INDUSTRY ANALYSIS

行业分析

互联网医院安全架构研究报告

2020 年 9 月

动脉网 vcbeat.top
VCBeat Research 蛋壳研究院 未来医健趋势研究
Neusoft 东软

前言

利用互联网、人工智能、大数据等技术，互联网医院构建了一种全新的医疗服务模式，赋予了医疗监管机构、医疗服务机构、医疗企业、医生、患者新功能，重构了医疗健康价值网络，尝试着解决“医疗不可能三角”难题。

而互联网医院本身处于互联网环境中，随时面临着未知人员的恶意访问与攻击行为，自身的安全性难以保障。2018年7月国家卫生健康委员会、国家中医药管理局印发的《互联网医院管理办法（试行）》提出“互联网医院信息系统按照国家有关法律法规和规定，实施第三级信息安全等级保护。”这是医疗行业首次将信息化建设与安全建设进行了捆绑，等级保护建设成为了互联网医院上线的必要条件。

为了解决网络安全建设与业务发展割裂的问题，从网络安全的角度为医疗机构提供互联网医院网络安全规划思路，蛋壳研究院联合东软网络安全事业部，基于目前互联网医院安全建设的现状，深度剖析互联网医院网络运营者面临的网络安全挑战与机遇、互联网医院安全保障与技术标准。

互联网医院网络安全建设需要医疗机构发挥网络安全的指导作用，再结合企业优质的产品和服务。双方结合在一起，才能更好地落地。最后进一步对东软网络安全产品及解决方案进行深入解读，以期为行业参与者提供较为全面的参考信息。

核心观点

1. 互联网医院作为医疗健康产业的新物种，刚经历新一轮的建设高峰，截至 2020 年 4 月 30 日，全国已成立 497 家互联网医院；

2. 互联网医院系统包括应用层、支撑层以及平台层三个组成部分。应用层面向用户提供服务，支撑层提供支撑服务所必须的功能模块，平台层主要提供基础架构服务。目前在平台层的建设相对比较落后；

3. 医疗机构网络安全建设落实情况依然不容乐观。三级医院通过等级保护三级测评的仅有 52.57%，三级以下医院仅有 24.92%通过等级保护测评；

4. 三级等保是互联网医院的第一道安全防线，涉及定级备案、规划设计、建设整改、等保测评以及运营管理五个关键步骤。随着互联网医院建设浪潮，将持续激发需求。

目录

一、互联网医院建设层级 1

1.1. 互联网医院概述 1

1.2. 互联网医院建设现状 3

二、互联网医院总体技术架构 7

2.1 互联网医院服务体系 7

2.2 互联网医院系统架构 8

三、互联网医院网络运营者面临的网络安全挑战与机遇 10

3.1 互联网医院安全建设面临的五大挑战 10

3.2 互联网医院安全建设带来的重大机遇 16

四、互联网医院安全保障与技术标准 17

4.1 医院和企业共同承担互联网医院网络安全建设职责 17

4.2 等级保护建设是互联网医院第一道安全防线 20

4.3 业务安全是互联网医院发展基石 24

4.4 网络安全人才是医疗机构网络安全根本 29

五、东软 NetEye 互联网医院安全最佳实践 30

5.1 以业务安全助力互联网医院网络安全体系规划 30

5.2 一体化服务助力互联网医院网络安全建设落地 33

5.3 专业的网络安全产品助力互联网医院网络安全建设落地 35

5.4 网络安全人才培养与输出助力医疗行业网络安全发展 42

一、互联网医院建设层级

1.1.互联网医院概述

1.1.1 互联网医院定义及模式

互联网医疗，是互联网在医疗行业的新应用，包括了以互联网为载体和技术手段的健康教育、医疗信息查询、电子健康档案、疾病风险评估、在线疾病咨询、电子处方、远程会诊及远程治疗和康复等多种形式的健康医疗服务，而互联网医院就是互联网医疗的载体和平台。互联网医院作为医疗健康产业的新物种，其诞生之初就带有三大创新源泉的基因。利用互联网、人工智能、大数据等技术，互联网医院构建了一种全新的医疗服务模式，赋予了医疗监管机构、医疗服务机构、医生、医疗企业、患者新功能，重构了医疗健康价值网络，尝试着解决“医疗不可能三角”难题。

根据国家相关政策的规定，互联网医院主要有两种模式：一种是医院主导型互联网医院，一种是企业平台型互联网医院。前者主要以三甲医院为代表，主要利用本院的医师开展互联网诊疗活动；后者以互联网医疗企业为代表，如微医、好大夫在线、春雨医生等，通过依托线下实体医疗机构，利用在本机构和其他医疗机构注册的医师开展互联网诊疗活动。

1.1.2 互联网医院功能

互联网医院作为医疗健康产业变革创新的新事物，有效地促进了医疗资源的流动，赋能基层医疗水平，提高了分级诊疗的实施效率，缓解了医疗资源分布失衡的难题。

图 1 互联网医院服务规范

资料来源：动脉网

互联网医院主要优势：

1）做强医疗资源价值链条，推动分级诊疗发展。

将诊疗从线下转至线上拓展医疗服务空间和业务范围，合理引流医生与患者，进行精准匹配。促进优质医疗资源流动，扩大医院品牌效应。同时面向基层医生输出技术支持和培训，提升基层首诊能力。

2）便捷患者就医，降低医疗支出。

通过优化医疗服务流程，打破时间和空间限制，节省排队挂号、候诊就医时间，可提高诊疗效率。尤其在农村和偏远地区，使患者可以在“家门口”便捷就医，真正实现足不出户求诊名医名家，缓解区域间医疗资源不平衡和医疗需求剧增之间的矛盾。

3）提高医生收入，拓宽多点执业的渠道，促进医师资源流动。

缓解了医生的工作压力，弥补了医生资源的不足，有效提高医生的工作效率，塑造医生个人品牌，将医生的价值发挥到最大化。

4）助推医院信息化建设，加快医疗大数据共享。

通过云平台、移动智能终端，获取患者健康数据和既往病例实现健康监控和病历共享，便于打通院间的信息壁垒和信息不对称。

5）可降低医患纠纷发生的机会概率。

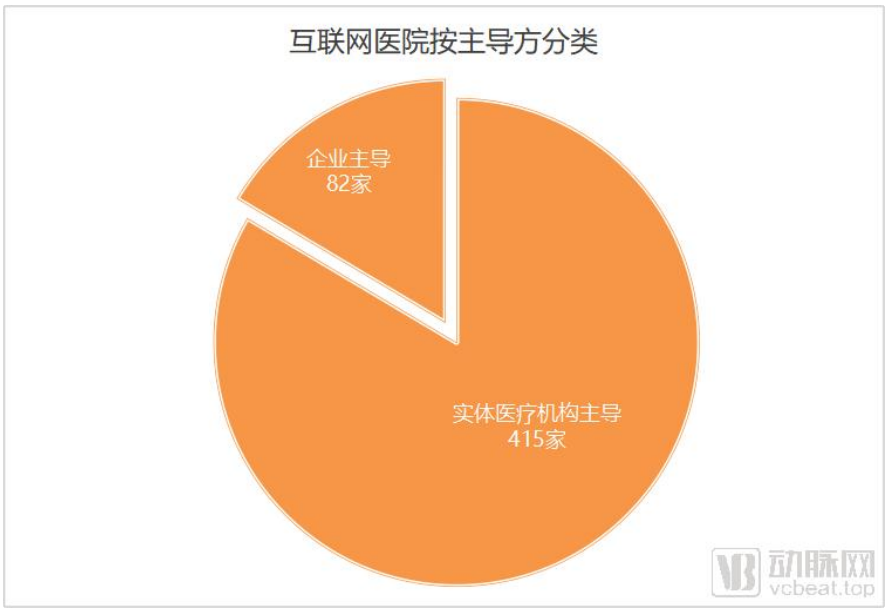
互联网能够全程留痕，服务过程更加透明。加强在线医患之间的沟通，也改善医患关系，扩大医院病人来源，形成口碑效应。

1.2. 互联网医院建设现状

1.2.1 互联网医院数量和类型

数据截至 4 月 30 日，从多个公开渠道搜集到目前 497 家互联网医院的资料。互联网医院根据申办主体的不同，分为实体医院主导型和企业主导型。497 家互联网医院中，有 415 家是实体医院主导，占 83.5%。

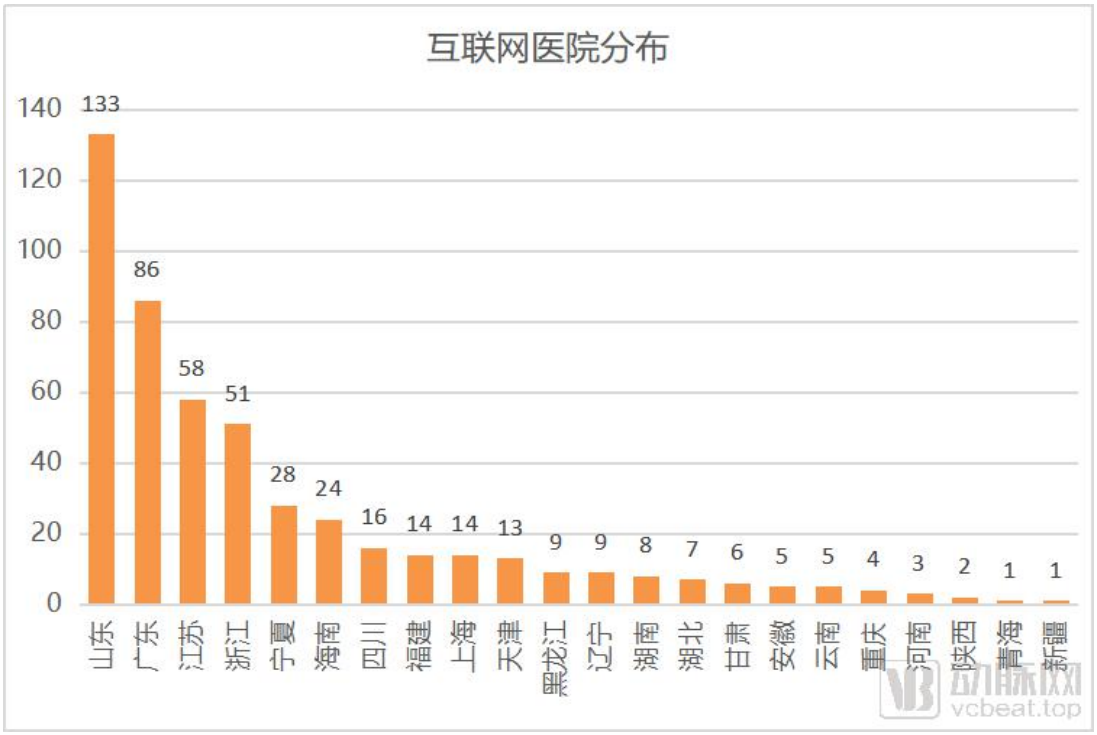
图 2 互联网医院按主导方式分类



资料来源：动脉网

由于全国各地医疗资源、医疗水平、医疗信息化水平不尽相同，各地建设互联网医院的情况也有较大差别。

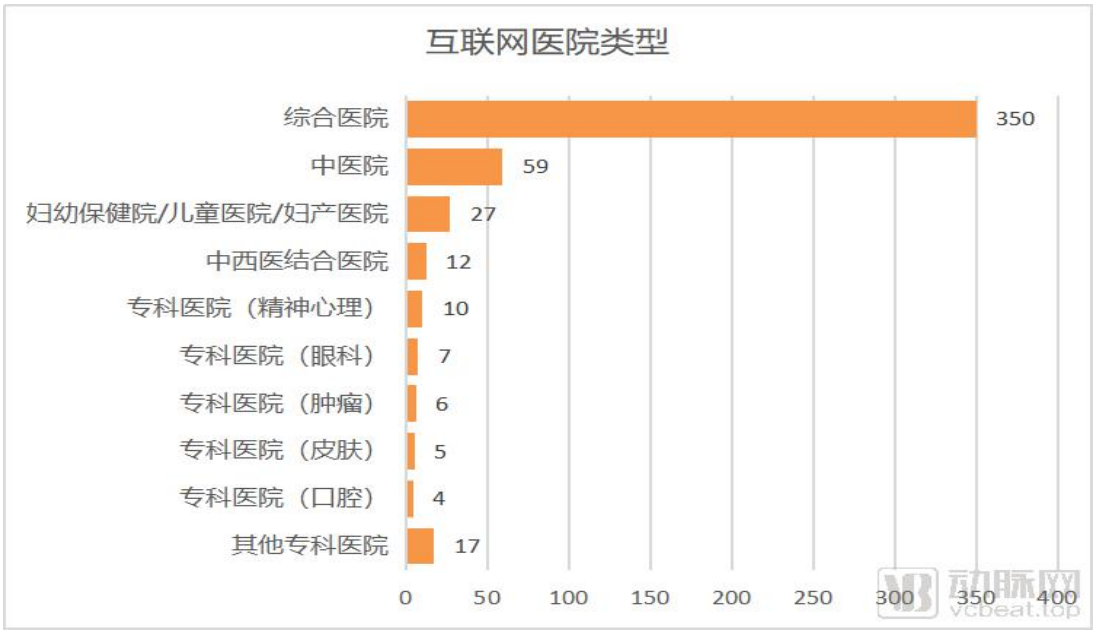
图 3 互联网医院整体区域分布



资料来源：动脉网

从上图可看出，现阶段互联网医院主要分布在东部、南部沿海省份，这些区域优质医疗资源集中、医疗信息化程度也较高，有良好的基础。其中，山东、江苏、安徽、浙江、福建、广东等省份还被国家卫健委确定为“互联网+医疗健康”示范省。互联网医院最多的几个区域，原本就是进行行业探索较早的地区。目前，山东的互联网医院已达到 133 家。

