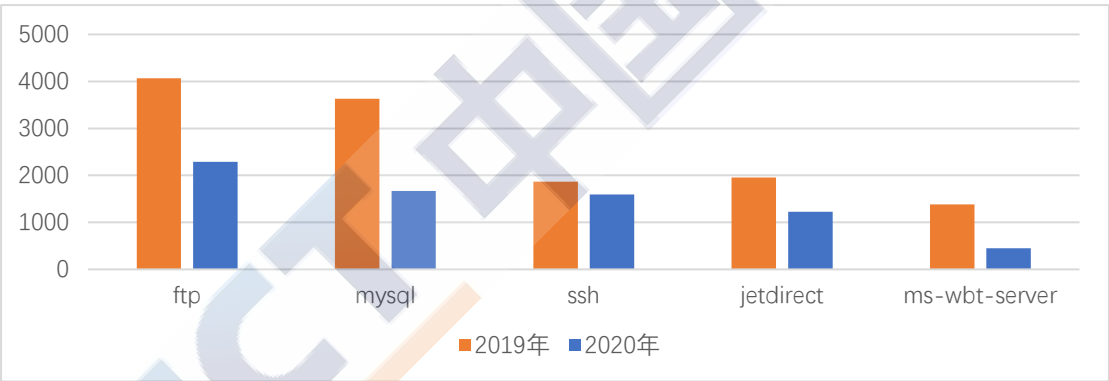



图 6 敏感服务风险单位数对比图

从各省维度分析，2020 年各省医疗单位存有的高危端口开放和敏感服务暴露的安全隐患数量上均低于 2019 年，一定程度上反映出各省医疗单位在解决此类安全风险方面皆有所精进。各省风险变化对比情况如图 7 所示。

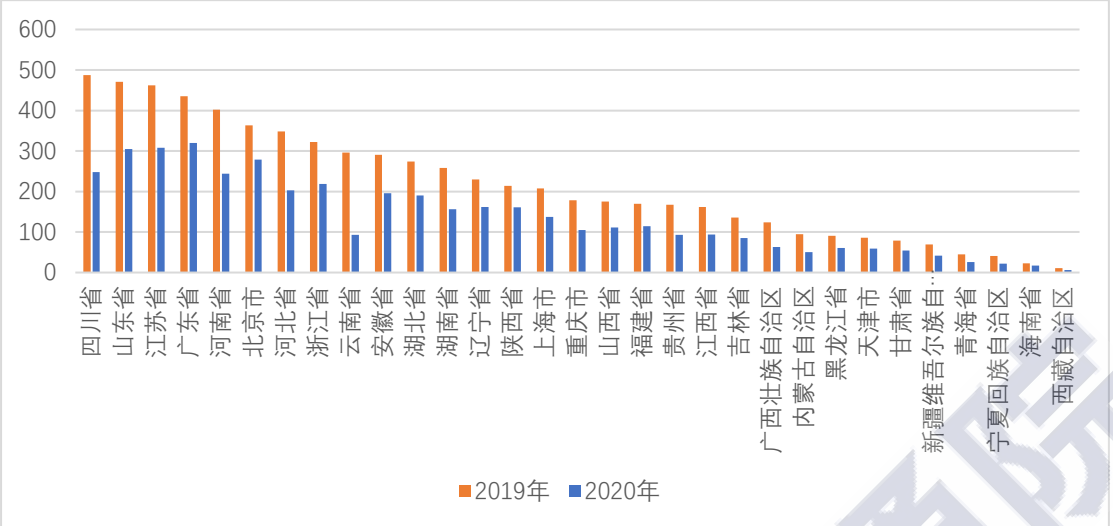



图 7 高危端口及敏感服务风险单位省份分布对比图

### 2. 服务版本过低风险占比已低于三成，主动防御仍需加强

除高危端口开放和敏感服务暴露问题外，医疗机构在互联网应用服务方面普遍存在组件版本升级滞后的问题。服务版本过低与持续升级的安全风险之间的能力失衡，给公共互联网环境下的健康医疗机构带来了更为严重的威胁。本次观测中，共有 4145 家单位涉及应用服务组件版本过低的问题，占比约 26%，相比 2019 年的 38%有所下降，但整体上仍居高位。从分省份情况可以看到，大部分省份应用服务版本过低风险涉及单位数量呈现下降趋势，如图 8 所示。为应对此问题，医疗机构应加强自身系统及设备的安全升级机制与流程建设，从主动防御角度出发，注重与安全服务升级联动，构筑更为有力的资产防护“壁垒”。

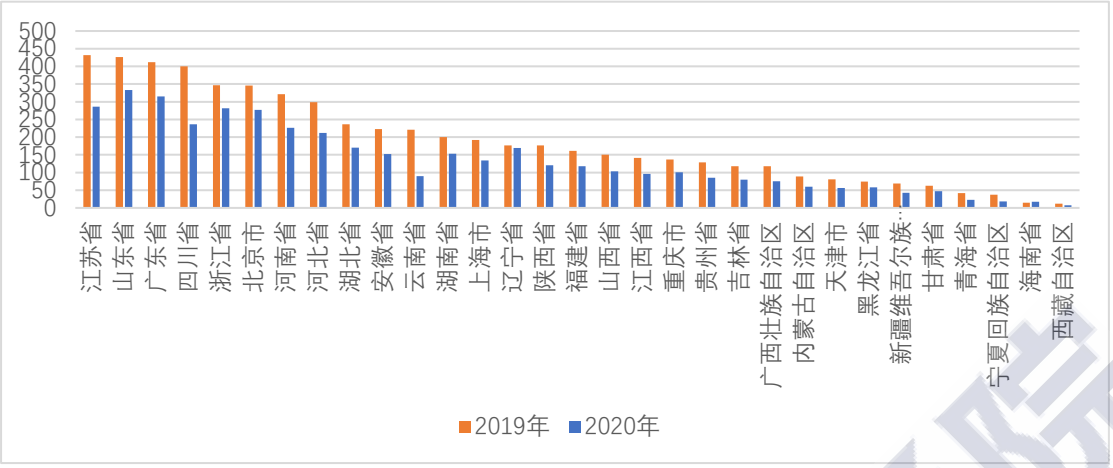



图 8 服务版本过低风险涉及单位各省份分布对比图

## （二）安全漏洞问题现状及趋势对比分析

随着健康医疗业务向公共互联网开放程度的提升，以手机 APP、网站、第三方医疗服务平台为载体的在线医疗服务如雨后春笋般涌现，并构筑了较之传统医疗服务更为复杂的应用环境。据腾讯安全早期调查数据显示，在拥有较成熟线上医疗服务的医院中，有超过 60% 医院的线上服务是搭载在第三方医疗平台上。而受资源汇集、安全能力限制等多方面因素的影响，第三方医疗平台存有的安全漏洞无疑给医疗机构线上业务和数据带来了更大的安全压力与挑战。一旦平台出现高危安全漏洞将对平台上所有医疗机构带来安全危机。

