CAICT 中国信通院　SANGFOR 深信服科技

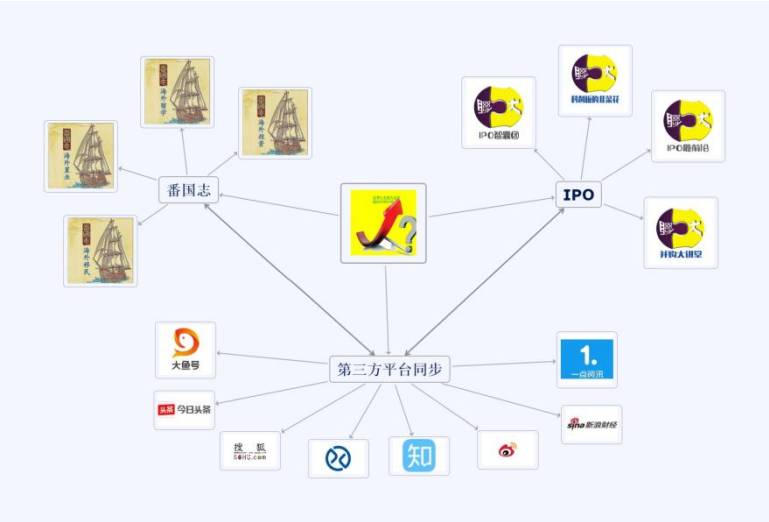
医疗物联网安全研究报告

（2021 年）

中国信息通信研究院安全研究所
深信服科技股份有限公司

2021 年 7 月

行业研究报告，服务于财经领域，整合发布高质量的财经相关领域精品资讯，提供各行业研究报告和干货。我们以微信公众号为基础，覆盖第三方平台为财经相关领域从业群体提供高质量的免费资讯信息服务。



我们的优势：

高质量的内容生产模式、多平台覆盖的整合营销服务、超百余万的高净值人群粉丝、专业、稳定的管理与团队。

旗下的矩阵号：

行业研究资本、行研资本、行研君、IPO 智囊团、IPO 最前沿、并购大讲堂、科创板的韭菜花、海外投资政策、海外置业政策、海外留学政策、海外留学、全球海外移民政策、番国志。

扫码关注公众号：

行研君　　IPO 最前沿　　全球海外移民政策

报告索取请加：report08　　商务合作请加：report998

版权声明

前　言

医疗物联网（IoMT，Internet of Medical Things）是物联网在医疗行业的重要应用。随着物联网、大数据、区块链、人工智能等先进技术的广泛应用，医疗物联网对加快“健康中国”建设和“智慧医院”“智慧诊疗”等推动医疗健康产业智慧化转型起到重要的支撑作用。

近年来，由于 IoMT 设备的激增，多类型、多型号的设备分布在多科室，且设备厂商的远程运维方式多样，导致风险暴露面积增加，原有安全防护手段难以应对，由此引发的医疗网络安全风险和挑战与日俱增。黑客越来越多地将目标对准我国的公共医疗机构，整体来看我国医疗机构的网络安全形势不容乐观。尤其在 2020 年新冠肺炎疫情期间，医疗机构的网络攻击和数据窃取事件激增，不仅造成了经济损失，也给患者的生命健康带来了威胁。

为促进医疗物联网及其生态系统的健康发展，厘清医疗物联网目前面临的安全风险，中国信通院安全研究所联合深信服科技股份有限公司共同研究编制了《医疗物联网安全研究报告（2021）》（以下简称：报告）。报告对后疫情时代 IoMT 设备可能面临的安全风险进行了分析，构建了医疗物联网安全防护策略框架，并提出了医疗物联网安全发展方向和建议，为医疗机构 IoMT 设备相关的安全规划提供参考。

目 录

图 目 录

表 目 录

一、医疗物联网概述

（一）医疗物联网的定义

物联网（IoT，Internet of Things）技术，是指通过感知设备，按照约定协议，连接物、人、系统和信息资源，实现对物理和虚拟世界的信息进行处理并作出反应的智能服务系统[1]。随着互联医疗设备数量的增加，支持医疗级别数据的采集和传输、互联技术、服务系统及软件的进步，医疗物联网（IoMT，Internet of Medical Things）由此诞生。