图 4 497 家互联网医院的类型



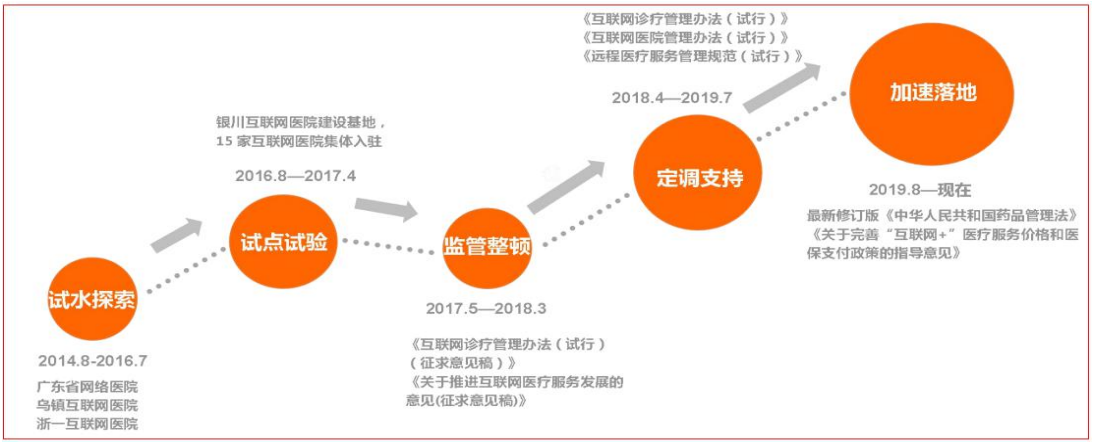
资料来源：动脉网

从目前互联网医院类型来看，综合医院和中医院占主流，专科医院类型多样。综合医院科室齐全，能满足患者多种就诊需求。中医院虽然在线上无法把脉，同样可以开出在线处方。妇幼保健院、儿童医院和妇产医院也是占比较高的医院类型。其他的专科医院中，以慢病或口腔、眼科类消费需求较强的专科为主，这些医院能够满足患者医疗、健康管理、消费等的多层次需求。

1.2.2 互联网医院建设历程

互联网医院基于远程医疗而兴起，在国家政策层面获得认可和鼓励后，迎来了大量参与者，开始涉及医疗核心业务。作为一个与政策强相关的行业，任何分析必须建立在对政策解读、监管梳理的基础上，我们首先从政策演进方向分析了互联网医院的发展之路。国家对互联网医院的监管经历了“试水探索期—试点试验期—监管整顿期—定调支持期—加速落地期”五个监管阶段。

图 5 互联网医院政策演变情况



资料来源：动脉网

同时，互联网医院刚刚经历了新一轮的建设高峰。

图 6 2019 年以来互联网医院成立情况

资料来源：动脉网

可以看出，成立数量整体呈上升趋势，2019 年 4 月迎来第一个高峰，在 8 月国家医保局《关于完善“互联网+”医疗服务价格和医保支付政策的指导意见》出台后，12 月又迎来第二个高峰。

到 2020 年，2 月建立的互联网医院最多，达到 65 家。这或许也是互联网医院诞生以来，单月建设数量最多的阶段。2 月正值新冠肺炎疫情的高峰期，疫情防控的迫切需要推动了互联网医院建设。疫情期间，原有互联网医院纷纷开通线上发热门诊、慢病复诊、肺炎咨询，此外还不断有互联网医院紧急获批和上线。随着疫情平稳，2020 年 3 月开始，互联网医院增长速度放缓，4 月回落到疫情之前的水平。

疫情期间，互联网医院满足了大量慢病患者的用药需求，提供在线复诊、开方、药品配送服务，部分还可医保报销。然而，互联网医院不能只靠疫情防控来推动，尽管行业在此期间进行了很好的用户教育、习惯培养，但疫情之后，在线问诊对患者的吸引力是否能维持，充满不确定性。

二、互联网医院总体技术架构

2.1 互联网医院服务体系

互联网医院建设主要包括医疗机构主导和企业主导两种。由于医疗机构和企业自身的资源与倾向性，医疗机构主导更加偏重于医疗机构与互联网医院信息联通，互联网医院实现医疗机构服务外延。企业主导更加偏重互联网医院与第三方机构连接包括药房、药品采购、商业保险等，最大发挥互联网医院商业价值。从全局出发，互联网医院建设应该从目前医疗行业面临的问题角度考虑，利用互联网技术解决部分医疗行业存在的问题。因此，整体服务体系建设至少应实现以下效果：

第一， 推动医疗机构从“医疗”到“健康”的转变

《健康中国 2030 规划纲要》的颁布，标志着我国医疗向健康的转变。当前医疗机构格局依然以治疗为主，对于慢性病、常见病的预防、康复以及健康管理等方面依然存在不足。互联网医院是保证供给侧结构性改革的一个重要举措，医疗机构需要借助互联网这个工具，与药品供应等第三方服务商及其药店合作实现药品配送，与支付机构连接实现智能化线上支付，与康复机构连接解决患者术后康复问题，同时引入可穿戴设备对居民进行健康监控与管理。互联网平台通过这些新的资源配置方式，能够实现更优化更智慧的会诊流程和服务模式。

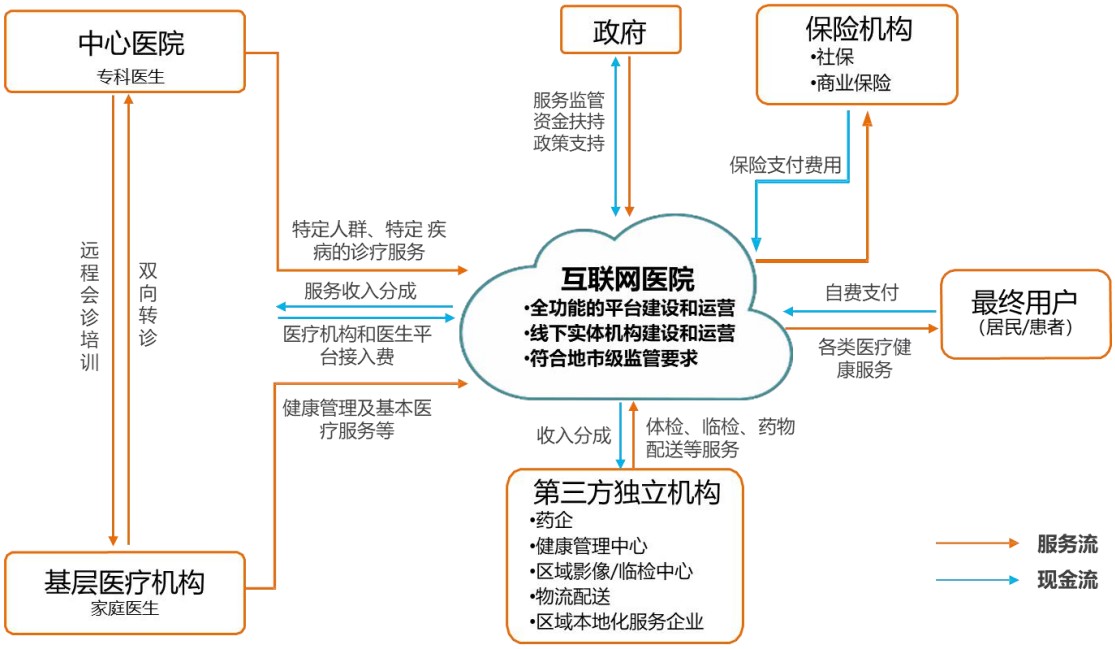
第二， 实现患者需求与医疗资源的智能匹配

当前智慧医院建设更多地从医疗机构信息化角度出发，提高诊疗效率。而这仅仅是信息化，并非智慧化。应该依托互联网医院利用 5G、物联网、“互联网+”等技术，实现患者需求和医疗资源的智能匹配，才能够真正将医疗机构所沉淀的医院管理标准变为智慧、智能医院的基础。

第三， 推动医联体、医共体落实

通过互联网医院将省一级医疗机构到各地各个诊所，再到卫生室、社区卫生服务中心等进行连接，把医联体构建起来。再通过精尖设备下沉、影像诊断资源下沉、服务规范标准建设，提高基层医疗机构的诊疗能力。把基层的患者留在基层，同时把优质医疗资源下沉到底，把药品配送到基层的老百姓身边，规范管理，落实宣教，还要把医疗的费用降到最低。

图 7 互联网医院服务体系



资料来源：东软集团，动脉网

由此可以看出，互联网医院应该是涵盖政府、中心医院、基层医疗机构、第三方独立机构、保险公司，面向居民提供医疗和健康管理的服务体系。

2.2 互联网医院系统架构

以互联网医院服务体系为目标，互联网医院系统建设应该是全面的、体系化的，其主要包括以下两方面的建设内容：

2.2.1 互联网医院系统建设

互联网医院系统包括应用层、支撑层以及平台层三个组成部分。

应用层面向用户提供服务，主要包含患者 APP、医生 APP、浏览器、基于微信、支付宝的应用服务。

支撑层提供支撑服务所必须的功能模块，主要包含互联网医院基础服务、互联网医院增值服务、互联网医疗集团资源共享服务共计 3 个服务层级，实现以下功能。

1) 以院内院外患者用户体验为核心开展互联网医院服务。基于“全流程”的移动化服务，提升患者的就诊体验、减少排队的困扰、降低平均等候时间，获取更多医疗资源相关的信息。

2) 构建院内院外、线上线下，一体化的信息共享诊疗服务；将医生诊疗服务、药师咨询及药品审核服务等合理地应用到线上，释放临床、医技、药剂等多类型医疗资源，提高医院服务价值与能力，扩大服务辐射范围。

3) 构建共享化的医疗资源服务体系，对跨机构诊疗资源重新进行整合与利用。通过开放性的服务平台，提升各个医疗机构诊疗资源的利用率，提升患者就医的便捷性。

平台层主要是为互联网医院多维度应用提供基础架构服务，保证线下、线上诊疗业务数据的一致性，并为互联网诊疗业务的正常运营提供技术支撑。主要包含：自助服务平台、预约服务平台、云诊室工作平台、随访服务平台、药品物流配送服务平台、健康教育服务平台、医院支付平台、在线服务平台、医疗资源共享平台、医疗资源协作平台，共计 10 个基础平台。

2.2.2 医疗机构信息集成平台建设

医疗机构信息化建设始于上世纪 90 年代，经过将近 30 年的发展，大型医疗机构已拥有几十个功能模型的医院信息系统。医疗机构信息系统在不同阶段关注点不同，建设之初只关注信息的采集不关注信息的共享和利用。在子系统数量较多的情况，系统间的关系线已经形成了网状结构，并且不同系统间的很多信息是重复的。调查显示，当前已有 70%以上的医院实现了医疗信息化，但仅有不到 3%的医院实现了院内信息的数据互通。面对互联网医院与内网数据融合需求，必须要实现院内信息整合，否则医疗机构内外网系统连接将错综复杂，系统间网状结构的情况将更加严重，内外网边界也将越来越模糊。可基于 ESB、SOA、XML 等建设医疗机构信息集成平台，实现各子系统的互联互通，消除信息孤岛，使医疗机构信息系统数据实现充分的共享。同时基于信息集成平台打通内外网数据，满足互联网医院业务扩展需求。

图 8 互联网医院系统组成构架

资料来源：东软集团，动脉网

三、互联网医院网络运营者面临的网络安全挑战与机遇

3.1 互联网医院安全建设面临的五大挑战

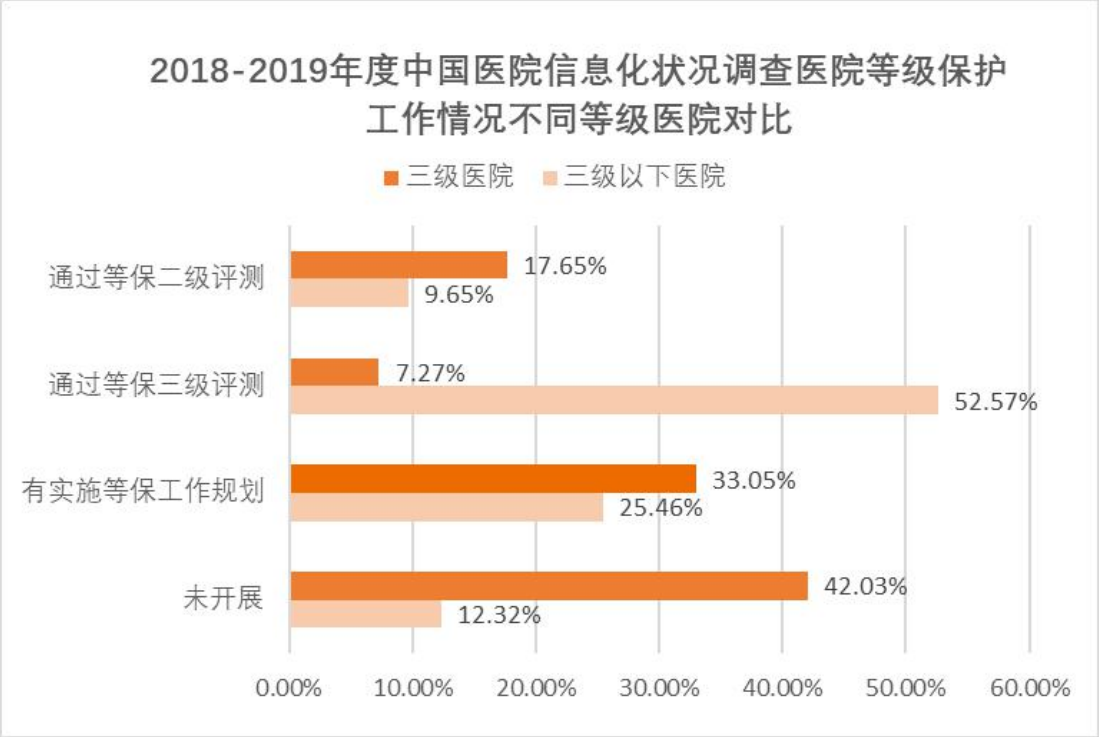
3.1.1 业务互联网化将进一步加剧医疗机构的安全风险

2011 年至今，我国推出《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）、

《关于印发医疗质量安全核心制度要点的通知》（国卫医发[2018]8 号）、《关于印发全国医院信息化建设标准与规范（试行）的通知》等一系列文件以等级保护建设为中心，推动医疗机构网络安全建设。同时在《电子病历系统功能应用水平分级评价方法及标准（修订征求意见稿）》、《国家医疗健康信息医院信息互联互通标准化成熟度测评方案（2019 版）》、《区域全民健康信息互联互通标准化成熟度测评方案（2020 年版）》等多项医疗能力评级标准中对医疗机构的网络安全建设也分别提出相应要求。