通过渗透测试，本次观测共发现 1216 个安全漏洞，涉及医疗单位 653 家，占观测对象总数的 4%。其中高危漏洞涉及单位 398 家，中危漏洞 229 家，低危漏洞 260 家，漏洞分布如图 9 所示。

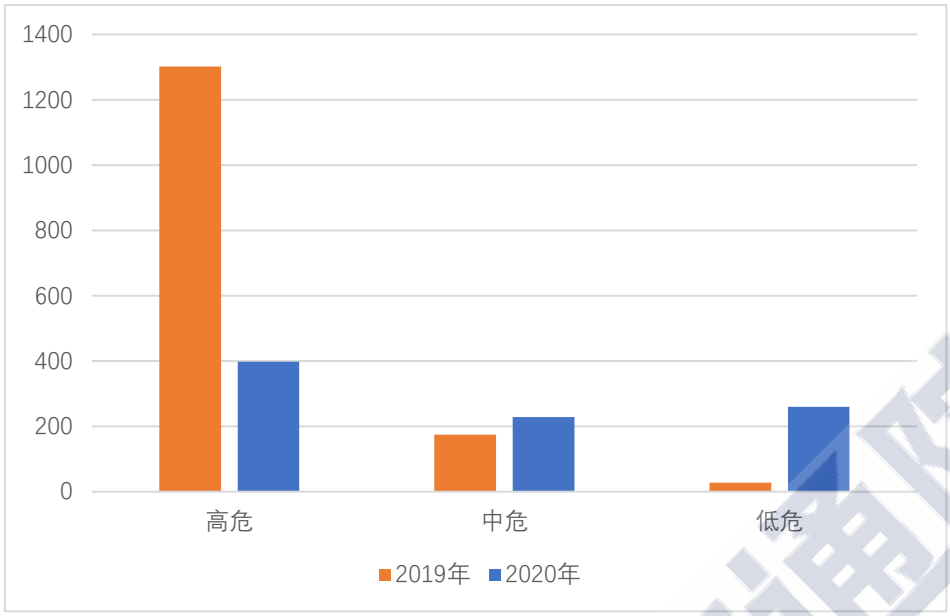



图 9 安全漏洞风险级别分布对比图

对比 2019 年观测结果，漏洞涉及单位由 1302 家到 653 家下降了近一半。其中高危漏洞降幅较大，占比已不到 1/3，分析主要原因是由于远程桌面服务远程执行代码漏洞（CVE-2019-0708）的数目的大幅下降，由 2019 年的 1012 家下降到 2020 年的 74 家，说明医疗机构及其服务厂商对此高危漏洞问题给予了较高的重视。与此同时，HTTP 协议远程执行代码漏洞、弱密码问题以及易引发数据泄露风险的通信协议漏洞成为当前健康医疗行业面临的三大高危漏洞，需要相关机构予以关注和解决，具体影响单位如图 10 所示。

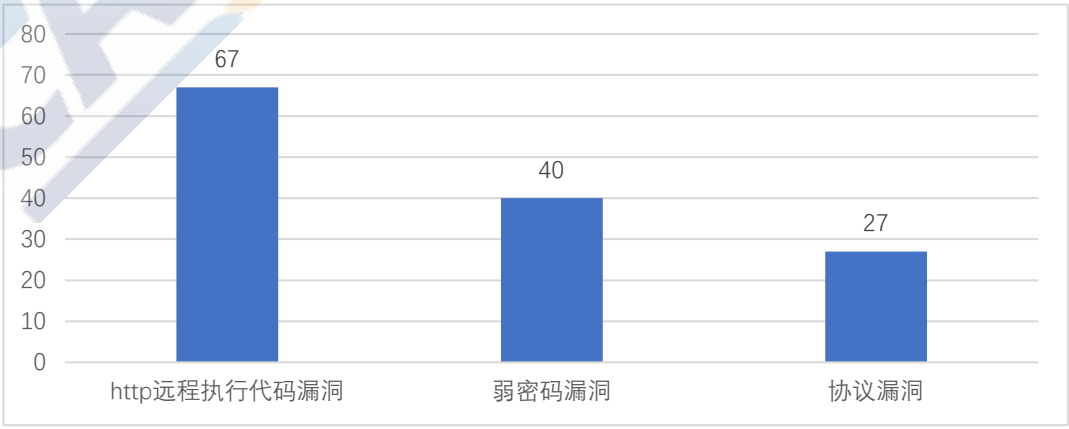



图 10 高危漏洞 Top3 分布图

各省市存有安全漏洞单位数目分布略有变化，但总体安全漏洞数量呈现下降趋势。2020 年，江苏、浙江、山东、安徽替代广东、山东、江苏、四川成为安全漏洞单位数目最多的四个省份，具体各省份漏洞变化情况如图 11 所示。