（二）医疗物联网的业务场景

医疗物联网综合了远程医疗、互联网、物联网、自动控制、人工智能等技术，是面向医疗机构全方位的运营和管理，致力于提高医疗品质，降低医疗差错，提升患者服务水平，提高整体运营效率的综合系统。典型的医疗物联网业务场景如下：

1.面向医务人员的智慧临床场景

智慧临床主要面向护士群体，移动智能终端结合无线通信技术的应用，让护士在病房服务中实现对患者入院信息、体征信息、手术资料、检查信息等数据实时准确的掌握，提高查房效率和质量。智能输液场景中每个患者输液位的状态通过无线传输实时传送到护士工作站的显示屏幕，护士在服务台就能实时监控患者输液进度。当液位较低临近更换输液瓶时，显示屏幕会语音提醒护士前去更换或终止输液，

[1] GB/T 33745-2017 物联网术语 2.1.1

同时提醒可以同步传输到移动 PDA[2]上，实现护理人员对病人输液状态及呼叫状态的实时掌控。智慧临床是医疗机构迈向智慧化转型的重要一步，也是医院等级评审复审的加分项目。

2.面向患者的智慧患者服务

智慧患者服务主要面向院内特殊或重症患者，服务包含院内导航、人员定位和报警求助等。通过智能穿戴手环、RFID[3]标签等手段，可以通过智能监控系统实时查看患者的行走路线和实时位置，一旦患者走出限定区域可产生告警，届时医护人员将及时协助患者返回安全区域，防止发生意外。此外，当患者发生身体不适急需求助时，可以通过智能穿戴设备实现一键报警，医护人员可以快速响应，保障患者的生命安全。

3.面向医疗机构管理的智慧管理

现代医院的院区规模呈现出快速扩张的趋势，而对应的医院所管理的资产数量和种类也呈现爆发式增长，传统的资产管理手段已远远不能满足医院管理需求。而基于物联网技术的智慧管理模式可以极大提高医院资产管理水平。利用 RFID 技术可以在购入设备资产时进行入账登记生成资产台账，由 WiFi 网络传递给资产综合管理平台，在资产分配使用、变更、回收、清点、报废等全生命周期中都可以实现跟踪管理，实现资产管理的精细化、规范化和专业化，满足医院业务快速增长的管理需要。

[2] PDA 是 Personal Digital Assistant 的缩写。
[3] 射频识别（RFID）是 Radio Frequency Identification 的缩写。

4.面向社区的远程健康管理

在公共卫生服务开展的过程中，由于医疗机构服务覆盖人群增多、地区医疗资源不平衡等因素，导致健康筛查无法及时覆盖到所有区域。利用 5G 技术传输的社区自助终端可以在家门口实现健康筛查，将身高体重、脂肪率、水份比、血氧、血压、心电等健康参数检测数据通过 5G 网络传输给医疗机构的后台分析系统，在中心端统一对检查的结果进行评估、分析和建议，可以让基层医疗人员工作更加轻松高效，让老百姓更加便捷的享受到我国公共卫生服务普惠政策。远程健康管理是“互联网医院”建设的重要环节，通过物联网和 5G 技术，把基层乡村医生和大三甲医院的门诊专家连接为一体，实现医疗资源全民共享，实现现代化技术造福于民。

由此可见，医疗物联网的应用遍布医疗行业的各个环节，国内大多数医院利用医院信息管理系统 HIS 具备了一定的信息化基础，但是也存在医疗信息无法及时同步录入，各科室之间信息交互相对独立的问题。而智慧医院的建设，让联网医疗设备、移动客户端设备、远程护理系统、互联临床信息系统、安防监控系统、医疗研究数据等海量数据融合交互，物联网技术可以打破各科室的信息孤岛，让医院能够进行综合数据采集，利用大数据分析提升整个医疗机构的效能和精细化运营管理，从而提高整体的信息化水平和诊疗服务能力。

（三）医疗物联网产业的发展态势和预测

1.医疗物联网产业发展态势

2019 年 3 月，《国家卫生健康委办公厅关于印发医院智慧服务分

级评估标准体系（试行）的通知》，提出建立 0 - 5 级医疗机构智慧服务分级评估体系，指导智慧医疗的落地和发展。我国医疗资源存在供需不平衡的突出问题，而智慧医疗的远程诊疗、简化沟通、自动化运营等优势对解决各地区医疗资源不平衡有重要作用。