但是目前我国医疗机构网络安全建设落实情况依然不容乐观。三级医院通过等级保护三级测评的仅有 52.57%，三级以下医院仅有 24.92%通过等级保护测评（包括二级和三级）。多数医疗机构尤其是三级以下医院，仍然未开展网络安全等级保护建设。

图 9 医院等级保护工作落实情况



资料来源：CHIMA《2018-2019》年度中国医院信息化状况调查报告

在对疾病预防控制中心、卫生监督所、卫生和计划生育委员会、医学会、公立医院、私立医院进行调研过程中发现，医疗机构自身的网络安全防护能力依然薄弱，面临网络安全风险依然严峻。青海省、海南省、内蒙古自治区、西藏自治区、宁夏回族自治区等地区网络安全风险相对严重。山东省和四川省网络安全风险较低。

由于互联网医院业务服务处于互联网环境，随时面临着未知人员的恶意访问与攻击行为，并且在与多方机构进行连接的过程中恶意流量极易进入互联网医院系统，因此互联网医院自身的安全性难以保障。其次，面对互联网医院线上线下的医疗信息互联互通共享的需求，传统的相对封闭的内网医疗信息环境与外部互联网对接融合。原本呈现网格状连接的院内系统与互联网医院连接后，内外网边界更加模糊，内网面临的网络入侵和信息泄露风险将明显增大。目前医疗机构网络安全防护能力存在不足的情况下，无法应对互联网化带来的安全风险，医疗机构整体安全风险将进一步增加。

3.1.2 网络安全人才短缺制约互联网医院安全体系防护效果

网络安全建设核心理念是“谁主管谁负责”，谁提供互联网医疗健康的服务，谁就必须要负责任，所以互联网医院要实行安全责任制，这也应该是互联网医院建设的一个基本原则。在互联网医院网络安全建设方面虽然强调了第三方平台的责任，但是互联网医院是以实体医疗机构为依托，责任主体依然是实体医疗机构。所以明确公立医疗机构主导模式、资源融合模式、互联网企业主导模式三种建设模式实体医疗机构和企业所需承担的责任，并根据本地部署、云部署等不同的部署方式选择互联网医院网络安全建设的内容是互联网医院网络安全建设的关键。

医疗行业网络安全建设并不是刚刚起步，绝大多数医院已经具备防火墙、上网行为管理等主要网络安全产品。因此面对互联网医院网络安全建设，合理进行安全规划，提高安全产品利旧率，一方面节约成本，另一方面将避免重复产品和管理制度增加运维人员负担。

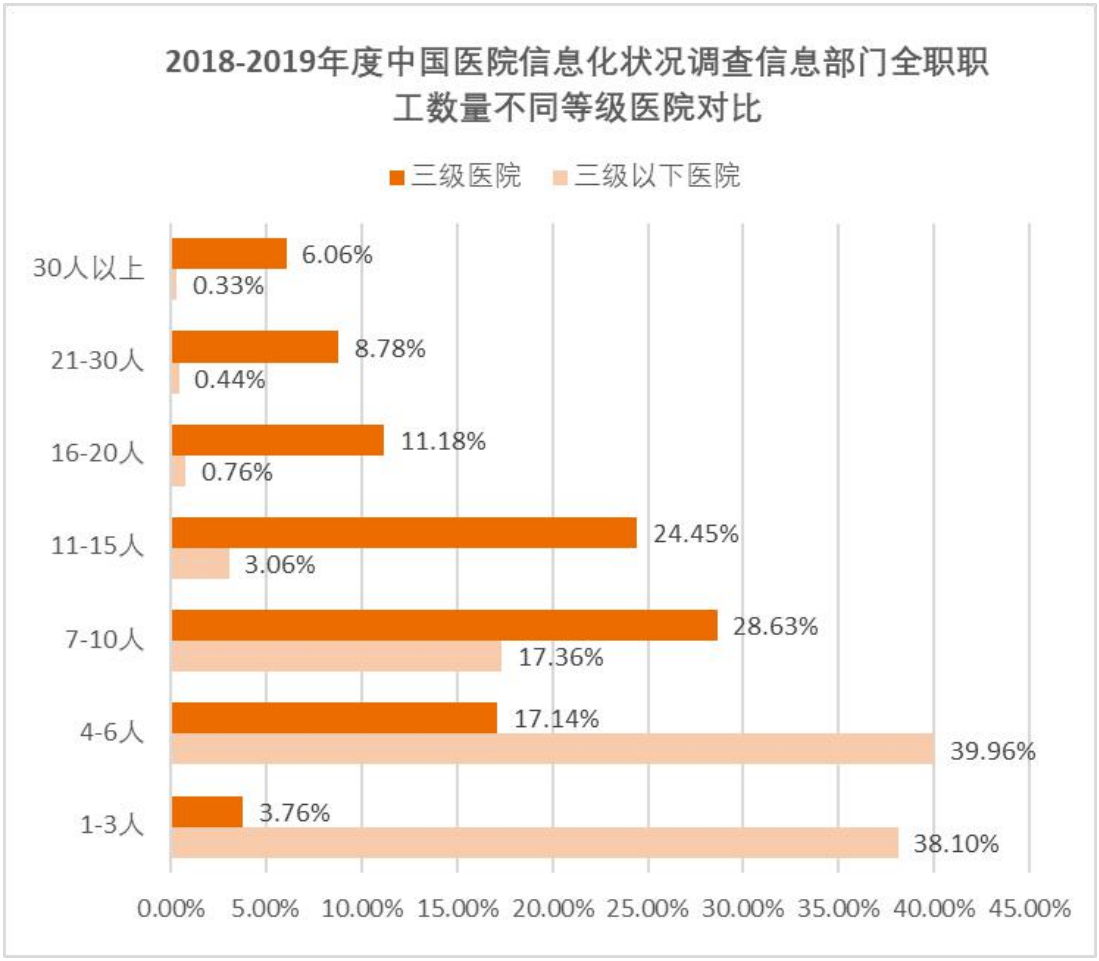
图 10 医院网络安全建设现状

资料来源：CHIMA《2018-2019》年度中国医院信息化状况调查报告

绝大部分医疗服务商在推动互联网医院的进程中抱着“只管杀，不管埋”的心态，并没有站在长远发展的立场来帮助医疗机构妥善规划内外网连通后能够应对互联网医院未来安全风险的网络格局和安全体系。大部分网络安全厂商不了解医院的业务，更多地站在网络安全从业者的角度考虑互联网医院网络安全建设，导致网络安全建设与实际业务错配，网络安全措施无法落实。

综合以上三点，专业的网络安全人才是医疗机构尤其是互联网医院建设后的网络安全建设关键，只有专业的网络安全人才能够帮助医疗机构合理进行互联网医院网络安全规划。然而根据调查，50%以上的三级医院信息中心人员仅有7-15人，而将近80%的二级医院信息中心人员在6人以内。医院信息中心负责信息化建设以及应用系统和硬件的维护等工作，在这样的人员配比情况下，信息中心人员的工作已经十分紧张。在重业务、轻安全的情况下，医院信息中心真正负责网络安全建设的人员更是寥寥无几。

图 11 等级医院信息部门职工数量差异



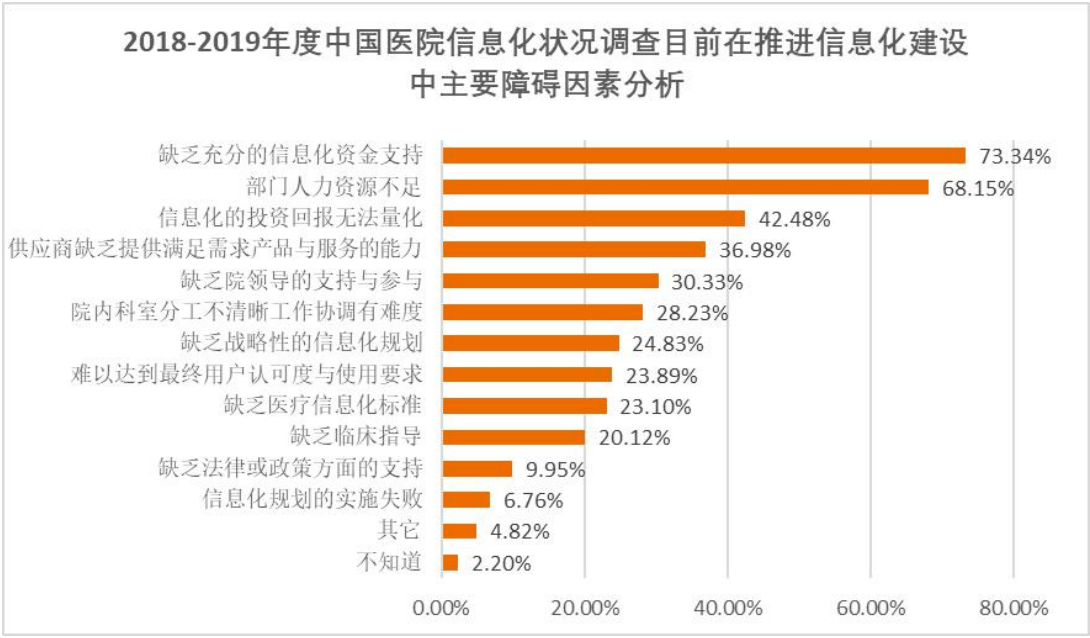
数据来源：CHIMA《2018-2019》年度中国医院信息化状况调查报告

2019 年 6 月网络安全人才市场需求的规模达到 2016 年 1 月需求的 24.6 倍，相比 2018 年 7 月也增长了 3 倍，增长速度堪称惊人。在网络安全人才市场整体短缺的情况下，更多的网络安全从业者向北京、上海等一线城市涌入，向收入更高的民营企业涌入。在这样的情况下，医疗机构寻找到专业的网络安全人才本就是一件困难的事情。同时网络安全人才需要更长时间的培养才能了解医院业务。因此现阶段医疗机构难以满足上述网络安全人才需求，最终影响医疗机构网络安全建设效果。

3.1.3 网络安全资金投入不足，限制了互联网医院安全的落实

近年来医疗行业信息化建设得到大力发展，但相对于金融、政府等其他行业，医疗行业信息化建设依然相对落后。HIS、EMR 等核心系统、智慧病房等提高患者满意度的系统、自助终端等提高医生效率的系统依然是医疗机构亟需落实的信息化建设内容。绝大多数医疗机构，尤其是三级以下医院，信息化建设资金主要来源于财政补款，这部分资金用于建设能够提升医疗机构效率的系统已经捉襟见肘，用于网络安全建设的资金更是微乎其微。并且根据 2020 年国家卫健委发布的部门预算，公立医院整体预算将下降四成。在资金不足的情况下，无法为医疗机构带来直接效益的网络安全建设更是难以推动。医疗机构网络安全建设中第一阻碍因素仍然是缺乏充分的信息化资金支持。

图 12 医院信息化建设主要障碍因素



数据来源：CHIMA《2018-2019》年度中国医院信息化状况调查报告

3.1.4 亟需新兴技术应对医院互联网转型过程中的新挑战

互联网医院网上问诊、预约挂号、学术分享等业务都需要系统良好的稳定性作为支撑。因此多数

医疗机构在互联网医院建设之初便充分考虑了应用系统性能的问题，甚至很多医疗机构选择使用云环境部署互联网医院系统，便于应用系统随着业务需求增加而性能扩容。然而在网络环境方面，互联网医院面对未知的互联网环境，高效选路和链路服务优化将成为业务发展的必要。就好像人们在面对复杂的城市交通环境一样，没有人能够确切知道交通的状况并做出有效的预测，往往选择一条错误道路就导致了堵车。面对这样的问题，互联网医院往往采取提高带宽或采取专线、MPLS 的方式提高网络性能及稳定性。这一做法导致医疗机构面临高额的网络建设费用的同时很难将资源发挥应有的效用。

重点医疗机构一号难求的状态一直存在，网上预约挂号、现场自助挂号、24 小时咨询挂号服务热线等手段很大程度上缓解了这一问题。但是号贩子仍然活跃在医疗机构门诊大厅非法倒卖号源，屡禁不止。互联网医院的建设，其根本是实现网上就医。“黄牛”利用他人身份证件或伪造身份证信息在互联网医院平台进行预约挂号，医院放号时通过专业设备快速“秒杀”囤号，之后开始进行倒卖。这一做法，将直接影响互联网医院对于患者的可用性，进而影响互联网医院的推广。

居民生活习惯的改变是一个渐变的过程，并不会一蹴而就。互联网医院发展的根本是患者从实体医院向互联网医院的转变。因此通过增强信息系统可用性，保护居民的权益，让群众对互联网医疗建立信心，是现阶段互联网医院发展刻不容缓的问题。无法解决将导致使用者信任度的降低，亦将对国家推动互联网医院建设力度造成影响，最终将影响互联网医院整个行业的发展。

3.1.5 数据共享引发的数据泄露问题将面临行政处罚

互联网医院将原本在医院内部流通的医生笔记、处方、检查信息等与诊疗相关的信息流转放到了互联网环境中，患者数据更加集中，更易获得。互联网医院与保险机构、药企、健康管理中心、物流配送等第三方机构进行数据共享，患者数据在各机构之间流转。患者数据涉及患者隐私和利益，一旦泄露不仅影响患者对互联网医院的信任，也将对实体医院形象造成严重影响，甚至面临监管部门的处罚。互联网医院所依托的实体医院和企业作为互联网医院网络运营者，采集和控制患者数据，承担着数据防护的职责。在数据防护方面，由于医疗数据的复杂性，脱敏、加密等技术难以落实，分级分类管理也缺乏明确的标准，数据安全管理成为了互联网医院网络安全建设的难点。面对不可控的互联网环境和多机构的数据共享，患者身份认证信息丢失、第三方机构数据保管不当、互联网医院系统被攻击都可能导致患者数据泄露。如何明确各方职责，界定数据泄露责任，进一步增加了数据管理的难度。在立法方面，我国目前尚未出台统一的保护隐私信息的法律法规，对保护患者医疗信息、个人隐私的规定都是碎片化的，缺乏实质性的立法，互联网医疗医疗信息安全面临巨大挑战。