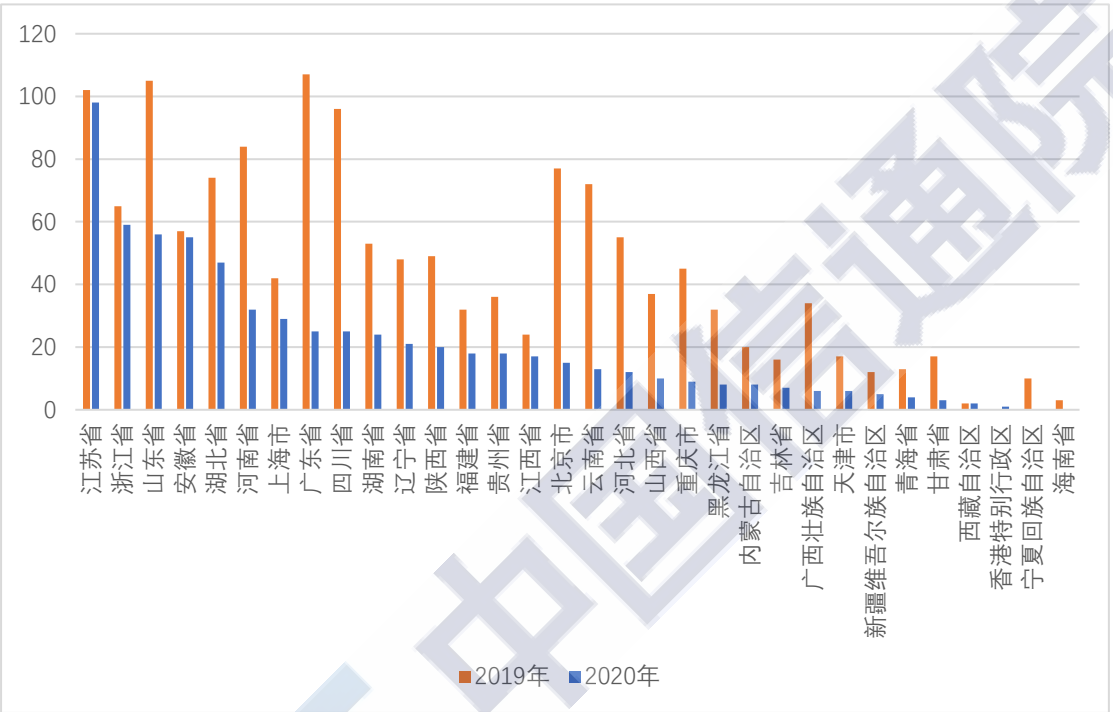



图 11 安全漏洞涉及单位省份分布对比图

从整体来看，受困于安全漏洞威胁的医疗单位数目呈现下降趋势，但仍有相当数量的中高危漏洞未得到及时修复。面对无孔不入的安全漏洞攻击与入侵，医疗机构应尽快构筑风险监测预警和响应修复的安全体系，定期开展风险评估和漏洞扫描，建立安全漏洞管理和跟踪机制，及时封堵和修补漏洞，避免因安全漏洞问题带来的严重后果。

## （三）僵木蠕毒问题现状及趋势对比分析

基于健康医疗数据高敏感性和多系统、多领域关联的特点，随着医疗业务服务与应用向外网的转移，在寻找到端口、敏感服务以及安全漏洞等“攻击点”后，医疗黑产多采用植入僵尸病毒、木马、蠕虫

以及勒索病毒等方式实现对相关医疗数据的窃取和深层次挖掘，甚至以此为跳板，实现对患者信息和医院业务数据的窃取与售卖等。为描绘出健康医疗行业在公共互联网环境下的安全威胁全貌，研究团队持续观测和分析了健康医疗行业面临的僵木蠕毒等恶意程序入侵风险。

在本次观测中，共有 962 家单位被检测出存有僵木蠕毒感染风险。勒索病毒、远控木马、挖矿木马、流氓软件与广告依旧为四类重点风险，分别涉及 96 家、283 家、253 家和 170 家医疗单位。对比 2019 年，整体数量有所上涨，但重点风险数目皆有不同程度的下降，如图 12 所示。

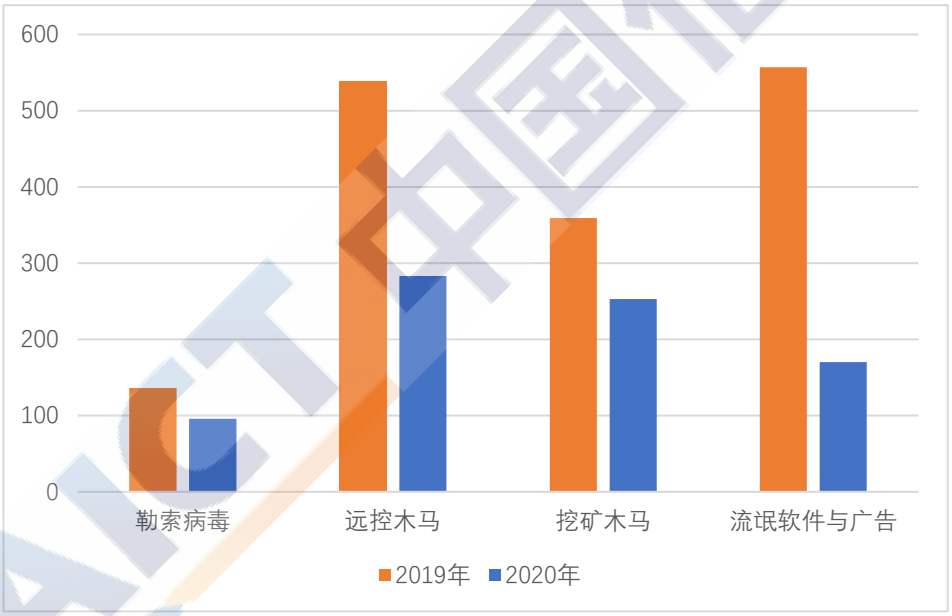



图 12 四类重点僵木蠕毒风险涉及单位数目对比图

除以上带有明确目的的破坏性僵木儒毒恶意文件外，还存在一类通用恶意僵木儒毒文件。该类文件存在通用安全定义上的一些恶意行为，例如木马、漏洞利用、与恶意域名通信等，但尚未表现出带有明确目的的破坏性行为，如勒索、挖矿等。2020 年感染此类恶意文件单位为 880 家，相比 2019 年的 727 家有一定幅度上涨，如图 13 所示。