2020 年物联网医疗市场的规模为 725 亿美元。预计到 2025 年，这一数字将增至 1882 亿美元。全球物联网医疗市场将迎来一个充满希望的激增，从 2020 年到 2025 年，复合年增长率（CAGR）接近 39%[4]。在我国物联网应用领域，**医疗物联网将成为仅次于工业物联网的第二大物联网市场应用领域。**

2.医疗物联网产业趋势预测

IoMT 设备厂商产品技术能力不断升级，医疗机构的业务智慧化转型加速。随着物联网通信技术和大数据技术在医疗行业应用愈发成熟，越来越多的信息和联网设备会在诊疗业务中为患者提供服务。如植入患者体内的单个智能设备，联网胰岛素泵和智能输液泵等，IoMT 设备在感知层的应用在医疗行业未来 5 年会保持高速增长。

医疗机构和 IoMT 设备厂商将深度协同。未来 IoMT 设备供应商将深入医疗机构的诊疗业务，双方不仅仅是强化固有的设备能力，还能够基于医疗机构已开展的各类智慧化诊疗数据和业务场景，共同开发形成新的医疗物联网产品。让医疗设备更加智能化，提升整个医疗系统的设备使用效率，为患者、护士、医生等相关群体提供更加深度且有价值的医疗物联网解决方案。

[4] ResearchAndMarkets. IoT in Healthcare Market by Component.2020.07

医疗数据隐私保护会成为 IoMT 设备厂商的首要考虑。由于 IoMT 设备智慧化业务能力的持续提升，覆盖的地点和范围更加广泛且呈现出无线化通信和维护的特点，导致感知层的设备数据会变得十分复杂，为此设备厂商需要一套完善的医疗数据隐私保护体系来保障医疗数据安全。相对应的，未来两年国内外会持续加强相关的法律法规体系建设，医疗卫生主管部门也会出台更多的监管要求来保障医疗物联网的数据安全和网络安全。