3.2 互联网医院安全建设带来的重大机遇

2018 年 7 月国家卫生健康委员会、国家中医药管理局印发的《互联网医院管理办法（试行）》提出“互联网医院信息系统按照国家有关法律法规和规定，实施第三级信息安全等级保护。”这是医疗行业首次将信息化建设与安全建设进行了捆绑，等级保护建设成为了互联网医院上线的必要条件。摆脱了业务先行，安全滞后的困境。在互联网医院按照等级保护进行建设的同时，医院外网环境安全防护水平也将明显得到提高。

互联网医院将原本在医院内面对面的就诊转移到通过互联网异地就诊，打破了就诊信息的传递介质与环境。为了实现诊疗业务向互联网环境中迁移，传统的医院信息系统不得不打破原来的“烟囱”式的信息化建设模式和已经形成的内外网隔离的信息“孤岛”状态。由于互联网医院系统存在与院内系统连接的情况，部分地区对建设互联网医院的实体医院的内网核心系统提出了安全要求，进一步推动了医院内网安全建设。例如部分地区对于互联网医院建设增加了附加规定，要求建设互联网医院的医疗机构内网核心系统需达到等级保护三级要求。

由此可以看出，互联网医院的业务转型对于医院整体网络安全建设提出了更高、更强的要求，同时也将对医院网络安全建设起到了极大的推动作用。我国医疗行业整体网络安全水平，有望在互联网医院建设过程中得到全面提高。

四、互联网医院安全保障与技术标准

4.1 医院和企业共同承担互联网医院网络安全建设职责

互联网医院网络安全建设需要医疗机构和企业共同来分担。但是整体的互联网医院网络安全管理，则需要医疗机构自己来把控。所以互联网医院网络安全建设需要医疗机构发挥网络安全的指导作用，再结合企业优质的产品和服务。双方结合在一起，才能更好地落地。

4.1.1 等级保护建设中各方职责

按照“谁主管谁负责”的原则，无论互联网医院系统归属方是谁，只要实体医疗机构是互联网医院网络运营者之一（即互联网医院依托其存在）实体医疗机构均承担着其互联网医院的网络安全职责。在互联网医院建设中，存在企业提供互联网医院基础设施（如运营商提供基础设施）或提供互联网医院系统（如宁夏银川互联网医院、天津微医互联网医院等）或企业直接收购私立医院独立发起（如丁香园、阿里健康网络医院等）的情况，因此落实互联网医院等级保护建设过程中，需强调企业的职责。根据常见的互联网医院建设模式，按照等级保护三级建设要求，明确医疗机构和企业在不同模式下的等级保护三级网络安全建设责任。

1) 资源融合模式

资源融合模式，企业提供互联网医院应用系统，实体医院仅通过业务终端接入互联网医院平台。此种模式下提供互联网医院系统的企业平台和应用系统需通过等级保护三级测评。实体医院需根据具体的部署情况，承担以下网络安全建设内容：

① 医疗机构网络安全建设责任

医疗机构实体环境侧

i 互联网医院业务终端安全

实体医院仅通过互联网医院终端访问平台，因此安全防护措施应确保互联网医院终端安全，参照等级保护建设基本要求落实安全计算环境中终端部分安全措施，包括恶意代码防范、安全加固等。

ii 互联网医院与内网核心系统交互安全

实体医院侧与平台进行数据交互，除互联网医院业务终端外还包括内网核心系统。根据等级保护

基本要求，应建立内网核心系统与平台的隔离措施。同时参照等级保护建设基本要求，落实安全计算环境中终端部分安全措施，包括恶意代码防范等。

iii 业务终端与互联网医院通信安全

医院访问平台存在两种方式。第一种方式，依托卫生专网或运营商搭建的专网访问平台，此时访问过程中的安全得到了保障，医院无需建设防护措施。第二种方式，考虑互联网便利性以及使用成本，医院通过互联网访问平台，此时传输行为和诊疗数据暴露在互联网环境中，需建立专用安全传输通道，以保障传输过程的安全性。

实体医院仅通过互联网医院终端访问平台，因此安全防护措施应确保互联网医院终端安全，参照等级保护建设基本要求，落实安全计算环境中终端部分安全措施，包括恶意代码防范、安全加固等。

② 企业网络安全建设责任

企业建设云计算平台包括设施、硬件、资源抽象控制层、虚拟化计算资源、软件平台和应用软件。企业承担云平台侧全部安全建设，企业应按照 SaaS 模式落实等级保护三级建设。

2) **医疗机构主导模式**

① 利用第三方机构提供的基础设施

医疗机构网络安全建设责任

第三方机构提供基础环境，最常见的是医疗机构租用运营商的机房或租用公有云环境。实体医院需对部署在第三方机构提供的云平台中的互联网医院系统以及访问互联网医院系统的业务终端所在环境进行安全防护。

i 医疗机构实体环境侧

参照资源融合模式中医疗机构在实体环境中的安全责任落实。

ii 云平台侧

由医疗机构自行部署应用系统，因此云平台侧的应用平台、软件平台以及虚拟资源层网络安全建设由医疗机构承担。医疗机构需按照《GBT22239-2019 信息安全技术 网络安全等级保护基本要求》云扩展要求进行防护，包括应用系统安全保障、操作系统安全监测以及虚拟资源隔离等。

企业网络安全建设责任

第三方企业作为云服务提供商，建设的云计算平台由设施、硬件、资源抽象控制层组成，其提供的基础环境需按照《GBT22239-2019 信息安全技术 网络安全等级保护基本要求》通用要求（三级部分）进行建设，包括物理环境、网络架构等，并且按照云扩展要求部分对云平台进行安全建设，使提供的云平台基础环境达到等级保护三级要求。

② 利用医疗机构现有机房

i 医疗机构网络安全建设责任

互联网医院合规建设中所有的安全建设内容均由实体医院承担，应按照《GBT22239-2019 信息安全技术 网络安全等级保护基本要求》中通用要求部分落实等级保护三级建设内容，包括技术部分中的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心以及管理部分中的安全管理机构等。

3) 互联网企业主导模式

互联网企业主导模式下承担互联网医院运营职责的实体医疗机构，包括互联网企业收购的医疗机构或依托的公立医疗机构，需落实等级保护三级建设。具体的建设内容可参考资源融合模式落实。而接入互联网医院平台的医疗机构，仅作为互联网医院系统使用方，不承担互联网医院运营职责，因此无需按照等级保护三级要求进行建设。

4.1.2 业务安全建设中各方职责

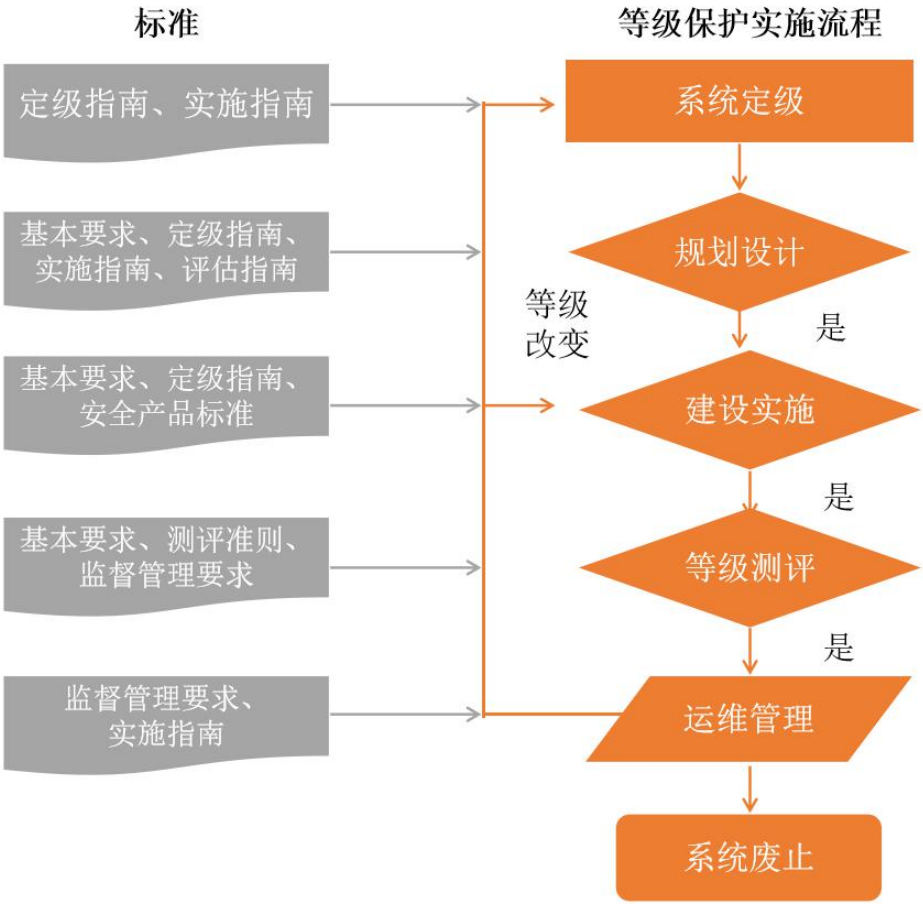
业务安全属于互联网医院网络安全建设的附加建设，医疗机构与企业共同参与的情况下，双方可根据服务内容划分业务安全建设职责并签订相应协议。

4.2 等级保护建设是互联网医院第一道安全防线

4.2.1 明确互联网医院等级保护建设时间

等级保护建设涉及定级备案、规划设计、建设整改、等保测评以及运营管理五个关键步骤。在这五个关键步骤中涉及定级材料准备与上报、网络安全调研与规划、招投标、等保测评材料准备与审批等一系列工作。其中《网络安全等级保护条例（征求意见稿）》将定级备案材料审核时间由原来的 30 个工作日缩短到 10 个工作日内。但由于等级保护建设涉及工作内容较多，仍然需要至少 1 至 3 个月才能完成。因此为避免由于等级保护建设导致互联网医院上线延期，互联网医院等级保护建设工作应在项目启动阶段就开始落实，与互联网医院信息系统建设同步进行。信息中心人员较少且网络安全建设基础较差的医院，至少应提前完成定级备案工作。

图 14 等级保护建设步骤示意图

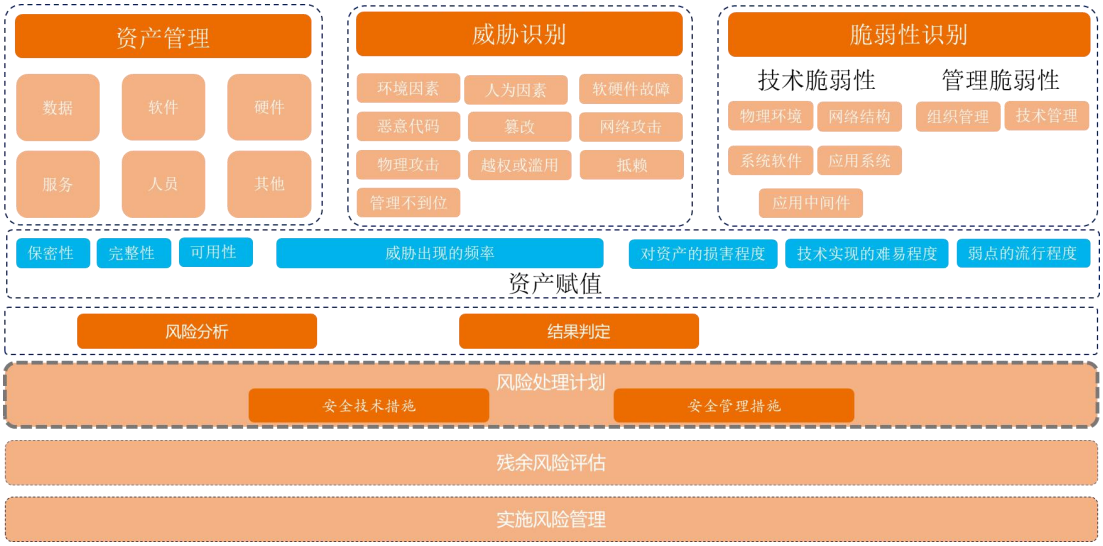


资料来源：东软集团，动脉网

4.2.2 以风险为中心筑牢等级保护建设安全防线

根据《GB/T 20984—2007 信息安全技术信息安全风险评估规范》对互联网医院环境进行风险评估。根据风险重点加强互联网医院安全，一是加强网络边界安全技术防护，做好网络边界访问控制、入侵防范、病毒检测等基本安全措施，确保无新的互联网边界死角。二是加强数据安全技术防护，采用数据防泄漏、数据库审计、数据脱敏等技术手段，确保医疗数据存储、提取、分析和发布等不同环节的保密性和完整性，同时需要关注医疗数据在不同阶段的访问控制权限应界定清晰。

图 15 等级保护安全防线建设



资料来源：东软集团，动脉网

可根据互联网医院自身面临的安全风险，从技术和管理两方面落实防护措施，完善网络安全防护体系。

1）技术措施

网络安全等级保护

① 等级保护通用要求技术部分要求对应措施

表 1 等级保护通用要求技术部分要求对应措施

等保要求	控制要求	推荐产品	实现机制
安全 物理环境	位置、访问控制、防盗窃、放破坏、防雷击、防火、防水和防潮、防静电、温湿度	门禁、监控报警系统、避雷装置、消防、水敏感检测仪、防静电设施、双路供电、电磁屏蔽	机房建设物理安全策略