尽管此类僵木蠕毒恶意文件尚未造成明显破坏，但其潜藏的风险可能造成的问题难以估量，需要医疗机构尽快予以定位和处置。

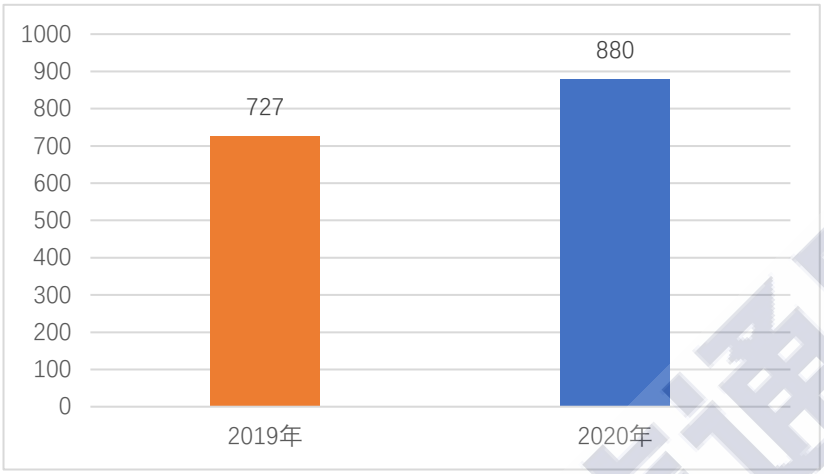



图 13 通用僵木蠕毒恶意文件感染单位变化图

从地域分布上来看，除北京市外，各省僵木蠕毒风险涉及单位数目均有不同程度的上升。其中，广东、江苏、浙江、山东、四川占比最高，五者中涨幅最大的浙江替代湖北成为 TOP5 之一，具体数据如图 14 所示。僵木蠕毒仍是各省医疗单位面临的主要安全问题。

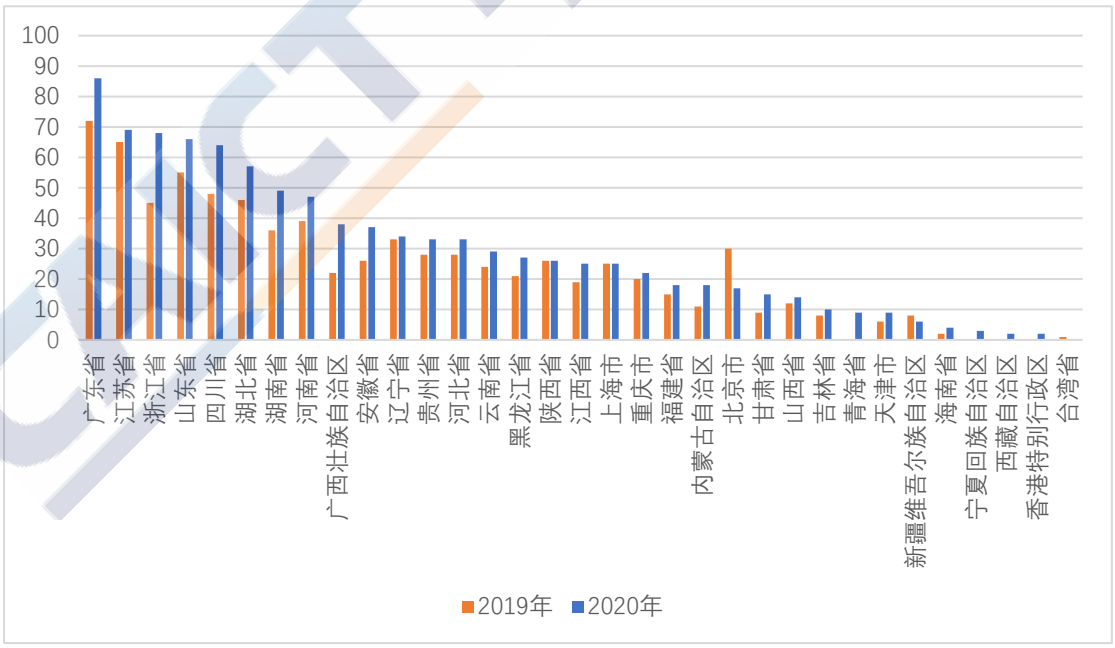



图 14 僵木蠕毒地域分布对比图

在四类重点风险中，远控木马、挖矿木马、流氓软件与广告的影

响单位范围虽远大于勒索病毒，但其破坏性和危害度却远不及医疗行业的最大“毒瘤”——勒索病毒。Verizon《2019 年数据泄露事件调查报告》显示，勒索软件攻击已连续第二年占据 2019 年医疗保健领域所有恶意软件事件的 70%以上。医疗行业信息系统数据价值高、业务连续性要求强是勒索病毒“偏爱”医疗行业的主要原因。通过骚扰、恐吓甚至采用绑架用户文件等方式，使用户数据资产或计算资源无法正常使用，并以此为条件向用户勒索钱财,是勒索病毒的惯用手法。作为医疗行业的“流行病”，勒索病毒仍在持续变种迭代中。加强包括软件漏洞、RDP 弱口令暴力破解、钓鱼邮件、网页挂马等在内的勒索病毒传播端的安全防护，是医疗机构实现机密文件和数据风险最小化的重要着力点。

此外，《2020 数字医疗:疫情防控期间网络安全风险研究报告》数据显示，新冠疫情期间，僵尸、木马、病毒等恶意程序感染风险更高，健康医疗行业随疫情爆发迎来在线业务快速发展趋势的同时，也面临着更为严峻的安全态势，提高整体安全防护意识和建立更高级别的安全防护手段成为行业共同诉求。

## （四）网站篡改问题现状及趋势对比分析

在线健康医疗服务的普及与应用，使得网站已然成为医疗机构开展公共服务和彰显公众形象的重要窗口与平台。与此同时，由于医疗机构网站具有精准的触达圈层和广角，导致其成为不法攻击者实施欺诈的重要介质。对于医疗机构而言，网页一旦被篡改，除了给机构形象和信誉带来严重损害外，还有可能导致由错误信息传播带来的患者

恐慌与损失，甚至带来危及患者生命安全的严重后果。因此，在有效检测网站篡改风险的基础上，及时制定出防篡改策略并实施，是确保健康医疗在公共互联网环境下安全发展的重点。