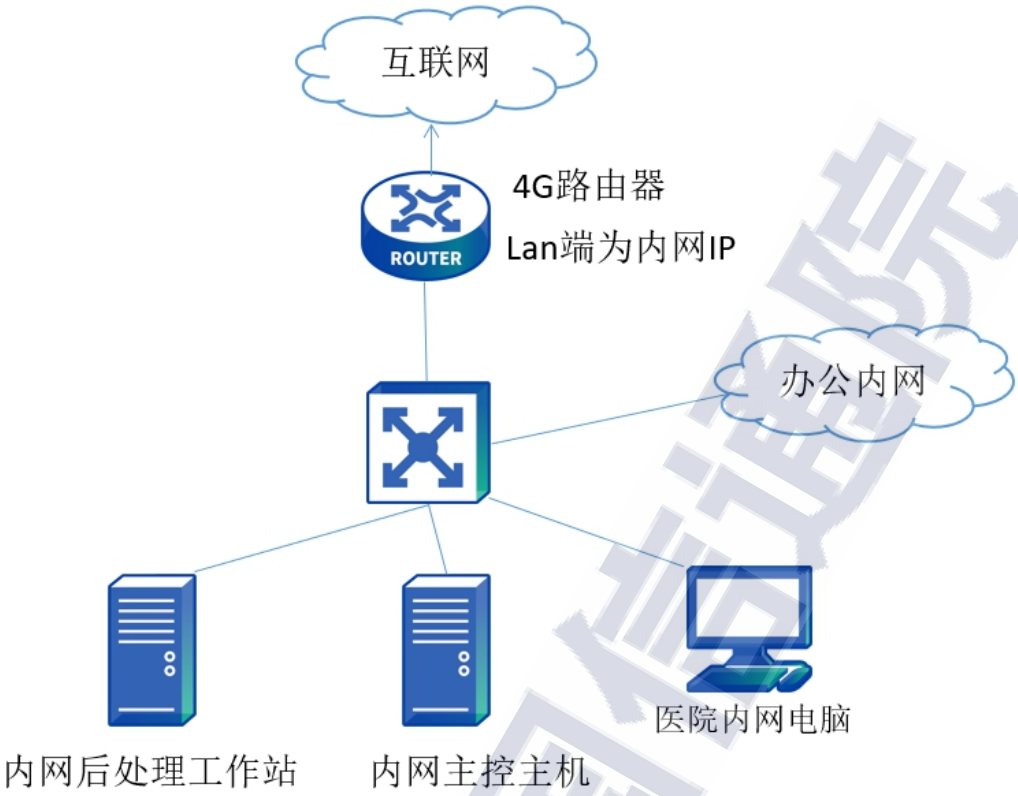
二、当前 IoMT 设备普遍存在的安全隐患

物联网技术的应用驱动万物互联时代到来。但同时物联网设备不同于传统的办公网络，其分布广、厂商杂、难管理的特性也带来了更多风险和新的潜在暴露点，物联网的设备、网络、应用将面临安全挑战。尤其在医疗物联网领域，网络安全更是需要重点考虑的头等大事。然而我国大多数医疗机构对新时代背景下物联网安全的复杂性认识仍有待提高。

医疗物联网感知层由医疗设备和 IoT 设备组成，医疗设备包含 X 线机、大型医疗器械等；IoT 设备包含传感器、摄像头、RFID 和网关等，主要功能是实现对信息的采集、识别和控制。无论是医疗设备还是 IoT 设备，由于投入使用周期较长，加上建设时坚持业务先行的原则，导致设备面临操作系统老旧、分布区域广泛、长期无人关注等安全问题，因此很容易受到恶意攻击进而导致医疗机构业务终端和数据泄露。医疗物联网感知层安全风险主要面临以下问题。

（一）远程运维带来数据泄漏和入侵的安全风险

IoMT 设备供应商主动提供全球运维服务，典型的有西门子、GE、飞利浦、迈瑞生物等。大型医疗设备配备外网通信组件通过远程连接到云端，通常情况下医院一般需要提供 3 个内网 IP 给到 IoMT 设备厂商，理论上通过外网可以和内网所有网络通信。如图 1 所示。境外运维厂商的运维云平台可能遭受外部攻击或内部泄密，或者由于运维厂商自身弱密码认证等原因，均有可能被入侵导致患者敏感数据泄露。



来源：中国信息通信研究院

图 1 医疗设备直连互联网

（二）IoMT 设备无安全防护能力被仿冒接入

感知层医疗设备操作系统版本多种多样，包括安卓、linux、嵌入式 Windows 等，由于设备供应商重功能、轻安全的商业理念导致医疗设备无法拥有完备的安全防护能力，使得医疗设备易遭到攻击，其次许多 IoMT 设备由于未进行更新补丁和漏洞修复，甚至为了便利的操作直接使用弱密码，导致被入侵和仿冒接入。如门诊楼的自助挂号机承载了挂号、缴费等核心业务，但是往往插拔网线就能实现患者个人信息和缴费信息窃取。真实攻击案例表明，攻击者在门诊楼内利用自助挂号机网线插入随身携带的笔记本电脑就可以在内网访问大量敏感数据，而目前医疗机构还未采取有效的管控手段。

（三）内网互联互通导致安全风险不可控

医疗机构的网络建设往往缺乏顶层设计，大量的办公终端、物联网终端、大型医疗设备混合在一张网络中。而大多数情况下，医疗机构虽然在边界部署了安全防护设备，但这些设备基于白名单的防护策略并未让安全风险降低。在医疗机构的网络中已经有大量的办公电脑和医疗设备，而 IoMT 设备大多使用 Wifi、蓝牙、ZigBee 等无线通信协议导致有线设备和无线设备混合在一张网络中，调研总结的医院各类 IoMT 设备联网方式如表 1 所示。由于无线设备可以私搭乱建违规接入网络，直接加大医疗机构网络的管理难度，而无线通信协议在使用过程中存在很大的安全风险，进而影响内网有线的办公终端和医疗设备，导致整体的网络安全风险增加。

表 1 医院联网设备连接方式

资产类型	联网方式	是否连接外网
中央监护系统	有线	否
血透机	串口转有线	否
监护仪	无线&有线	否
心电图机	无线	否
B 超机	有线	否
放射类设备	有线	部分远程运维
检验类设备	有线	部分远程运维

