基于内生安全的智慧医院网络安全体系重构*

刘 阳

（中南大学湘雅医学院附属海口医院（海口市人民医院）信息管理处 海口 570208）

文 霞

（中南大学湘雅医学院附属海口医院（海口市人民医院）发热门诊 海口 570208）

〔摘要〕 介绍医院网络安全现状及内生安全概念、特点，阐述基于内生安全的智慧医院网络安全体系重构方法，分析存在的问题并提出建议，包括加强全员安全宣传教育、网络安全制度执行以及管理人员知识储备等。

〔关键词〕 网络安全；内生安全；外生安全；等保测评

〔中图分类号〕R-058 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673-6036.2023.03.014

Reconstruction of Intelligent Hospital Network Security System Based on Endogenous Security *LIU Yang*, *Department of Information Management*, *Affiliated Haikou Hospital of Xiangya Medical College*, *Central South University*, *Haikou 570208*, *China*; *WEN Xia*, *Fever Clinic*, *Affiliated Haikou Hospital of Xiangya Medical College*, *Central South University*, *Haikou 570208*, *China*

〔**Abstract**〕 The paper introduces the current situation of hospital network security and the concept and characteristics of endogenous security, expounds the reconstruction method of intelligent hospital network security system based on endogenous security, analyzes the existing problems and puts forward suggestions, including strengthening the safety publicity and education of the whole staff, the implementation of the network security system, and strengthening the knowledge reserve of management personnel, etc.

〔**Keywords**〕 network security, endogenous security, exogenous security, evaluation of network security level protection

1 引言

“互联网+”时代，随着各行业中业务应用逐渐智慧化，数据安全日益成为核心要务[1]。目前，5G、云计算、大数据等新兴技术应用范围不断扩大，在数据中心外以设备堆叠式建设围栅的传统防御手段已经无法应对当前的网络威胁。在实体医院基础上构建互联网医院的思路，使物理世界和虚拟空间的边界日益模糊，给智慧医院网络安全带来全新挑战。

2 医院网络安全现状分析

等保测评曾是评价医院网络安全状况的唯一手段，许多医院通过了等保测评后即停滞不前，缺乏规划、缺少经费、人员紧张、运管松懈情况普遍存在[2]。与此同时，随着“互联网+医疗健康”的迅速发展，医疗机构传统的网络安全体系面临新兴技

〔修回日期〕 2022-10-26

〔作者简介〕 刘阳，高级工程师，发表论文 17 篇；通信作者：文霞，副主任护师，发表论文 7 篇。

〔基金项目〕 国家自然科学基金“面向点数据集的超分辨数字病理图像拼接及可视化研究”（项目编号：82160345）。

术安全漏洞、个人隐私数据泄露、勒索病毒黑客攻击等更加严峻的挑战。缺乏科学、合理的安全体系是网络安全建设始终落后于业务应用建设的重要原因之一，而内生安全体系重塑正是破解这一发展困境的关键。

3 内生安全概念和特点

3.1 概念

内生安全就是在信息系统环境内部不断衍生出来的“规划先行、叠加演进、实战运行”的一种安全能力，即使网络边界防御失效或者被击穿，该系统仍能保持运行不影响业务应用，并且保证数据和业务安全[3]。

3.2 特点

3.2.1 自我免疫 内生安全能够从自我发现、自动预测和告警能力升级为具备应急响应能力。在面临灾难性网络安全事件时，可以保证关键业务自我免疫和自我修复。

3.2.2 拥有自主安全能力 网络安全体系仅靠外部安全大脑和外部力量无法解决内部安全问题，内生安全针对业务特性，立足于自身安全需求，与内部业务应用深度融合，拥有自主安全能力。

3.2.3 自我进化 网络安全能力需要伴随业务应用系统更新而不断升级和加强，网络安全体系只有在不断发现问题、解决问题的循环中才能持续改进和逐步提高。

3.3 原则

将这些内生安全的思想落地实现，除了需要使用“计划－执行－检查－处理”（plan－do－check－action，PDCA）循环不断改进，还需要遵循同步规划、同步建设、同步运营的“3 同步”原则，建立有效的保障机制[4]。