本次观测共发现 2083 家单位存有网站篡改风险，其中被篡改为博彩的单位 1776 家，被篡改为色情的单位则有 566 家。从涉及单位数量趋势上看，2020 年与 2019 年相比有明显上涨，涨幅超 70%。这一差距主要来源于 2020 年检测引擎能力的升级，增强了网站篡改检测的敏感词库。观测结果体现出健康医疗网站上存在较多的敏感内容，其中超过 84%的网站篡改风险均出现在私立医院网站，私立医院亟需加强其网站安全管理，及时检测和修复篡改问题。在地域分布上，山东、四川、江苏、北京、河南、广东等医疗大省被观测到的网站篡改风险较多，详细数据如图 15 所示。

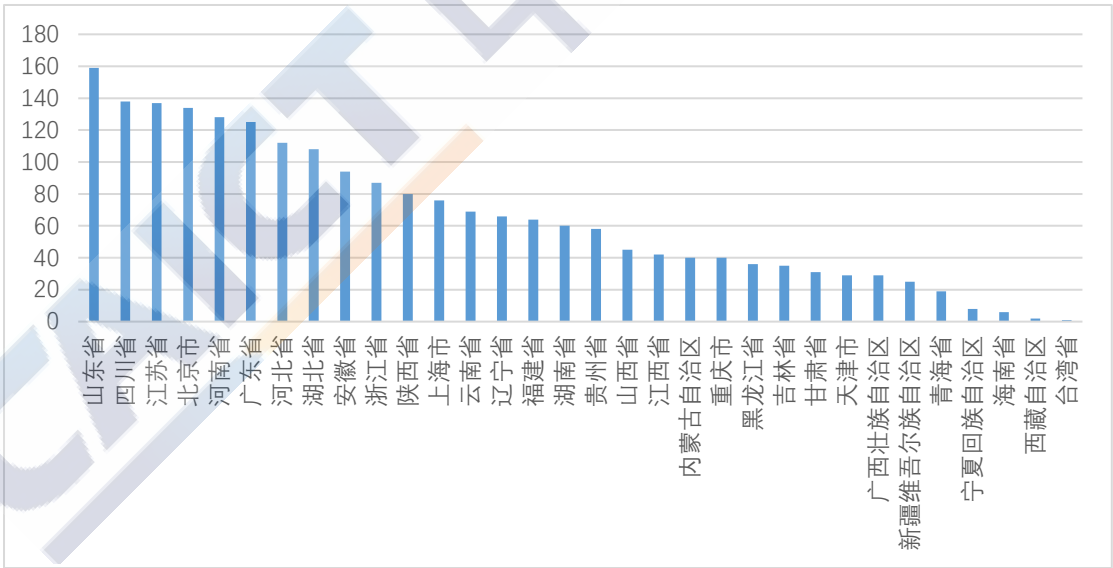



图 15 网页篡改问题涉及单位省市分布图

基于对篡改数据的分析发现，以植入色情、博彩、诈骗等非法信息为主要方式的隐式篡改仍是医疗行业网站篡改问题的主流手段。在当前互联网医疗服务快速发展的形势下，医院官方网站将越来越多地

受到公众的关注和使用，提升公共互联网环境下网站应用的风险感知和实时防御能力，是健康医疗行业安全建设的重点方向。

# 三、医疗机构安全风险对比分析

随着互联网医疗、智慧医院、远程诊疗等新型医疗业态的快速发展，健康医疗机构及服务呈现多元化发展趋势。不同类别机构及业务由于业务特点、承载平台等的差异，其业务环境和面临的安全风险也各有不同。如互联网医院与非互联网医院因业务服务模式的差异，形成了不同的业务应用布局。互联网医院较之非互联网医院在公共互联网上拥有更多的应用服务和数据接口，其公共互联网安全暴露面更大，进而可能面临着更多的网络安全风险。公立医院与私立医院因业务规模、管理模式和考核机制的不同，导致其业务侧重的差异，也可能面临不同的网络安全挑战。

为更好地评估各细分类别的医疗机构面临的网络安全风险，以协助相关机构制定更具场景适用性的安全策略，实现防护效果最大化，研究团队着重对互联网医院与非互联网医院、公立医院和私立医院的安全风险开展了对比分析。以期为相关医疗机构提升安全防护措施的精准性和有效性，为针对性地解决场景安全问题提供参考与依据。

## （一）互联网医院与非互联网医院的安全对比分析

我国互联网医疗自诞生以来经历近 20 年的发展。近年来，随着新基建上升为国家战略并向各行各业渗透，互联网医疗等新型医疗服务作为融合基础设施迎来新一轮的发展契机。尤其是在 2020 年新冠肺炎疫情暴发后，线下诊疗渠道受阻，导致医疗资源紧张，进一步加快了互联网医疗的发展进程。从在线问诊、快速筛查到在线处方和医保在线结算，互联网医疗打破空间局限，成为科技“战疫”先锋，也

因此成为国家和地方致力推动卫生健康事业发展的政策倾斜重点。据动脉网和蛋壳研究院发布的《乘新基建之风，防疫常态化下互联网医院的价值归宿》报告显示，截止到 2020 年 6 月，国家和地方共发布了 126 条互联网医院相关政策，覆盖互联网医疗业务规范、监管对接、医保结算等多个方面；2020 年上半年各地已审批设立互联网医院近 600 家，新建互联网医院数量接近 2019 年全年数量；2020 年上半年全国已有 29 个互联网医院中标项目，超过 2019 年全年总量。可见，从政策利好到项目支撑，互联网医院将成为健康医疗行业未来重点发展方向。据前瞻产业研究院及健康界研究院预测，到 2020 年，中国互联网医院市场规模有望突破 1000 亿元人民币。

然而，据健康界研究院发布的研究报告显示，在互联网医院建设运营过程存在的问题及面临的挑战中，患者就诊数据安全得不到保障提及率高达 40.5%，位列互联网医院建设运营问题前五。就目前来看，互联网医院主要以实体医疗机构互联网医院和依托实体医疗机构独立设置的互联网医院为主要存在形式，即互联网医院建设必须依托实体医疗机构开展。因此，研究团队对互联网医院与非互联网医院进行的安全风险对比分析，一方面旨在分析和挖掘互联网医院在公共互联网上面临的网络安全风险特点和变化规律；另一方面期望为互联网医院和非互联网医院制定高精准度安全防护策略提供思路和建议。