自助类设备	有线	否

来源：中国信息通信研究院

（四） 缺乏全面的资产台账导致安全风险黑盒化

全面的资产梳理是安全管理的第一步，但是不少医疗机构都存在资产管理不清晰的问题。尤其随着医疗物联网业务的发展，智能输液泵、医疗穿戴设备、移动查房终端、智能巡检机器人等医疗物联网设备爆发式增长，医疗机构的信息管理员更加难以建立清晰的资产台账，导致内网资产管理混乱，出现安全事件无法及时精准定位，极大降低了安全事件的处置效率。医疗机构资产管理普遍面临以下问题：**一是** IoMT 管理服务器向外网开放了高危端口，如 3306、1433 等数据库敏感端口；**二是** IoMT 设备只需开放移动端，却把管理后台一起开放到了外网；**三是**已下线系统或已完成测试的业务系统没有及时回收；**四是**服务器资源已回收，网络链路关系未清除，服务器 IP 重新分配给新的业务系统，导致新的业务系统被放到了外网。

（五）利用通信协议漏洞中断诊疗业务

在智慧病房建设中，每张床约有 10 个 IoMT 设备，包括智能输液泵、智能穿戴、传感器等。各类 IoMT 设备都部署在无人监控的场景下，直接暴露在物理环境中导致攻击者很容易接触并非法连接这些设备。国家信息安全漏洞共享平台（CNVD）披露的医疗数位影像传输协议 NEMA DICOM 存在编号为 CVE-2019-11687 的漏洞，利用该漏洞，攻击者可以移植可执行恶意软件，对诊疗数据非法篡改。由此

可见，攻击者可以通过 WiFi、蓝牙、DICOM 等协议漏洞造成通信中断，也可以利用信号传输过程中的漏洞篡改数据，上传被修改的血液数据和输液情况等数据，直接影响患者的生命健康。

（六）医疗机构工作人员自身安全意识薄弱

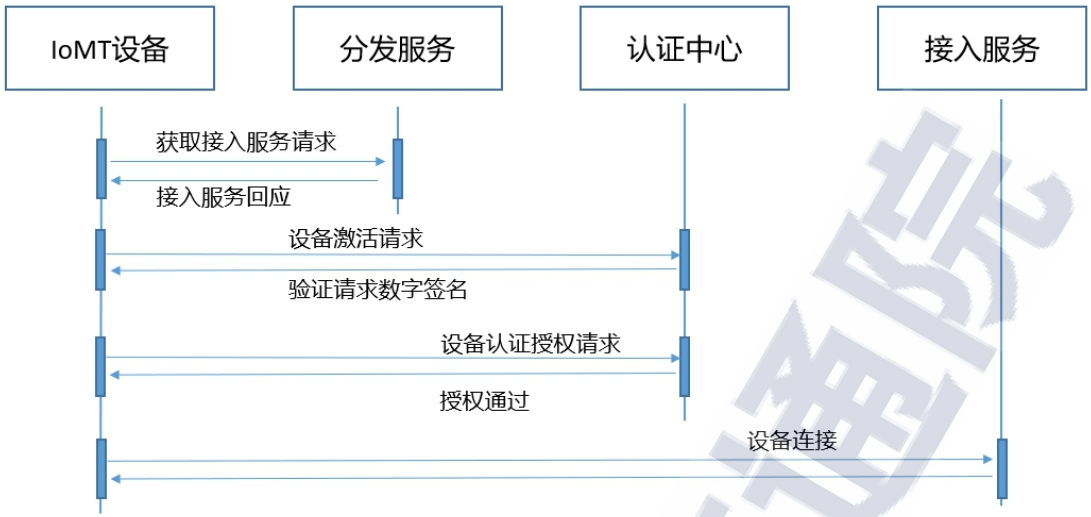
混合 IT 趋势下，人是信息安全管理过程中最脆弱的环节。随着医疗机构的联网设备的增加，工作人员的信息安全意识并没有随之增强。甚至部分医疗机构错误的认为，由于他们的医疗设备由医疗器械厂商提供运维，保护其应用的安全依靠医疗器械提供商就可以了。虽然医疗器械提供商在 IoMT 设备交付使用时提供通用性的安全防护措施，但是医疗设备厂商数据备份恢复以及业务自身安全性是医疗机构的主要责任而非医疗设备提供商的责任。