	口控制、电力供应、电磁防护		
安全通信网络	网络架构	防火墙、网闸、光闸、UTM、无线安全网关	设备性能、多出口带宽、冗余链路、冗余设备、安全域划分、国密算法
	通信传输	VPN	
	可信验证	基于可信根产品	
安全区域边界	边界防护	防火墙、网闸、光闸、UTM、准入控制系统、无线接入安全网关、上网行为管理	策略白名单原则、策略的优化、关键网络节点识别、威胁识别防范的有效性、审计的覆盖范围及粒度
	访问控制		
	入侵防范	IPS、IDS、抗 APT 攻击系统、威胁情报检测系统、抗 DDOS 攻击系统、WAF	
	恶意代码和垃圾邮件防范	防病毒网关、垃圾邮件网关	
	安全审计	网络审计系统、网络流量回溯系统	
	可信计算	基于可信根产品	
安全计算环境	身份鉴别	堡垒机、终端安全管理与审计、4A 系统	安全计算环境的组成、身份鉴别技术有效性、访问控制策略的粒度、审计的覆盖范围及粒度、漏洞验证与修复、威胁的识别范围、重要数据的分级分类、敏感信息的识别
	访问控制	堡垒机、终端安全管理与审计、4A 系统	
	安全审计	堡垒机、终端安全管理与审计、日志审计系统、数据审计系统	
	入侵防范	漏洞扫描系统、终端检测与响应（EDR）	
	恶意代码防范	防病毒软件	
	可信验证	基于可信根产品	
	数据完整性	网页防篡改产品	
	数据保密性	数据加密、数据防泄漏	
	数据备份恢复	本地和异地备份系统	
	剩余信息保护	应用系统开发商解决	
	个人信息保护	数据脱敏、业务安全网关	
安全管理中心	系统管理	特权账号管理系统	三权分立、独立认证、独立审计
	审计管理		
	安全管理		

	集中管理	日志审计系统、安全管理平台、态势感知平台	管理区的保护、汇总分析能力、联动效果、事件的处置能力

资料来源：东软集团，动脉网

② 等级保护云扩展要求技术部分对应措施

表 2 等级保护云扩展要求技术部分对应措施

等保要求	控制要求	所需产品	实现机制
安全通信网络	网络架构	云安全资源池（SND）	根据云计算的服务模式，基于云集成商和与云服务客户的不同责任进行安全的落实。
安全区域边界	访问控制	虚拟化防火墙、微分段微隔离产品	
	入侵防范	云抗 D、云 WAF	
	安全审计	云安全资源池（SND）、云工作负载保护平台	
安全计算环境	身份鉴别	云堡垒机、云工作负载保护平台	
	访问控制	云工作负载保护平台	
	入侵防范	云工作负载保护平台	
	镜像和快照保护	云集成商统一保护	
	数据完整性和保密性		
	数据备份恢复		
	剩余信息保护		
安全管理中心	集中管理	云安全资源池（SND）、云工作负载保护平台	

资料来源：东软集团，动脉网

2） 管理措施

现阶段医院等级保护建设中要求的管理措施更多的是通用的制度，并没有根据系统重要程度进行拆分。所以对于完成内网核心系统等级保护建设的实体医疗机构，管理制度可以结合互联网医院

业务系统特性复用与完善。对于未进行过等级保护建设的实体医疗机构，需注意在不同的互联网医院建设模式下，秉承“谁主管谁负责”的原则。因此实体医院应结合业务状况，按照等级保护管理要求，落实互联网医院业务及其相关信息系统安全管理制度。

表 3 等级保护管理部分要求

类别	内容
总体管理架构	《ISMS 文件框架》
安全管理制度	《信息安全方针及安全策略文件》《文件评审及发布制度》
安全管理机构	《信息安全领导机构组成与职责》《信息安全部门岗位职责说明》《授权及审批管理制度》《沟通与合作管理》《安全检查和审核管理》
人员安全管理	《信息系统人员管理制度》《信息安全培训管理》《第三方安全管理规范》
系统建设管理	《网络与信息系统安全设计规范》《IT 产品采购管理制度》《软件开发管理规范》《代码编写安全规范》《外包软件开发管理》《工程实施管理制度》《工程测试验收管理》《系统交付管理》《服务商安全管理》
系统运维管理	《机房安全管理制度》《办公环境保密管理》《资产安全管理制度》《介质安全管理制度》《设备安全管理制度》《安全和监控中心管理》《网络安全管理制度》《系统安全管理制度》《主机运维操作规程》《恶意代码防范管理》《账号口令和权限管理》《变更管理程序》《备份与恢复管理》《安全事件报告和处置》《信息系统应急预案》

资料来源：东软集团，动脉网

4.3 业务安全是互联网医院发展基石

等级保护标准作为我国网络安全领域最重要的标准之一，是一套得到长期实践的体系化的标准，从技术和管理上具备一定的指导性和全面性。但随着业务间耦合度的逐渐提升及业务特性的多变，合规基础安全建设加业务安全建设将会成为更有效的安全防护思路。因此互联网医院网络安全建设需要在等保建设的基础上从业务角度识别互联网医院的安全风险。在全面建立安全防护体系的基础上，增加互联网医院业务安全防护措施。解决以下医疗机构、居民、第三方机构在互联网医院建设中的担忧，才能保证互联网医院业务稳定、顺利开展。

4.3.1 互联网医院对内网安全影响最小化

在复杂的攻击形势下，60%的医疗行业网络安全事故，都是因为同一个误区：认为隔离就是安全。

面对互联网医院与内网核心系统的交互需求，单纯的隔离已无法保障院内系统安全。内网与互联网交互安全应该从以下两个方面落实：

1）降低外部风险

降低互联网医院对内网安全性影响的关键是梳理互联网医院与内网的连接点。将连接点控制在安全范围内，医疗机构内网安全性将大幅度提升。现阶段建立医院集成信息平台仍需一段时间，因此当前互联网医院与院内核心系统的交互，仍以部署前置机的形式落实，前置机作为连接内外网的桥梁。其次，部分医疗机构业务终端并未进行内外网隔离，部分业务终端既可以访问互联网医院也可以访问内网。

因此降低互联网医院对内网安全影响应主要从前置机和业务终端两个方面入手。首先应通过主机加固、病毒检测等手段，确保前置机和业务终端安全性。其次，前置机与内网交互涉及数据传输，因此应加强前置机与内网流量安全防护，根据业务传输需求，利用单向网闸或双向网闸实现数据摆渡，并通过防病毒网关等设备对病毒进行过滤。对于业务终端与内网交互，主要是访问行为，这也是医疗机构常常忽视的安全建设内容。2018 年以来医疗机构被勒索病毒攻击，绝大多数是终端设备先被攻击，然后通过端口对系统发起攻击。因此应在不影响业务的情况下采取严格措施限制内网核心系统对互联网以及业务终端暴露的端口，并关闭 445 等高危端口。

2） 提高自身防护能力

面向不断扩展的互联网医院服务，内网与互联网的边界将越来越模糊。单点的防护只能解决一时的问题，应该落实院内核心系统等级保护建设工作，建立内网完善的安全防护体系，全面提高院内核心系统安全防护能力。

4.3.2 保证互联网医院面向用户的可用性

1） 多种技术结合解决医疗机构长期面临的“黄牛抢号”问题

我国医疗资源供需失衡问题日渐突出。目前医疗机构从分级诊疗、提升医院就诊效率等政策及技术维度尝试解决这一问题。但整体推进依然需要一定时间。伴随着人民生活质量的提高，大医院的医疗资源与患者需求的差距将越来越显著。因此在提高医疗资源的同时，利用号源随机释放、

加大验证码强度，设计行为识别系统等技术手段，是目前医疗机构解决“黄牛抢号”问题的有效手段。

号源随机释放就是指患者取消预约或者退号的号源不会立即释放到资源池中，而是经过一段随机时间后，通过相应技术手段将这些号源重新释放到资源池中，以便其他患者再次预约和挂号。通过这种技术手段随机放号，也就意味着号贩子想把之前已经预约好的号源退掉时，就无法轻易用他的买主的帐号再预约回来，这样就大大增加了其他患者预约的成功率。但是随机释放的号源也不一定能为真正需要的用户所约到，相反，号贩子有可能利用外挂程序不断的查询号源，从而给网站服务器带来一定的压力。

加大验证码的强度，不但要增加长度，至少到 8 位以上，而且必须对验证码进行扭曲、污染，必要时可以加入中文汉字，使得外挂使用者在需要输入验证码的环节无法用外挂识别，只能通过人工识别并输入。但是面对年老或不熟悉上网操作的用户，过于复杂的验证码无疑增加了其网上挂号的难度。

互联网预约环境下号贩子主要利用退号、绑定、抢号等环境的漏洞进行技术抢号。医院管理和技术部门针对这些情况制定应对方案，在单个账号管理、号源管理退号管理等维度上利用大数据技术识别正常用户操作行为，封堵和限制异常操作，例如控制单个用户在单位时间内的挂号次数等。这类单纯从安全角度采取的应对手段往往在短时间内能够限制一定的非正常访问请求，但同时也会“误伤”大量正常用户的请求，例如不熟悉上网操作导致重复挂号将可能导致正常用户请求被“误杀”、一个账号为多个家属挂号被“误杀”、某段 IP 被整体禁用后这段 IP 对应的这个地区的所有用户都无法正常挂号等，产生用户体验下降甚至对人民群众正常的求医问药产生障碍。另外，魔高一尺道高一丈，这类业务安全问题如果单纯从网络信息安全技术角度寻找解决方案往往会在前期奏效，但后期随着“黄牛”手段迭代提升，防护效果会大幅削弱，甚至是不再奏效。所以这类业务安全问题应该从安全技术加业务属性两个维度实施业务安全解决方案，单一的网络信息安全技术、传统 Web 应用安全产品难以奏效。

2） SD-WAN 为互联网医院业务连续性提供技术支撑

广域网具有网络状态波动性大、随机性强的特点。随着互联网医院生态的快速发展，各种互联网医院服务将大量增加，服务内容、连接边界将不断扩大，关键业务需要选择一条可靠路径进行传输，降低延迟和丢包率。利用 SD-WAN，互联网医院业务可以在广域网上实现不同等级的 QoS（服务质量），实现按需分配网络资源，实现弹性网络，实现网络切片与分层。面对持续发展的

互联网医院业务，业务的多样性决定了 SD-WAN 技术对于互联网医院建设的重要性。

《互联网医院管理办法》规定，互联网医院网络至少由两家宽带网络供应商提供服务，结合 SD-WAN 技术，实现业务智能负载、无缝切换等业务场景，大大降低由于互联网诊疗业务逐步增加可能产生的高峰期丢包或时延的业务风险。

4.3.3 解决个人健康数据安全问题

互联网医院安全防护从本质上讲依然是数据防护，尤其是检验、医生笔记等涉及患者隐私及重要信息的数据。因此必须加强互联网医院信息安全体系建设，保障数据信息安全，防止医疗健康数据泄露。目前，我国互联网医院正处于发展初期，在保障医疗信息隐私与安全的前提下，应本着鼓励发展的原则，在共享数据的同时，寻找“隐私保护”与“开放利用”之间的平衡。建议从制度建设和信息技术两个维度来构建互联网医院信息安全保障体系。

1）制度建设方面

需要制定互联网医院信息安全规范和医疗数据分级分类审查制度，对医疗数据的采集、传输、储存、应用、转让等全周期进行监管。医疗数据分级可根据数据重要程度和风险级别以及对个人健康医疗数据主体可能造成的损害以及影响的级别。根据《健康医疗数据安全指南》，健康医疗数据可以分为个人属性数据、健康状况数据、医疗应用数据、医疗支付数据、卫生资源数据以及公共卫生数据等类别。

2) 信息技术保障方面

数据传输：综合利用身份认证、传输加密等技术确保数据传输安全性。

数据存储：利用数据审计、数据加密、授权管理、访问控制、身份认证等技术手段从安全评估、实时监测、主动防御、全面审计多个方面确保数据存储安全性，防止患者隐私数据泄露。

数据共享：可参考《信息安全技术 个人信息去标识化指南》，对共享数据进行去标识化处理。去标识化的数据应用于受控公开共享或领地公开共享（控制者完全控制的环境），宜通过数据使用协议约定数据使用目的、方式、期限、安全保障措施等。去标识化策略从不对个人造成危害这个角度落实，解决数据可用性和数据安全的平衡问题。

表 4 共享数据标识化处理

属性	去标识化方法建议	适用数据
姓名（例如：受试者姓名、研究者姓名、医生姓名等）	建议删除或置空	受试者姓名、医生姓名、研究者姓名、家庭成员姓名
联系方式（例如：个人电话号码、邮箱、详细住址等）	建议删除或置空或泛化 例如：住址只具体到市县级，隐藏县级以下地址	个人电话号码、邮箱、账号、住址
日期（例如：入院日期、治疗日期、手术日期等）	建议采用“时间偏移方法”、转换法或泛化 例如： 为不同研究项目定义不同的随机偏移量，通过日期时间+或- 随机偏移量进行数据扰动，以实现数据的去标识化 例如： 入院日期2018-01-01 + 随机偏移量 100 = 入院日期：2018-04-11 出院日期2018-04-01 + 随机偏移量 100 = 出院日期：2018-07-10 出院日期 - 入院日期 = 90天 通过该方法可以保证数据去标识化的同时保证计算逻辑正确。 转换法即用其与其他日期运算得到结果来替换，例如年龄、住院天数。 泛化只保留年月，甚至只保留年。	医疗应用数据中能通过数据分析关联到个人的时间信息：例如入院日期、出院日期、手术日期等
出生日期	建议删除、置空或者替换为年龄	出生日期
年龄	建议采用“数据泛化”方法 例如 - 年龄≤89 或者 >89 - 年龄区间 <25, 25-29, 30-34,...,85-89 >89	年龄
号码（例如：邮编、身份证号、社保号等）	建议删除或置空 如需要利用号码的唯一性进行逻辑分析，例如通过身份证	身份证号、社保卡号、工作证号、

	号判断多份病历是否属于一个人的场景，可采用基于原数据的随机化产生唯一标识进行替换。 如需要利用邮编等隐含地理信息的号码，可采用扰动和泛化方法进行处理。 例如：原始邮编记录100080，去标识化后100***	居住卡号
医疗机构内部所用号码	建议置换或删除 通过这些号码进行逻辑分析而需要保留的，可采用基于原数据的随机化产生唯一标识进行替换。 如不需要这些号码进行逻辑分析，则删除这些号码。	检验结果报告单号、检查报告单号、住院号、门（急）诊号等