本次观测主要从资产脆弱性风险、僵木蠕毒感染风险、网站篡改风险以及安全漏洞风险等维度进行对比分析，并对互联网医院和非互联网医院的风险现状进行了安全量化评分。安全评分显示，非互联网

医院的整体安全评分（859 分）略高于互联网医院（834 分），两者的总体风险值均处在“一般风险”级别，与行业总体评分差距不大。

从细化风险维度分析，34.27%的非互联网医院存在资产脆弱性的安全隐患，这一比例高于互联网医院的 19.35%，一定程度上反映出互联网医院在安全基线方面建设相对更好。在安全漏洞方面，互联网医院存在安全漏洞的医院比例为 6.05%，略高于非互联网医院的 4.02%，推测与互联网医院在公共互联网提供较多应用服务有一定相关性。在衡量实际被攻击的僵木蠕毒感染风险和网站篡改风险层面，互联网医院和非互联网医院呈现较为明显的差异，其中互联网医院的僵木蠕毒感染风险明显高于非互联网医院，而其网站篡改风险明显低于非互联网医院。由于网站是互联网医院的重要服务载体，很多用户需要通过网站访问互联网医院服务，互联网医院对其防护较好，而非互联网医院的网站访问人数相对较少，防护能力也可能较弱，这一点上与预期相对一致。与此同时，互联网医院存在大量被僵木蠕毒等恶意程序感染和入侵的风险，推测可能由于互联网医院在公网信息系统上存在较多高价值数据，招致各类不法分子的觊觎和攻击。可见，僵木蠕毒感染风险是互联网医院需要重点监测和防控的安全问题。详细数据如图 16 所示。

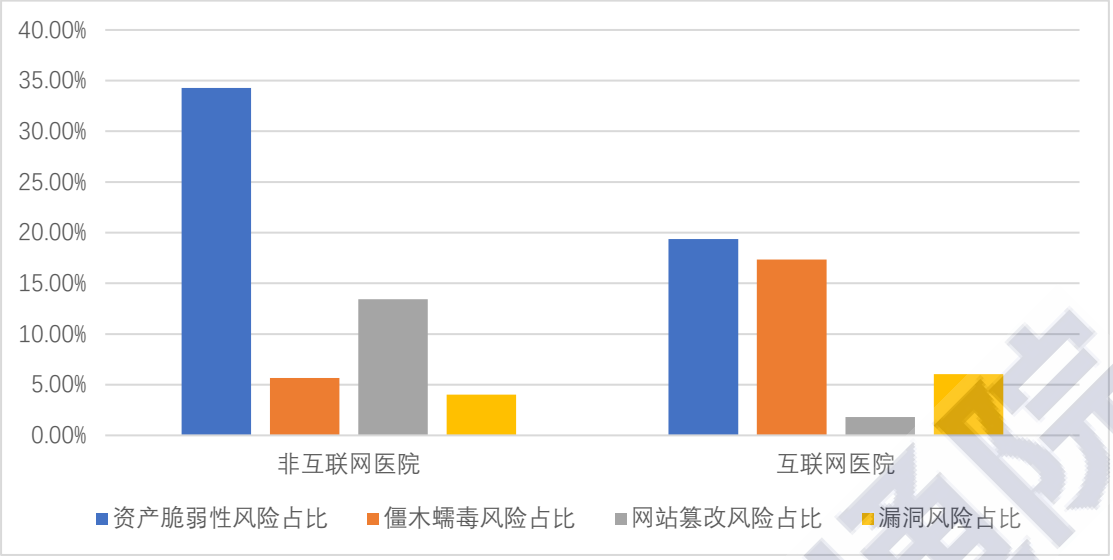



图 16 互联网医院和非互联网医院风险占全部医院风险比例图

基于以上分析可知，互联网医院在资产脆弱性防护方面相对非互联网医院做得更好，其安全意识相对更强，网站等可见的互联网业务服务安全风险较小。然而，由于业务系统开放在公共互联网，互联网医院显然承受着更大的网络攻击压力，各类用户不可见的僵木蠕毒等恶意程序实际入侵的风险很高，可能带来数据泄露或业务瘫痪等严重后果，亟需互联网医院管理者和安全人员关注和重点防控。互联网医院相对传统医疗具有不同的业务和风险特点，需要有相应融合场景的安全标准规范予以进一步规范和指引。

## （二）公立医院与私立医院的安全对比分析

综观国家卫生健康委发布《2019 年我国卫生健康事业发展统计公报》数据可知，公立医院与私立医院依旧是我国医疗卫生资源的中坚阵地。在新基建和产业上云趋势的共同推动下，无论是公立医院还是私立医院都在加快业务“上线”的节奏，以适应当下大众日益增长的在线医疗服务需求。当前，很多公立医院依托于院内 HIS 系统搭建线上业务体系，并以 APP 为主要切入载体，而私立医院则多采用微

信公众号或服务号为切入载体，不同形态的线上服务模式可能衍生出不同的安全风险。研究团队对公立医院与私立医院的安全情况进行了对比评估与分析，以期在剖析两者安全风险差异的基础上，针对性提出两类医疗机构网络安全工作的思路和建议。

在剖析公私立医疗机构安全风险上，研究团队继续从资产脆弱性、僵木蠕毒、网站篡改以及漏洞四个风险维度进行探究。从总体安全评分上，私立医院总体风险评分为 872 分，略高于公立医院的 805 分，两类医疗机构均处于“一般风险”级别，与行业总体处于同一风险级别。

在具体风险维度上，两者在资产脆弱性的风险占比基本持平，安全漏洞风险差别不大；但公立医院的僵木蠕毒风险远高于私立医院，而私立医院的网站篡改风险则为公立医院的 2.5 倍以上，具体数据如图 17 所示。