三、IoMT 设备安全防御有效方法

IoMT 安全不是单一维度可以解决的，需要从设备自身、软件开发设计、数据安全管控、安全运营等多维度综合考量。本章节从设备供应商、软件设计人员、医疗机构 IT 管理员、医疗机构 IT 运维人员的职责角度给出建议。

（一）IoMT 设备出厂前应具备安全基因

IoMT 设备供应商在设备生产时应结合较为成熟的网络安全体系构建终端级别的安全防护能力。在出厂前应探索内置安全芯片和身份标识，实现设备身份认证与鉴权防护，身份认证通过设备安全芯片为所有接入的设备分配唯一可信 ID 标识，设备 ID 具备不可复制、篡改与破解的强安全特性，合法设备通过 ID 实现入网的身份鉴别和授权，非法设备通过直接入网或伪造身份入网将会被快速准确识别，并阻断其入网传输，避免其对终端通信的安全造成危害。利用安全芯片实现身份认证、数据加密、安全存储，构建一个轻量级的安全体系，有效的防止设备伪造，与服务器、APP 间实现双向的安全认证，保障云端、终端、控制端的安全认证和通信。示例终端安全芯片认证接入流程如图 2 所示。在遭受物理攻击时，IoMT 设备厂商应确保设备在被突破后其身份认证以及账户信息相关的重要数据不会被攻击者利用。



来源：中国信息通信研究院

图 2 终端安全芯片认证接入流程

通过终端安全芯片实现对 IoMT 设备身份认证与鉴权及通信过程中会话、数据、攻击防御等多维度的安全防护。通过终端安全防护能力实现对设备的统一身份标识与安全可信认证，并在此基础上解决设备通信过程中安全会话、通信数据密钥管理与分发等安全防护需求与难点，保障医疗机构系统中各类设备运行期间通信安全。

（二）入网时确保具备可信认证校验和威胁防护机制

可信认证的校验机制是 IoMT 设备自身安全防护的第一道屏障。医疗机构应对大型医疗器械强制进行多重身份认证鉴权；确保只有经过授权的医疗设备才能连接医疗机构的内网；确保终端设备在接入时经过严格的标识和认证，接入系统中应具有可用于 IoMT 系统中通信识别的唯一标识，如序列号、设备 ID、MAC 地址等。

医疗机构信息化部门应建立精准可靠的 IoMT 设备台账，包含设备厂商、型号、类型、通信协议、开放端口、责任科室、责任人、责

任人联系方式等信息。利用安全接入设备实现对入网请求的 IoMT 设备的指纹特征进行校验，确保符合入网标准的设备才能联网。

设备威胁防护机制可以为 IoMT 设备建立一道安全的护城河。利用漏洞防御技术和权限收敛技术，通过深入分析网络及应用层协议对隐藏在流量中深层次攻击行为进行识别、控制、阻断，实现对 IoMT 设备的漏洞攻击实时检测和防护，达到在网络层降低威胁的目的。同时对 IoMT 设备日常访问的对象建立访问基线，利用基线在边界防护设备建立访问白名单策略避免设备过多访问后端主机对象造成风险暴露面的增加。

（三）对远程运维数据进行审计和外发管控

对存在远程运维大型医疗设备的厂商应建立运维数据审计机制。设备供应商应明确远程运维过程中使用的数据明细，确保只采集医疗设备的自身状态信息。医疗机构 IT 管理部门应对医疗设备上传的数据进行监测分析，对各类 IoMT 设备向外网发送的数据进行统一采集，利用大数据分析技术和 AI 技术进行建模分析，对 IoMT 设备的数据外发时间、目的地址、数据包、频率等建立行为基线，及时发现非常见用户访问、非常见地址外发、非常见时间段外发、非常见数据包外发等风险行为，对非法外发敏感数据及时发现和阻断，确保不包含患者诊疗数据和患者个人隐私数据。

医疗机构 IT 部门应针对第二章提出的远程运维带来的安全风险对供应商提出管理要求。如采用运营商或公网环境运维，对运维产生的数据流量应配合 IT 管理部门进行检测分析，避免供应商内部管理