4 基于内生安全重构网络安全框架体系

4.1 重构思路

将内生安全体系建设定义为“安全运营＋安全过滤”。首先，实现“安全运营”需要建设安全运营中心，通过安全规划、安全能力、安全人才和安全生态建设，运用大数据分析、人工智能等技术，建立制度化、流程化、场景化、标准化、集约化多维安全运营中心，提高整体网络安全管理效益和治理水平。其次，“安全过滤”指所使用的网络安全、身份验证、数据保护、应用安全、行为验证等过滤手段。基于内生安全的网络安全体系，其指导思想就是将安全能力内置在业务应用系统中，通过人员、系统、数据的不断融合，“由系统内部生长出来”能够自我免疫、自我进化的安全能力。重构包括网络安全能力体系、网络安全规划方法论与工具体系、网络安全能力化组件模型、建设实施项目库、网络安全部署参考架构、网络安全运营参考架构共 6 个部分的网络安全框架体系，促进信息技术应用人才和安全人才的整合、业务应用系统和网络安全系统的聚合、业务数据和安全数据的融合，应对各类已知和未知网络安全威胁。

4.2 网络安全能力体系

网络安全能力体系是保障数字化业务所必需的安全能力集合，定义了整体内生安全框架的安全目标。网络安全能力体系细分为 5 类能力领域：基础结构安全能力领域、纵深防御能力领域、态势感知与积极防御能力领域、威胁情报收集分析能力领域、反制能力领域。除反制能力主要由国家级网络安全防御能力提供，其他 4 类能力领域是单位或组织网络空间安全防御体系的必备要素[5-6]。从智慧医院快速迭代更新的角度来看，5 类能力领域之间存在密切的联系，相互融合，共同促进。

4.3 网络安全规划方法论与工具体系

网络安全具有专业性强、复杂度高的特点，采用科学合理的规划方法论，在系统整个生命周期中合理规划系统安全，可以确保项目的科学性和经济性以及成果的实现[7]。利用网络安全规划工具，将软件工程、项目管理、运营管理等理论融入网络安全规划方法论中，可以确保目标达成[8]。网络安全

体系规划过程分为：相关依据确立、现状及差距不足、安全需求分析、安全目标规划、安全体系展望、路线图设计方案、科研与立项成果达成共 7 个步骤。

4.4 网络安全能力化组件模型

网络安全能力化组件模型的构建是在网络安全能力体系和规划方法论、工具体系理论基础上进行实践化的成果，得到可执行、可运作的实践能力化组件[9]。网络安全能力包括安全管理机制、安全技术手段、安全系统等内容。这些可执行的安全组件可以在信息化建设的不同层次和阶段呈现出相对应的控制方式，充分反映出与安全能力化组件深度融合的思想。网络安全能力化组件模型和网络安全规划方法论、工具体系，是面向网络安全规划整个生命周期的方法论和关键工具，基于访谈、调研、路线设计工作，可梳理出信息化现状与安全目标之间的差距，定义安全建设方向。

4.5 建设项目库

借鉴行业内网络安全最佳实践和网络安全架构研究成果，通过建立能力化组件模型，以重点项目为抓手，合理调配资源，通过制定有条不紊的项目建设计划完善管理机制，为网络安全体系建设工作提供充足保障和有力推动，从而实现网络安全能力演进提升，保障信息化业务平稳、可靠、有序和高效运营[10]。随着项目经验不断积累，形成有针对性的建设项目资源库，同时为未来项目规划建设提供有力的知识库支撑。建设项目库为安全类项目立项、建设提供依据，定义了安全目标与安全建设方向下的具体安全建设任务[11]。

4.6 网络安全部署参考架构

在建设项目库的同时积累不同类型网络安全部署参考架构模型，从网络安全、身份验证、数据保护、应用安全、行为验证等多个层面有效实现对网络安全体系的管理，用工程化、体系化的方式进行实施。与此同时，随着部署参考架构的不断修正和优化，反作用于网络安全组件模型、规划方法论与工具体系，推动内生安全框架体系不断完善。网络安全部署参考架构是以安全技术部署架构图的形式，全面表达智慧医院信息化和网络安全的融合全景，展示网络安全能力内生于信息化环境的目标部署状态，定义了安全建设方向下的技术演进路线。

4.7 网络安全运营参考架构

运营参考架构是信息系统必不可少的组成部分[12]。信息化项目的规划设计、部署实施、运行维护、升级迭代是一个持续优化的过程，网络安全贯穿其整个生命周期。网络安全运营推进各阶段工作同步开展，强化安全管理关口前移，实现网络安全与信息化建设齐头并进。网络安全运营参考架构描述各阶段工作所需的能力要求，明确网络安全、运维、开发等人员之间的协同工作机制，定义了安全建设方向下的安全管理范围。