资料来源：《健康医疗数据安全指南》

4.4 网络安全人才是医疗机构网络安全根本

1) 网络安全人才培养

任何规范化的企业管理，都不可避免地需要引入流程，医疗机构运维管理也不例外。完全基于个人经验和判断的操作，往往隐藏着重大的故障风险，医疗机构信息中心要强化流程管理。任何重要的操作，必须严格按照流程执行。建立流程文化是数据中心规范化管理的一个重要环节，数据中心最重要的三类流程是标准操作流程(SOP)、维护保养操作流程(MOP)、应急响应流程(EOP)。

同时医疗机构数据中心基础设施牵涉到电力、暖通、弱电、消防、建筑等诸多专业，每一个数据中心的配置和特定的操作流程都不完全相同，因此对于医疗机构信息中心来说，在数据中心运维方面需要学习的专业知识非常多，定期的专项学习培训应该成为医院运维团队管理的重要部分。

2) 网络安全人才引进

网络安全人才的培养具有特殊性，从学习的角度来说，网络安全的攻防是不对称的，科班出身的人普遍接受的教育是怎么防御，很少知道怎么进攻。不知道攻击的防御，容易落到纸上谈兵。因此医疗机构在培养内部网络安全人才的同时，应该注意网络安全能力的外部引进。适当选择安全厂商提供的安全服务、咨询服务、运维服务，弥补医院专业安全技术人员不足，最大程度减少因网络安全事件所带来的医院运营中断以及管理成本增加的风险。

五、东软 NetEye 互联网医院安全最佳实践

5.1 以业务安全助力互联网医院网络安全体系规划

网络安全建设根本是为业务提供支撑，保障业务稳定运行。东软 NetEye 以业务驱动安全为理念，结合东软集团多年的医疗行业从业经验以及东软 NetEye 网络安全从业经验，将网络安全与业务融合，为互联网医院网络运营者提供既满足合规需求又能够解决医疗业务互联话产生的新网安全挑战的解决方案。解决网络安全建设与业务发展割裂的问题，从网络安全的角度为医疗机构提供互联网医院网络安全规划思路，为医疗行业网络运营者赋能。

5.1.1 东软 NetEye 互联网医院网络安全框架

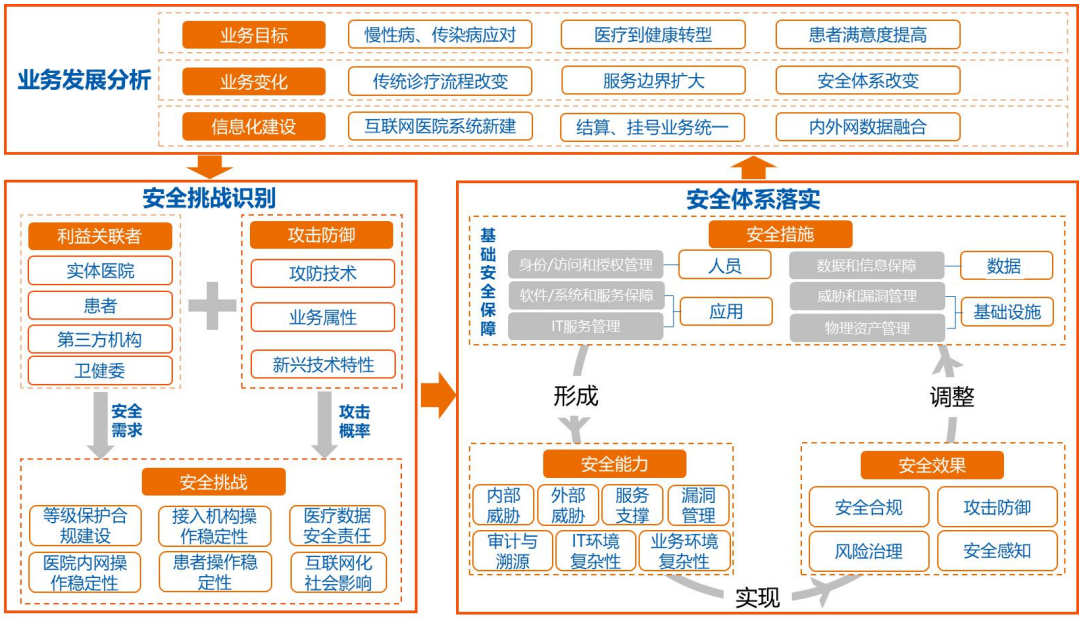
东软 NetEye 认为互联网医院网络安全规划建设应重点关注以下几点：

1) 互联网医院的信息化建设包含互联网医院系统上线、内外网数据融合以及接入机构网络建设三个方面。

2) 从互联网医院建设中的利益相关者（实体医院、患者、第三方机构、卫健委）以及攻击防御技术角度出发，互联网医院网络安全面临的根本挑战，主要包括等级保护合规建设、接入机构操作稳定性、医疗数据安全责任、医院内网操作稳定性、患者操作稳定性以及互联网化社会影响几个方面。

3) 互联网医院网络安全建设应围绕数据、应用、人员和基础设施四个方面提供全面的防护措施。通过安全措施的部署和组合，形成能够抵御内部威胁、外部威胁等安全能力。最终达到安全合规、攻击防护的安全效果，应对由于信息化变化产生的安全挑战。

图 16 互联网医院网络安全规划流程



资料来源：东软集团，动脉网

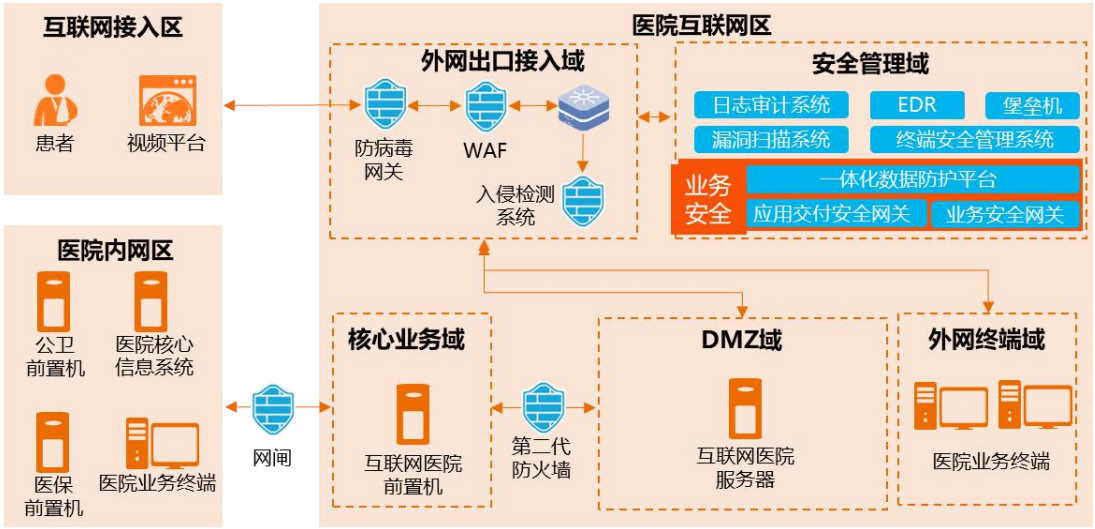
5.1.2 东软 NetEye 互联网医院网络安全防护模型

东软 NetEye 根据互联网医院建设模式，从部署方式的角度提出三种模式下的基本防护模型，为互联网医院网络安全建设提供思路。

1) 本地部署

本地部署模式医院承担全部安全职责，包括物理环境、网络建设、互联网医院平台防护以及院内核心系统保障等，所需部署防护措施如下图所示。

图 17 本地部署所需部署防护措施

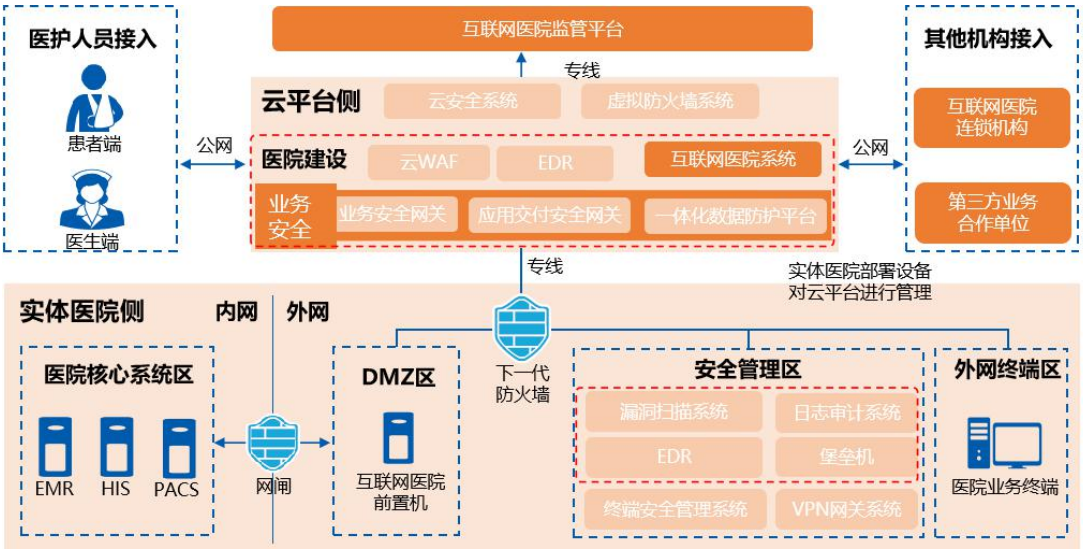


资料来源：东软集团，动脉网

2) 第三方机构提供基础设施

第三方机构提供基础设施情况下，第三方机构负责承载互联网医院物理环境和网络搭建。医院需保障互联网医院平台安全、实体医院互联网医院终端安全以及院内核心系统保障等，所需部署防护措施如下图所示。

图 18 第三方机构提供基础设施所需部署防护措施



资料来源：东软集团，动脉网

3) 资源融合模式

第三方机构提供承载互联网医院环境以及互联网医院系统。医院仅负责接入互联网医院的业务终端安全性、互联网医院业务安全性以及内网核心系统安全性。所需部署防护措施如下图所示。

以上防护措施仅体现部分所需产品，具体落实措施包括策略配置、管理制度配合等方面需结合实际情况进行调整。

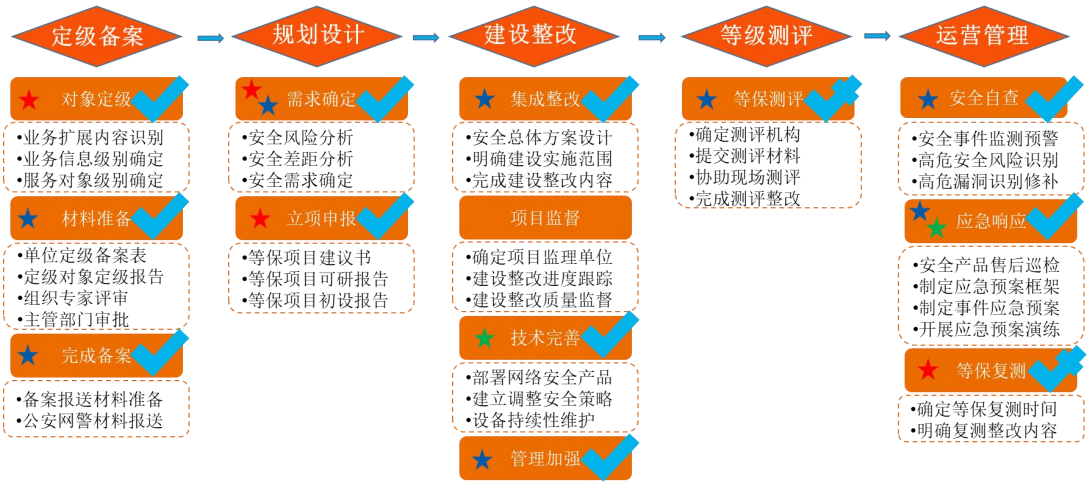
5.2 一体化服务助力互联网医院网络安全建设落地

5.2.1 东软 NetEye 基于等级保护建设的网络安全服务

互联网医院等级保护三级建设是互联网医院上线的必要条件。等级保护建设是一项体系化建设工作，包括定级备案、规划设计、建设整改、等级测评、运营管理五个关键步骤。在等级保护建设流程中涉及材料编制、机房改造、产品部署、管理制度落实等一些具体工作。多数医院由于自身人员等条件限制，难以独立完成。东软 NetEye 具备多年等级保护建设经验，可通过服务助力医院完成互联网医院等保三级建设。

东软 NetEye 为医疗机构提供一体化等级保护建设服务，针对 5 阶段能够完成 10 项工作任务，辅助完成 2 项工作任务，全面支撑等级保护建设工作。协助医院从信息安全和业务连续性两个角度确定定级对象以及定级级别，采取分期、分批建设方式进行规划，为网络运营者提供精准的咨询规划与现场服务。在全部五个环节，依托专业人员（CIIP-A、CISP、等保工程师）、集成能力（等保建设资质、集成资质、等保集成经验）、等保生态（安全友商、测评机构），为网络运营者提供高效的集成实施与保障服务。