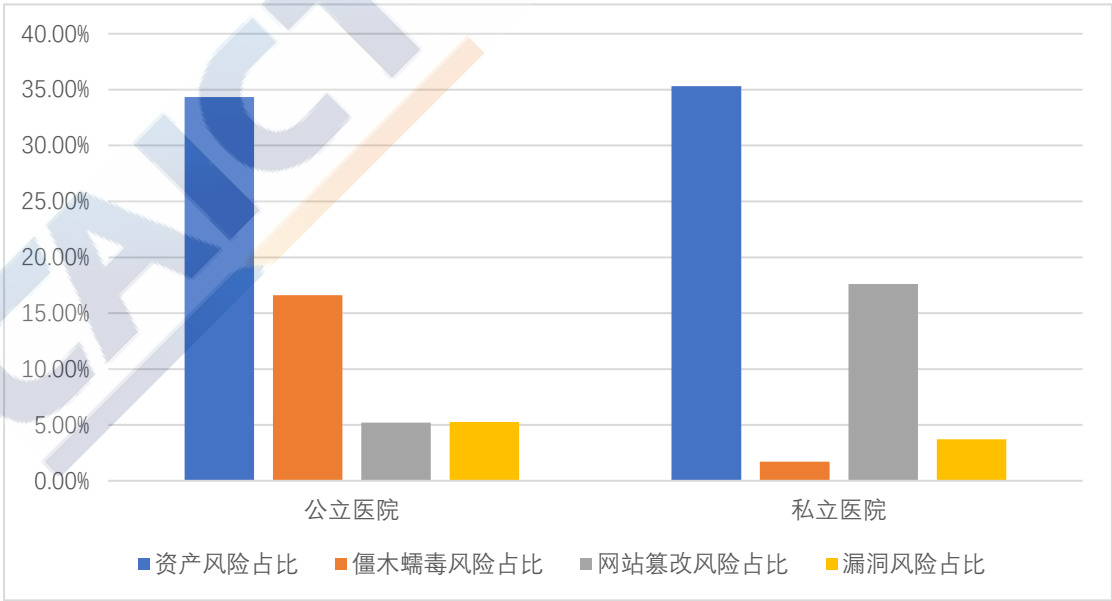



图 17 公立医院和私立医院风险占全部医院风险比例图

虽然在公立医院与私立医院在安全漏洞风险整体占比上差异不

大，但深入分析漏洞类型可以发现，存在高危漏洞的私立医院数量明显高于公立医院，而公立医院的安全漏洞则主要以中低危漏洞为主，说明公立医院在安全漏洞防护方面要强于私立医院，具体数据如图 18 所示。

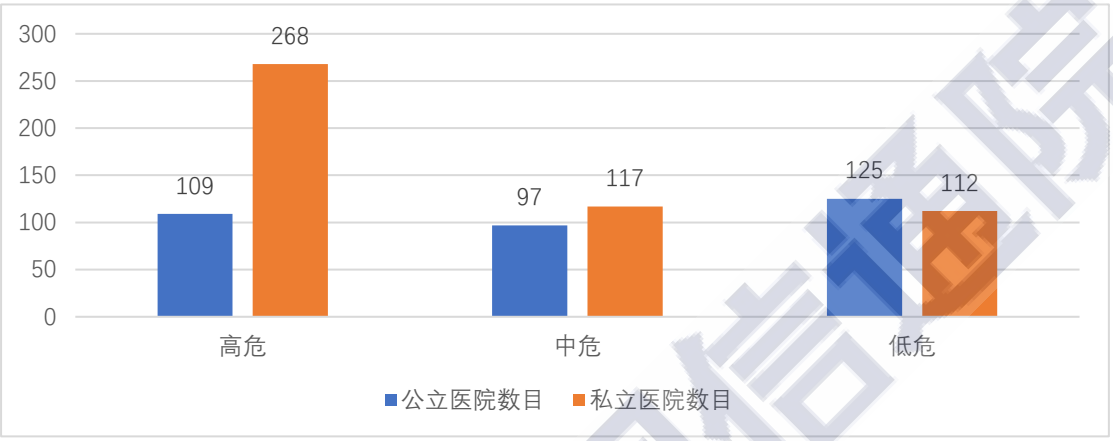



图 18 2020 年公立医院和私立医院安全漏洞分类对比图

基于以上数据分析可知，在基础安全防护方面，公立医院和私立医院均处于较差水平，但公立医院安全漏洞防护要优于私立医院；在遭受安全攻击方面，公立医院与私立医院各有特点，公立医院主要承受僵木蠕毒等恶意程序感染入侵压力，而私立医院主要受到网站恶意篡改等问题困扰。

# 四、健康医疗安全工作思路与建议

## （一）主管部门应重点推动行业规范发展

### 1、健全标准体系，落地安全规范

融合行业场景的安全标准体系建设对于行业安全建设具有重要的前瞻性和指引性作用，对于行业安全发展具有重大价值。从观测数据可以发现，同类医疗机构的安全建设水平可能参差不齐，这不仅反映出机构安全意识的差异，更显示出行业安全建设和考评标准的不足。随着互联网医疗、智慧医院等新场景应用的深耕拓展，行业安全标准不完善或不落地的问题可能会更加凸显。因此，行业主管部门应优先推动健康医疗领域安全标准的体系化建设，补足健康医疗各类场景下的安全标准和安全规范，以安全标准为安全建设基线和安全考评指标，进而推动安全标准体系在行业内的真正落地实施，促进行业整体安全水平提升。

### 2、加强监测预警，完善态势感知

网络安全是攻防双方的对抗博弈，安全风险呈现不断动态变化的趋势，网络安全问题和风险解决无法指望毕其功于一役。行业主管部门应统筹行业内外资源，建设健康医疗行业的安全监测预警和态势感知机制和手段。一方面能够监测、感知和评估下属医疗机构安全建设情况，及时发现和预警安全风险，推动下属医疗机构进行整改，提升行业整体安全水平；另一方面能够基于整合和积累的行业安全数据，开展基于安全大数据的分析、研判和预测，挖掘新型网络安全风险，