4.8 框架体系结构

内生安全框架体系 6 部分之间是相互协作的关系，见图 1。以建设项目实施库和网络安全能力化组件模型为参考依据，在网络安全能力组件的指导下，基于网络安全规划方法论和工具的底座支撑，在信息系统建设和运维的全生命周期中，对智慧医院网络安全的规划设计、建设实施、系统运维等阶段进行网络安全部署参考架构和网络安全运营参考架构的同步构建，并不断优化。重构整个信息系统网络安全框架体系，使智慧医院具备由内而生的安全能力。各安全能力组件是网络安全框架体系不可或缺的组成部分，只有通过这些组件之间的有机整合、相互作用才能构成整体的内生安全框架体系，在智慧医院网络安全工作的不同阶段起到无法替代的重要作用，使网络安全工作有质的提升。

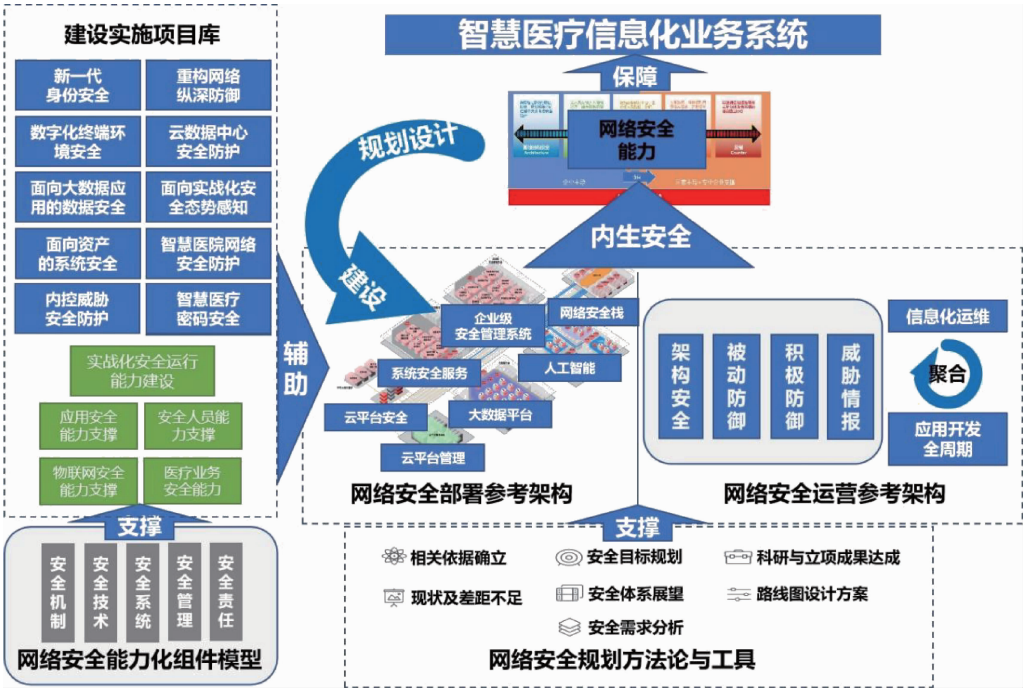

图 1 内生安全框架体系

5 分析与讨论

5.1 强化内生安全能力建设，促进网络安全体系重构

智慧医院的安全运行有赖于内生安全能力的提升与强化。首先，内生安全的特点是利用系统的架构、机制、场景和规律等内在因素获得安全功能或属性。其次，内生安全体系中各手段之间的衔接和相互协调是关键，要求对安全体系进行“整体规划，分步实施”，在医疗行业网络安全体系的基础上，实现安全框架组件化，使这些组件既能够融合到新体系中，又能够部署到旧业务系统中，从而适应信息系统生命周期的迭代进程，避免将已有旧业务系统推倒重建，确保复杂度高且不同时期建设的医疗业务系统都能够应对新时期的安全威胁，避免重复投资、减少资金浪费。最后，内生安全是以能力导向进行体系化的建设，针对医院网络安全防护能力薄弱的问题，强调“关口前移”的规划设计，基于“叠加演进”原则建设安全能力，重点是需要管理、技术与运行维护一体化，强调实战化运行。项目库和参考架构模型的及时修正和优化是内生安全体系的生命力，对重构网络安全体系起到动态指引作用。