和自身平台漏洞导致患者诊疗数据泄露。同时应配合 IT 部门采用基于风险闭环的管理方法保证其网络安全。

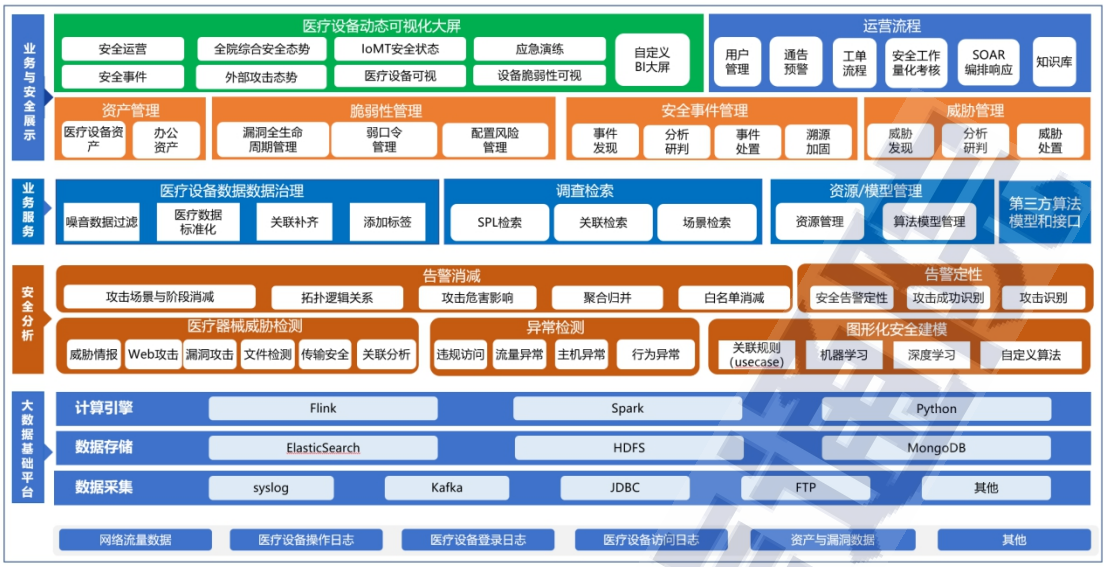
（四）IoMT 设备应重点强化开发安全

IoMT 设备供应商的开发人员应当从开发阶段充分考虑安全架构的设计。IoMT 设备开发人员会习惯性利用第三方组件提高开发效率，但三方组件会依赖其它更多组件，多层级依赖关系形成一个复杂的树状结构，这种结构对于研发人员和使用人员来说都是黑盒，导致 IoMT 设备供应商无法证明开发的医疗设备所部署的软件是安全的。比如证明从身份认证、授权、访问控制、可审计、设备保护等方面描述产品安全功能初始化过程中为何是安全的。

开发人员应提供产品设计文档描述产品的安全结构，安全测试方案和测试用例，提供相应的安全测试报告。开发人员应通过代码检查工具对编写完成的代码进行静态、动态的检查，尽早发现代码层面的缺陷、漏洞。医疗机构的信息化部门应当定期组织对 IoMT 设备进行安全漏洞检查，及时发现代码漏洞并制定处置闭环的流程。

（五）应建立针对 IoMT 设备安全运营体系

IoMT 设备作为医疗机构智慧化转型的核心，医疗机构的 IT 部门应建设立体化的 IoMT 设备的安全运营体系，包括对医疗设备网络安全威胁的识别、防护、探测、响应、恢复的能力。建立覆盖感知层、网络层、平台层和应用层的立体化安全运营体系，完整的 IoMT 安全运营体系如图 3 所示。



来源：中国信息通信研究院

图 3 医疗物联网安全运营框架

参考网络安全等级保护 2.0 的建设标准，通过大数据、机器学习、UEBA、SOAR、威胁情报等技术和工具，结合自动化流程和安全运营专家服务，打造“威胁感知、分析定位、智能决策、响应处置”的快速安全闭环能力，最终实“自动响应闭环、持续安全运营”的目标。对 IoMT 设备实行全面综合防护，保障智慧医疗业务的稳定运行。