预判行业安全发展变化态势，为健康医疗行业整体安全建设和规划提供支撑。

### 3、防控重点场景，保障安全创新

在疫情的影响和刺激下，互联网医疗、远程医疗、智慧医院等新型医疗服务获得快速发展，人工智能、大数据、5G、智能机器人等新技术在健康医疗场景进一步应用落地。然而，伴随着新业务和新技术而来的网络安全风险同样不容忽视。行业主管部门应加大对新业务新技术的网络安全监督管理力度，推动相关应用及技术的安全防护手段及标准研究，融合借鉴电信业、互联网、金融等行业领域的先进应用经验和安全防护举措，在保障网络信息和数据安全的前提下促进行业创新发展。

## （二）医疗机构应持续改进自身安全建设

### 1、提升安全意识，加强安全培训

在网络安全的各项影响因素中，人员的影响是最为显著和重要的。医疗机构的网络安全防护能力，在很大程度上取决于机构从业人员的安全意识和安全能力。尽管 2020 年健康医疗行业整体安全水平相对 2019 年有所提升，但对比其他行业，健康医疗行业整体安全情况仍处于较差水平，行业从业人员安全意识和安全能力仍有很大提升空间。因此，医疗机构应着重加强全体从业人员的网络安全教育培训，尤其应培养针对钓鱼邮件、恶意网页、弱密码设置等典型问题的安全防护意识，降低由于安全意识不足带来的网络安全隐患，切实提升机构整体的安全防护基线水平。

### 2、完善自评机制，推动持续改进

由于网络安全攻防技术手段不断升级迭代，单位的网络安全建设需要持续迭代和改进，才能够起到应有的安全防护效果。然而在实际情况中，大部分医疗机构的专职网络安全人员较少，或缺失专职网络安全人员，进而缺乏定期的网络安全测评或扫描。基于这样的背景，医疗机构应充分应用安全数字化和智能化手段，引入自动安全扫描测评技术手段和自主安全评估模式，开展定期的网络安全状况自检和自评，及时封堵脆弱性、安全漏洞及恶意程序等基础安全隐患和问题，不给外部攻击者可乘之机。与此同时，医疗机构也应建立定期开展渗透测试等制度机制，引入外部专业安全团队开展评估，发掘安全风险，开展系统性的安全整改和建设，持续提升安全能力水平。

### 3、构建试点机制，促进安全发展

随着互联网医疗、智慧医院、健康医疗大数据开放应用等政策战略的持续推进，健康医疗行业的数字化转型趋势不可逆转，医疗机构的开放程度不断深化。传统的信息系统一关了之和物理隔离的网络安全解决方案已经逐渐难以适应和满足业务发展需求。医疗机构应从自身业务战略和需求出发，构建新业务新技术试点应用安全机制。一是充分学习和理解监管机构对于互联网医疗等新业务发布的政策法规，在安全合规的前提背景下开展建设；二是要充分重视新业务新场景下的潜在安全风险，建立适用于新业务新场景的安全管理制度和管理机制；三是要加强市场沟通交流，及时了解和尝试新型防御手段和防御技术，如联邦学习、多方安全计算等技术架构，解决传统的健康医疗

数据安全统计和计算问题。

## （三）安全服务机构应加快提升服务质量

### 1、加速技术研发，提升安全水准

健康医疗行业安全技术水平的提升，很大程度上依赖于医疗机构安全服务厂商的技术升级。在当前日趋复杂的国际环境下，医疗机构的信息化和安全服务厂商，更应该加大网络安全产品和技术研发投入，增强自主创新能力，提升其产品和服务在国内及国际安全市场的竞争力。提升安全服务水平和安全服务质量，一方面要切实满足医疗机构传统安全防护需求，从产品技术维度推动医疗机构安全建设水平提升；另一方面应积极布局健康医疗新技术新场景下的安全产品和服务，做好网络安全的支撑和保障工作。

### 2、压实管理规范，完善安全运营

医疗机构信息化和网络安全建设绝大多数都需要安全服务机构参与，由于外部厂商管理及运维问题导致的健康医疗行业安全事件已屡见不鲜。从外部安全服务机构角度，一是应该加强自身安全管理规范建设，严格控制服务人员操作、管理、运维医疗机构信息系统及网络的行为，规避恶意操作等风险；二是应做好售后服务工作，协助医疗机构相关人员理解和掌握系统操作和使用规程，帮助医疗机构将网络安全防护手段和设备真正利用起来；三是要做好系统上线后的善后服务工作，及时将系统中的测试账户、测试数据等删除，降低此类问题带来的安全隐患和风险。

### 3、融合行业场景，促进合规应用

网络安全作为信息化的重要分支，其核心价值是支撑和促进业务的健康发展。传统的通用安全解决方案并不能完全满足医疗机构平衡业务发展和网络安全的诉求，这就需要安全技术和服务与健康医疗行业场景进行深度融合，挖掘每个场景下的业务特点和安全需求，并针对性的提供解决方案。例如在健康医疗大数据开发利用层面，医疗机构的强诉求是数据不出本地，这样就需要联邦学习、安全多方计算等安全技术手段来支撑落地。在场景深度融合方面，安全服务机构应持续加大投入力度，切实理解行业痛点，深入贯彻行业合规要求，才能够提供更加有竞争力的产品及服务，并实现在健康医疗行业各场景下安全产品服务的应用和落地。

# 附录 A 网络安全量化风险分级

| 风险级别 | 对应分数段 | 风险级别说明 |
| --- | --- | --- |
| 重大风险 | 0-500 分 | 威胁种类多、攻击频率高，存在大量安全隐患，缺乏安全防护能力 |
| 较大风险 | 500-800 分 | 威胁种类较多、攻击频率较高，存在较多安全隐患，缺乏基础的安全防护能力 |
| 一般风险 | 800-900 分 | 威胁种类一般、攻击频率一般，存在安全隐患，具备基础的安全防护能力 |
| 低风险 | 900-1000 分 | 威胁种类较少，攻击频率较低，存在较少的安全隐患或暂未发现网络安全风险，具备较强的安全防护能力 |

**中国信息通信研究院 安全研究所**

地址：北京市海淀区花园北路 52 号

邮政编码：100191

电子邮箱：liupeng1@caict.ac.cn

传真：010-62304364

网址：www.caict.ac.cn