图 20 东软 NetEye 一体化等级保护建设服务



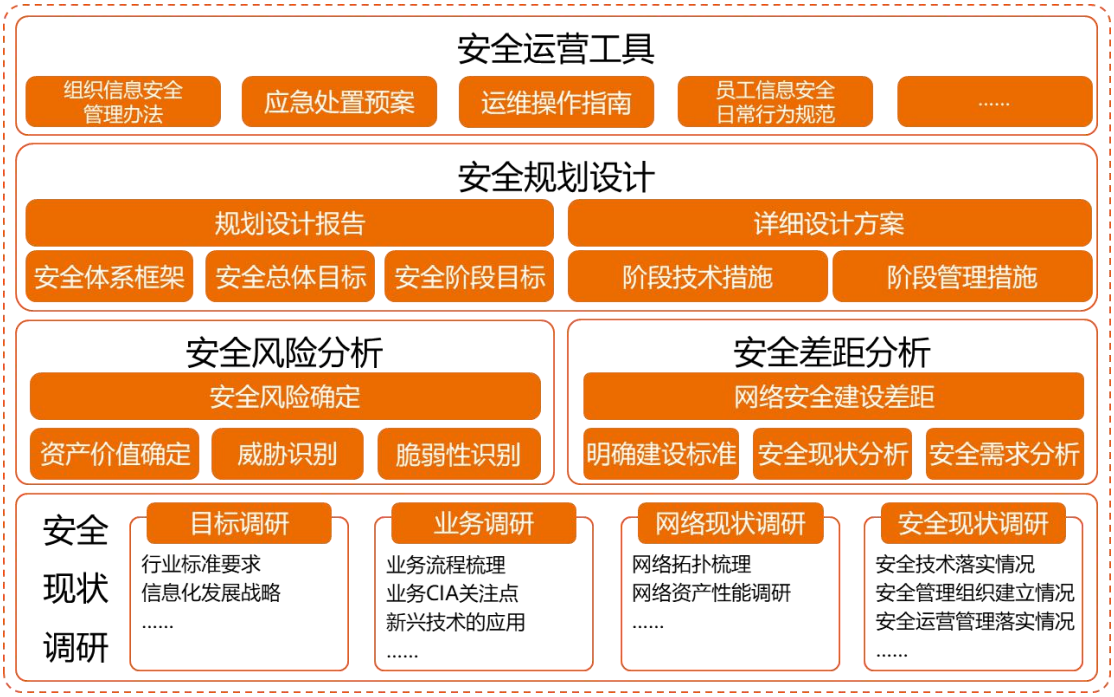
资料来源：东软集团，动脉网

5.2.2 东软 NetEye 咨询规划服务保障医院网络安全规划与实施

东软 NetEye 提供围绕核心业务的稳定运行的咨询规划服务，专业人员通过调研、分析、设计、运营赋予网络安全建设运营更为统一的建设思路、更为精准的防护策略、更为细致的建设任务、

更为持续的保障能力，减轻医疗机构网络安全建设运营压力，构建体系化、动态化的网络安全运营保障体系。

图 21 东软 NetEye 咨询规划服务



资料来源：东软集团，动脉网

东软 NetEye 咨询规划服务从服务的角度解决以下互联网医院网络安全建设存在的问题：

1） 梳理安全目标，确保由上到下目标一致性

通过东软 NetEye 咨询规划服务，与信息化主管领导、关键业务部门主管领导进行访谈，明确网络安全建设的战略和目标。识别医疗机构的安全风险、安全人员、安全建设等基本情况，确定网络安全建设的总体需求和整体框架。制定阶段性建设计划，确保了信息化建设和网络安全建设的同步性,从而保证了信息化建设发展过程中业务的持续稳定运行。编制网络安全规划与设计文档，明确运维人员的网络安全建设目标和工作，并提供工作中的指导建议，解决“书不尽言，言不尽意”的问题。通过指导和修正，确保网络安全建设理念落实效果。

2） 制定可执行的标准操作流程，提高运维效率

互联网医院的网络安全运营常常呈现资产众多、人员紧缺、网络覆盖广等特点。医疗机构作为互联网医院责任方，存在业务运维权限设置混乱，数据资产操作和使用监控缺失等问题，加之人员

不足使管理制度疲于表象，导致安全技术手段成摆设，大量安全事件堆积，增加了用户的安全运维压力，降低了网络运营的效率。

网络安全运营是一个持续改进和调整的过程，通过持续开展东软 NetEye 咨询规划服务，对业务的运转流程进行深入分析，明确了网络安全运营的核心关注点，通过全面的用户资产信息梳理，确定了网络安全运营的问题出处。通过安全管理制度的改进和完善，将用户现有安全技术措施与安全管理机制进行有效结合，既保证了安全技术手段的防范处置效果，又提升了网络安全事件的处理能力，从而有效提升了网络安全运营的效率。

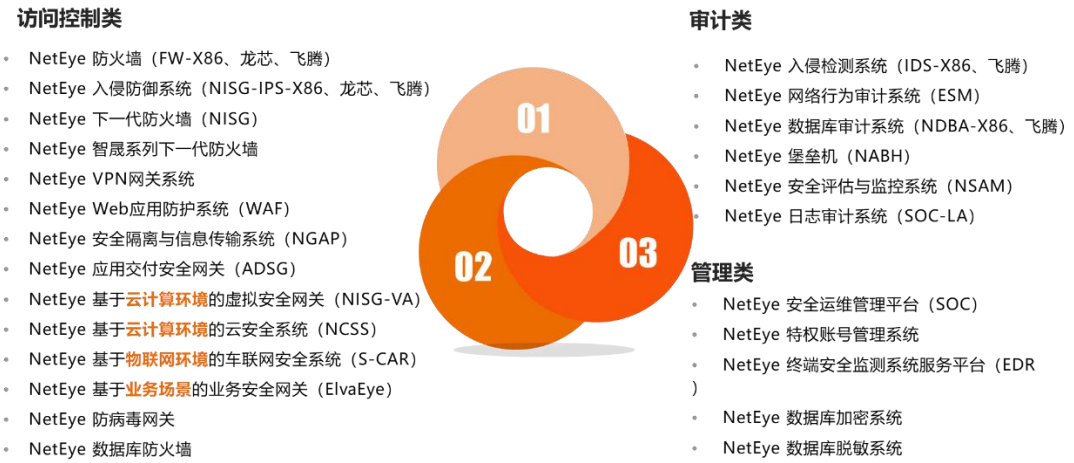
5.3 专业的网络安全产品助力互联网医院网络安全建设落地

网络安全产品是互联网医院网络安全体系落实过程中必不可少的一部分，稳定可靠的安全产品可以保障业务顺利开展，减少运维人员工作负担。东软 NetEye 自 1996 年开始研发并生产网络安全产品，建立包括研发、功能测试、性能测试、出厂前拷机等完善的生产机制，为互联网医院安全建设提供全方位、可靠的网络安全产品，帮助客户建设和完善安全防护体系。

5.3.1 东软 NetEye 全面的网络安全产品助力互联网医院合规建设

东软 NetEye 网络安全产品包括访问控制类、审计类以及管理类三大部分并且具备云安全产品。基本能够覆盖等级保护三级建设中全部所需的网络安全产品，从网络安全产品方面为互联网医院合规建设提供支撑。

图 22 东软 NetEye 网络安全产品



资料来源：东软集团，动脉网

由于医疗机构患者量、开展服务内容存在差异，导致网络安全需求不同。东软 NetEye 为满足不同医疗机构以及场景的需求，推荐了不同型号的网络安全产品。

1） 面向三级医院互联网边界防护

数据大流量、数据类型复杂是三级医院开展互联网医院业务的主要特点。因此具备高性能、高准确率的互联网医院边界防护措施是三级医院主要需求。东软 NetEye 防病毒网关基于病毒特征建立 1500+万条病毒特征库，可对实体医院、医疗服务、第三方医疗机构等流入互联网医院的多种数据进行深度检测，有效应对多形态病毒、恶意软件逃避技术等不易检测的攻击行为。同时东软 NetEye 防病毒网关具备防火墙和 VPN 功能，实现一款产品满足多个需求。针对不同访问需求建立访问控制策略，并为远程运维人员提供专用的安全运维通道，建立全面可控的访问路径，防止非法访问和过度开放带来的安全风险。

2） 面向基层医疗机构互联网边界防护

乡镇卫生院、村卫生室等基层医疗机构不具备独立的机房且业务简单、数据量小。面对这种情况，东软 NetEye 提出了专为中小型用户定制的桌面级集成安全网关。由于其自身体积小，更加适用于基层医疗机构物理环境。同时东软 NetEye 桌面级集成网关具备访问控制、入侵防御、防病毒、URL 过滤、VPN 等传统集成网关所具备的全部功能。通过部署东软 NetEye 桌面级集成安全网关，可以建立基层医疗机构的网络边界防护措施。为基层医疗机构建立访问互联网医院的专用安全通道，避免互联网访问的不安全因素。

3） 面向医疗机构内网与互联网医院交互防护

东软 NetEye 安全隔离与信息传输系统（网闸），实现一定意义的“物理隔离”，将 TCP/IP 协议全部剥离，将原始数据通过存储介质以“摆渡”方式传输到内部系统中。这样防护方式实现数据同步过程中，有效过滤了以 TCP/IP 协议为载体的攻击行为，包括泪滴攻击、TCP 会话劫持等，并对数据包进行初步检测识别正常业务流量中夹杂的攻击行为。同时东软 NetEye 安全隔离与信息传输系统延迟在 1ms 以内，可满足互联网医院与实体医院数据传输实时性要求。东软 NetEye 下一代防火墙，可通过策略设置，实现覆盖网络 L2-7 层的安全防护，基于用户组、策略组限制院内访问行为，对院外核心系统（互联网医院系统）与院内核心系统（HIS、PACS、EMR）交互行为进行全面管控，限制访问行为，服务器仅开放必要的端口和服务，同时关闭网络环境中暴露的高危端口和服务。屏蔽外部非法人员的恶意访问，阻断内部非法操作产生的安全隐患，确保网络的使用得到有效控制。

5.3.2 东软 NetEye 先进网络安全技术助力互联网医院业务防护

东软 NetEye 以防火墙为代表的网络安全产品具有业界领先的技术，赋能医院业务安全发展，为客户带来明显的价值收益，优势如下：

1） 大流量、高带宽

设备的不稳定性 80%由 CPU 过载导致，而东软 NetEye 防火墙提供两种 ASIC 芯片，分别专门处理网络层和应用层的数据转发，CPU 得以解放出来只负责新建会话建立连接。这种分布式处理方式，有效保障了稳定运行能力。在大流量高带宽的场景下，也能够快速无损耗地转发流量，适合互联网医院业务、远程诊疗业务的开展，避免让安全产品成为制约医院业务开展的瓶颈。

2） 低延时

东软 NetEye 防火墙具有独特的 X86+ASIC 硬件设计架构，ASIC 芯片对各种网络环境下数据包处理都能实现极低的延迟，最高延时 8us，最低延时 3us，而电信测试中 96 微秒就能通过，一般防火墙能达到 70 微秒就已不错，极低的延时大大降低了设备对整体网络性能的损耗。随着 5G 网络的广泛应用，其竞争力优势将更加凸显。在互联网医院远程医疗的场景，可保障视频影像等清晰流畅地传输，两端实时同步不延迟。

3） 业务延展性强

- 接口密度大，类型丰富：当前不少医院内部网络尚未升级改造成千兆或万兆光纤网络，未来随着 5G 的广泛应用，网络升级改造不可避免。东软 NetEye 防火墙网络接口数量大，类型丰富，可扩展支持 Combo 口、光电共享口、千兆光口、万兆光口，可满足不断增长的各业务网络区域的接入防护需求。

- IPv6 无缝升级：随着 IPv4 地址空间的耗尽，许多应用需要升级改造为 IPv6。工信部于 2019 年曾发布《关于开展 2019 年 IPv6 网络就绪专项行动的通知》，以深入贯彻落实《推进互联网协议第六版(IPv6)规模部署行动计划》，全面提升用户渗透率和网络流量，加快提升我国互联网 IPv6 发展水平。随着 5G 的商用普及，医院网络将运行越来越多具有 IPv6 地址的医疗设备，对网络性能运行要求也越来越高。东软 NetEye 防火墙支持 IPv4 和 IPv6 双栈协议，无需改造现有的 IPv4 网络应用，可通过 ALG 技术直接访问 IPv6 应用；并且在 IPv6 网络环境下，性能运行无损耗。东软 NetEye 防火墙对 IPv6 的良好兼容性可支持更多的医疗传感器、可穿戴设备接入，可满足未来医疗物联网或智慧互联网医院的运行需求。

4） 一体化防护，功能丰富

东软 NetEye 防火墙，同时支持防病毒、反垃圾邮件、DLP、IPS、Web 过滤、防僵尸网络、防 APT 攻击、应用识别与控制、广域网优化功能、IPSec VPN、SSL VPN、虚拟防火墙、SSL 检测等功能。一台物理防火墙具备多款产品的使用功能，满足等保多项高危风险项要求，如恶意代码防范、入侵攻击防范等。对应 4.2.2“等级保护通用要求技术部分要求对应措施”列表中的安全通信网

络、安全区域边界、安全计算环境需求，覆盖网络架构、通信传输、边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、数据保密性、数据完整性等多个等保测评控制项。

针对入侵攻击和恶意代码的检测防范一般依赖特征库，衡量检测防护能力的强弱主要在于特征库数量的大小。东软 NetEye 防火墙具有数量达 1500 万种的病毒特征库，而国内传统安全产品病毒库数量多在 500 万左右；东软 NetEye 的 IPS 特征库在 1 万左右，国内安全产品一般在 5000-8000 左右；东软 NetEye 的 URL 库的数量是 2.5 亿左右，国内安全产品一般 1.4 亿左右，东软 NetEye 优势明显。

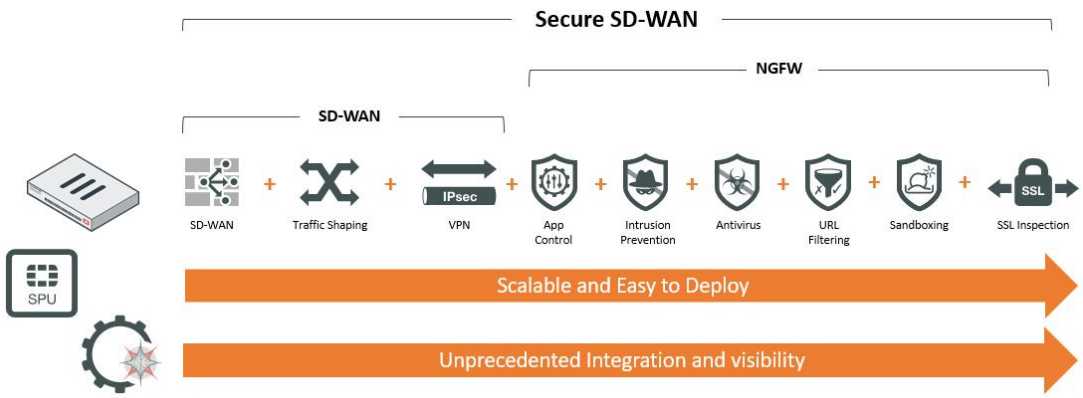
5.3.3 东软 NetEye 新兴网络安全技术助力医疗互联网转型

互联网医院是实体医疗机构向互联网转型的关键举措。在转型过程中互联网医院将面临新的网络安全挑战。东软 NetEye 将机器学习、SD-WAN 等先进技术运用到网络安全产品中，帮助医疗机构应对互联网医院业务转型过程中的新挑战。