四、对 IoMT 设备安全的发展建议与展望

（一）重视体系建设，完善 IoMT 安全防护体系

医疗机构智慧发展是必然趋势，我国 IoMT 业务正面临着严峻的安全挑战，完善 IoMT 安全体系的建设已经刻不容缓。同时，国内网络安全企业和医疗器械生产企业都缺乏针对 IoMT 设备的安全管控以及 IoMT 安全顶层设计与统筹管理。

医疗机构应提高对于医疗领域网络安全防护的重视程度。IoMT 设备安全应等同于麻醉安全、手术安全、药品安全。应为 IoMT 设备建立科学分类、风险分级、安全审查、责任管理规章制度，建立网络安全事件应急响应机制；第二，医疗机构网络安全管理部门应加强对 IoMT 安全产品质量及技能的测试评估机制，加大对 IoMT 安全企业产品及服务的监督管理；第三，网络安全企业应进一步完善 IoMT 安全体系架构，大力研发针对 IoMT 领域的网络安全产品，完善医疗 IoMT 运营平台的建设。从而以医疗机构、管理部门、安全厂商三者为重要抓手，持续完善 IoMT 安全体系的建设。

（二）产业深度协同，打造 IoMT 设备安全生态

首先，在政府鼓励其自主创新的前提下，国内 IoMT 设备供应商应继续加大对近距离无线通信、数据存储、数据挖掘、云计算等物联网关键技术的研究投入、增加大型医疗设备的研发投入。其次，应鼓励国内网络安全厂商将已有的网络安全技术与医疗领域相结合，用网络安全技术为 IoMT 赋能，让 IoMT 设备在产品开发中纳入安全性并进行测试，确保满足所有法律法规的安全性要求。最后，应鼓励从事

物联网技术研发的科研院所、高校与网络安全厂商、医疗机构三者间的深度合作及技术交流，在三方就防止医疗健康数据丢失及非法窃取等网络安全防护意识层面达到高度一致的基础上，制定有关于安全技术的统一验证及实施标准，培养具备网络安全意识的医疗机构信息化从业人员，从而确保安全技术产业化，最终满足医疗机构对于 IoMT 网络安全日益增长的需求。

（三）面向能力建设，助力 IoMT 安全自主可控

各种新兴技术发展促使医疗机构的业务快速变化，从宏观层面来看，IoMT 安全体系建设应由面向安全风险转变为面向安全能力。首先，在 IoMT 设备注册审批阶段要根据国内外的强制标准由政府公共安全管理部门进行评估，对物理安全、数据安全、通信安全、开发安全、软件安全等技术环节加强信息安全的把控，确保 IoMT 在感知层就建立安全能力。其次，政府应鼓励网络安全厂商开展 IoMT 设备安全评估服务，包含对大型医疗设备的漏洞检测、可信入网控制、违规外连审计、非法外发数据防护等，网络安全厂商要加强统筹和运营，要投入足够的人员、资金资源成立专业的安全评估团队，为 IoMT 设备供应商和医疗机构提供专业的信息安全服务，保障医疗设备的安全运行。最后，网络安全厂商和医疗机构应协同开发，通过内外部协同来培养安全人才，双方应主动拥抱技术创新，对检测能力、响应和处理能力、防御能力以及密码技术进行提升，培养一批具备实战能力的高水平人才梯队，应对不断变化的网络安全风险。最终推进 IoMT 安全体系在我国成功落地实施，实现 IoMT 安全自主可控。

（四）灯塔效应指引，消除 IoMT 安全落地障碍

医疗机构监管部门应大力支持市场需求旺盛的 IoMT 安全领域，医疗机构应在地方政府的政策及资金支持下，主动寻求与网络安全厂商联合创新成为 IoMT 安全应用先行示范点，让自身成为优秀示范工程，大力推动 IoMT 安全防御体系在自身智慧化业务中的落地。示范医疗机构在 IoMT 设备全面清查、精准防控、建立全网监测、快速应急处置等建设过程会累积大量成功经验，打造灯塔效应为同行业的 IoMT 安全体系建设提供指引。政府应鼓励结合优秀的示范工程形成大规模的推广复制，以最佳的工程实践消除在落地过程中的障碍。

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

邮编：100191

电话：010-62300264

传真：010-62300264

网址：www.caict.ac.cn