1）网络安全与 SD-WAN 融合，建立稳定、可靠的互联网链路

医疗机构选择 MPLS 和专线的第一原因是保障链路通信的稳定性，第二个原因是保障数据传输过程中的安全性。而 SD-WAN 技术只能保证链路通信的稳定性，因此东软 NetEye 在传统防火墙的基础上将 SD-WAN 与安全防护功能融合，提出更全面的解决方案。利用 SD-WAN 技术确保互联网医院关键业务应用的高可用性和 QoS（服务质量），且根据优先级 SLA 或链路质量指标选择链路，在 SLA 稳定后恢复到所需的链路。通过具备 SD-WAN 和 VPN 功能的防火墙，对传输链路进行加密，并对流量进行过滤。保障互联网医院边界安全的同时确保业务的稳定性。在两个服务商情况下，SD-WAN 技术比起 MPLS 更具稳定性，安全方面 VPN 加密技术比起 MPLS 更加安全，因此 SD-WAN 与网络安全融合的产品可以更好地替代 MPLS 技术。东软 NetEye 对 SD-WAN 产品中的远程零接触部署、WAN 链路故障和切换、服务质量保障的动态链路选择、链路饱和与拥塞、链路选择条件与基于应用的选路等关键功能和性能进行了测试，均位于市场前列，旨在为互联网医院通信提供稳定、可靠的互联网链路。当互联网医院系统部署在公有云场景下，实体医院终端与云上互联网医院系统的访问请求，在多出口链路的情况下，则可在实体医院出口部署 SD-WAN，实时探测对端链路情况，自动选择最优链路。

图 23 网络安全与 SD-WAN 融合



资料来源：东软集团，动脉网

2) 解决黄牛抢号问题，提高患者满意度

黄牛抢号难以应对的根本原因是抢号方式多种多样，包括人工抢号、抢号软件、盗用等，单一的技术方式难以应对。东软凭借软件开发对各行各业的业务经验，凝聚了多年业务风控经验，开发东软 NetEye 业务安全网关，综合人机验证、设备指纹、实时风险决策、行为分析技术，对互联网医院在线挂号用户访问数据进行分析，解决互联网医院面临的黄牛抢号问题。

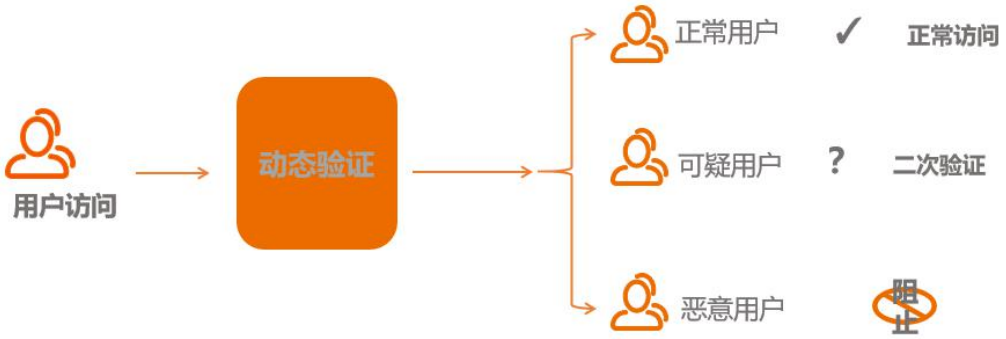
图 24 解决互联网医院黄牛抢号问题

资料来源：东软集团，动脉网

人机识别

当用户访问互联网医院时，采用基于“JS 挑战”的验证方法，向用户客户端发送特定的、浏览器能解析的应答 JS，通过“挑战”的用户会带有一个特定的 Cookie 值，线上实时模型会依据此 Cookie 的信息来决定是否放行此请求。未通过挑战的认定为机器行为进行阻断，通过挑战的认定为正常用户访问行为进行放行，利用此方法可以解决恶意软件刷号的问题。

表 25 人机识别系统



资料来源：东软集团，动脉网

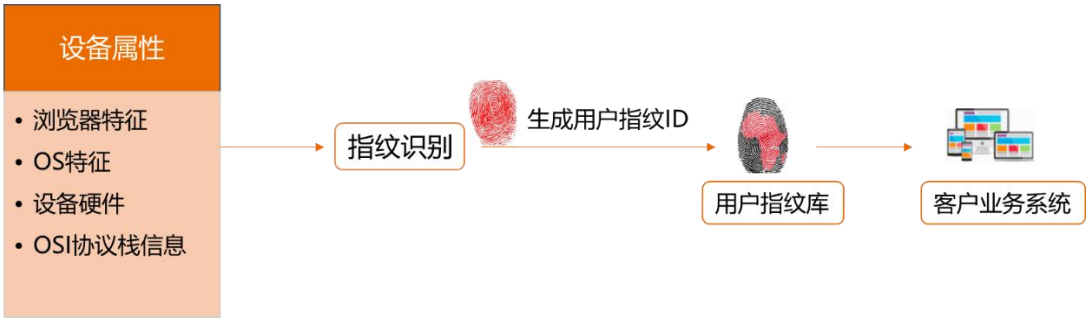
设备指纹

传统的安全防护设备和措施，通常以 IP 为维度去做访问控制和阻断等策略，实际误删率极高。比如小区互联网出口通常为几个固定 IP，一旦小区内某用户触发了安全规则 IP 被目标网站拒绝访问，将直接导致整个小区都无法访问。（移动网络环境 4G 出口同理。）

为更精准的识别互联网用户，防止误伤，引入设备指纹技术。设备指纹采用在网站端集成 JS 脚本来采集终端设备的硬件、网络、浏览器等非敏感的设备特征信息，然后提交到服务端，通过特定的 hash 算法为每一个终端设备生成一个全球唯一的设备指纹标识写入用户 cookie，伴随整个会话生命周期，进而实现对访客的服务鉴权、行为跟踪等。

一旦基于该设备指纹的用户触发了安全规则，将直接阻断此设备指纹的会话，不阻断 IP，防止影响统一 IP 出口的其他用户的访问。设备指纹作为风控产品链的关键技术之一，将其作为风险识别的重要维度数据，可以精准识别用户身份，能有效解决互联网医院中的盗号查询、欺诈等风险问题。

图 26 指纹识别风控技术

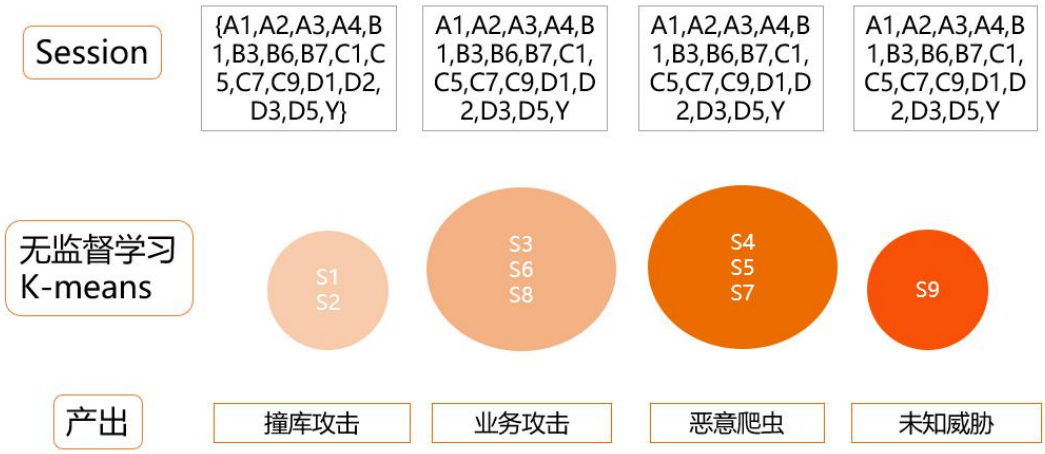


资料来源：东软集团，动脉网

行为分析

行为识别的核心就是给互联网用户画像，采用非监督式和监督式学习相结合的方式打造了一套基于多层动态模型的风险评分体系和决策系统，从而将设计聚焦在真正用户的动机和行为上。采用非监督式和监督式学习相结合的方式打造了一套基于多层动态模型的风险评分体系和决策系统，能够有效识别人工恶意抢号等行为。

图 27 行为识别原理



资料来源：东软集团，动脉网

实时决策

实时决策系统是一款基于设备指纹、规则引擎、指标策略、风险数据、机器学习等多项技术的业务风险防控产品，支持快速私有化部署，帮助客户快速建立自有的业务安全体系，解决仿冒、盗用、欺诈、作弊、垃圾、爬虫等各类风险。

实时决策引擎是一套强大的智能决策系统，支持包括实时决策、近线分析、离线挖掘的多层次决策分析。能够在毫秒级作出响应，利用策略和实时计算，同步识别风险，直接阻断恶意风险，或通过二次验证确认疑似风险。

近线分析能够进行 t+秒级和分钟级的近线计算，计算各种特征，为实时决策提供指标参数，并从更多维度观测安全状态，发现异常及时报警。

离线挖掘通过各种离线的挖掘和模型技术的使用，为实时决策和离线处置提供依据和能力，例如：特征挖掘、模型平台训练、用户风险画像、设备风险画像等。

图 28 实时决策系统

资料来源：东软集团，动脉网

5.4 网络安全人才培养与输出助力医疗行业网络安全发展

东软集团于 2000-2003 年先后在大连、南海和成都投资建设 3 所 IT 大学，构建了产学研互动生态系统，推进专业教育与实际需求间的衔接。2008 年，成立了 IT 人才实训中心，目前，在沈阳、大连、南京、成都和无锡已建立分布式的实训基地。通过以能力为导向的软件人才培养路径，帮助学生完成知识向行为、技能和工程实践能力的转化，为行业培养高质量人才，也为东软自身初级人才规模化的供应开辟重要渠道。

目前，东软在三地建立的信息学院，通过教育教学改革的不断探索与实践，已为经济和产业发展培养了大批实用化、国际化、个性化的 IT 应用型人才。同时，利用自身人才实训中心的培训优势，东软承接了一系列省内高校学生技能培训工作。学生通过在校期间的“准就业”提前适应了社会，开启了良好的职业生涯。这也为东软自身及其客户、合作伙伴持续性地获得专业人才奠定了基础。

增加信息安全专业，按照“岗位为目标、技能为本位、素质为基础”的三位一体模式，培养学生具有信息安全技术应用能力和信息安全的分析与实施能力，具有较强的操作技能，掌握一般的防黑客技术及防病毒技术，具备信息系统的安全性设计与信息安全软、硬件产品开发的基本素质，掌握信息安全学科的发展动向和与其他学科的交叉应用。使学生具有较强的信息安全方面的分析问题和解决问题的能力，特别是实际的动手能力，成长为具有良好的科学素养和职业道德的高技能实用型信息安全技术专业人才。持续为社会输送网络安全人才，满足网络安全市场需求。

免责申明:

本报告的信息来源于已公开的资料和访谈，蛋壳研究院对信息的准确性、完整性或可靠性不作保证。本报告所载的资料、意见及推测仅反映蛋壳研究院于发布本报告当日的判断，过往表现不应作为日后的表现依据。在不同时期，蛋壳研究院可能发布与本报告所载资料、意见及推测不一致的报告。蛋壳研究院不保证本报告所含信息保持在最新状态。同时，蛋壳研究院对本报告所含信息可在不发出通知的情形下做出修改，投资者应当自行关注相应的更新或修改。

研究团队:

动脉网蛋壳研究院:

罗仕明　执行总监

杨绍波　高级研究员

东软网络安全事业部:

王华铎　咨询方案部部长

李梅　　咨询顾问

蛋壳研究院（VBR）：

蛋壳研究院关注全球医疗健康产业与信息技术相关的新兴趋势与创新科技。蛋壳研究院是医健产业创投界的战略伙伴，为创业者、投资人及战略规划者提供有前瞻性的趋势判断，洞察隐藏的商业逻辑，集合产业专家、资深观察者，尽可能给出我们客观理性的分析与建议。

更多信息，请关注动脉网微信公众号：VCbeat

蛋壳研究院提供服务：

初创项目竞争力评估；初创项目战略规划；创投细分领域定制研究；蛋壳 VIP 会员研报畅读。

☎ 联系电话：023-67685030
✉ 电子邮箱：research@vcbeat.net

东软 NetEye：

作为中国网络安全行业的领导厂商，东软 NetEye1996 年成立，连续多年保持稳健成长。基于东软集团多年行业积累，提出业务驱动安全理念，将安全技术与业务发展深度融合，面向云计算、移动互联网、物联网、大数据、关键基础设施等新技术应用的快速发展和市场需求的不断变化，云安全支付网关、物联网安全、信息技术创新安全网关、数据中心防火墙、虚拟安全网关、桌面型无线安全网关、智能网联汽车信息安全、预警威胁管控平台等一系列创新产品因需而生，在政府、金融、能源、电信、医疗、交通及大中型企业中得到良好应用。

秉承多年的专业技术经验积累，东软持续为用户提供成熟、先进的网络安全产品以及高效、完善的安全解决方案与服务，努力将东软 NetEye 打造成为全球领先的网络安全产品及服务供应商。

更多信息，请关东软 NetEye 微信公众号：Neusoft_NetEye

☎ 400 655 6789(7*24 小时)
servicedesk@neusoft.com