5.2 存在问题及建议

首先，网络安全体系重构过程中各方共同参与、统一思想的积极性不高。实践中受到安全理念、专业队伍、工期压缩、资金投入等影响，安全体系建设困难重重。例如各级领导重视程度不足、安全意识淡薄、网络安全机制体制无法落地实施；信息管理人员“重视应用、忽略安全”，信息化项目设计阶段着重考虑业务需求，未能关注安全需求；网络安全预算落实不到位且与方案内容不匹配等问题[13]。针对这些问题需要从加强医院领导层的安全意识入手，开展全员安全宣传教育，提高安全意识以及重视程度。其次，由“齐抓共管”变成“无人管理”问题突出。针对此问题需明确网络安全责任、落实分工，树立正确的网络安全观，落实网络安全责任制[14]，强化网络安全制度执行。最后，在信息化实践中常存在将网络安全作为整体信息系统运维保障工作的一部分来实施的现象，不仅给业务系统运行带来安全风险，还导致后期整改难度加大和成本增高[15]。针对此问题，需要加强管理人员的知识储备，增强协调能力，以提高项目的设

计、实施、运维阶段对网络安全“3 同步”原则的落实。

6 结语

依托内生安全思路构建医院网络安全框架体系，进行网络安全顶层规划，引导网络安全建设从局部走向全面，为网络安全生态发展创造更大空间[16]。展望未来，需要业界同仁携手共进，协同网络安全建设单位、系统开发商等，共同重塑基于内生安全的智慧医院网络安全体系。

参考文献

1 颜浦钰. “互联网 +” 网络信息安全现状与防护研究 [J]. 长江信息通信，2021，34（9）：94 – 96.

2 刘阳，俞准. 网络安全等级保护 2.0 时代医院管理的方法与对策 [J]. 海南医学，2022，33（4）：535 – 537.

3 邬江兴. 网络空间内生安全发展范式 [J]. 中国科学：信息科学，2022，52（2）：189 – 204.

4 齐向东. 从两大“失效定律”和四个“假设”看网络安全防护体系构建 [J]. 保密科学技术，2017（9）：12 – 15.

5 齐向东. 面向新基建，用内生安全框架支撑网络安全体系建设 [J]. 中国科技产业，2020（8）：18 – 21.

6 徐语聪，吴云坤. “内生安全”时代把安全内置到业务系统中 [J]. 数据，2021（6）：35 – 37.

7 江伟玉，刘冰洋，王闯. 内生安全网络架构 [J]. 电信科学，2019，35（9）：20 – 28.

8 徐恪，付松涛，李琦，等. 互联网内生安全体系结构研究进展 [J]. 计算机学报，2021，44（11）：2149 – 2172.

9 张伟丽，贺磊. 关于新型内生安全信息基础设施的思考 [J]. 无线电通信技术，2020，46（4）：399 – 404.

10 郭星华，梁浩，王玲玲. 基于拟态安全的网络信息体系内生安全思考与实践 [J]. 指挥信息系统与技术，2021，12（6）：33 – 38.

11 张文建. 面向软件定义网络的内生安全关键技术研究 [D]. 郑州：中国人民解放军战略支援部队信息工程大学，2021.

12 罗论涵，李翔，余新胜. 数字化时代网络空间内生安全技术发展与应用 [J]. 电子技术与软件工程，2021（19）：255 – 257.

13 苏悦洪，申志航，邢洪伟，等. 医疗行业网络安全防护体系建设分析 [J]. 网络安全技术与应用，2022（4）：104 – 106.

14 郭峰. 做好数字化组织的“首席安全官”——构建有效落地的网络安全一体化防御体系 [J]. 中国信息安全，2021（11）：40 – 43.

15 张红彬. 医院网络安全体系构建与实现探析 [J]. 网络安全技术与应用，2018（8）：95，112.

16 吴云坤. 面向数字化保障的新一代安全体系建设 [J]. 软件和集成电路，2021（9）：43 – 44.

（上接第 73 页）

2 乔元芳. 运用机器人流程自动化技术进行审计正当时 [N]. 中国会计报，2020 – 02 – 28（9）.

3 VAN DER AALST W M P, BICHLER M, HEINZL A. Robotic process automation [J]. Business & information systems engineering, 2018, 60（4）: 269 – 272.

4 尹德静. 大数据时代医院统计工作的新策略分析 [J]. 中国卫生产业，2018，15（31）：158 – 159，162.

5 RATIA M, MYLLÄRNIEMI J, HELANDER N. Robotic process automation – creating value by digitalizing work in the private healthcare [C]. Tampere: ACM International Conference Proceeding Series, 22nd International Academic Mindtrek Conference, 2018.

6 赖伏虎，张铮，徐庆十，等. “统计机器人”在医院统计领域的应用 [J]. 中国医院统计，2020（5）：476 – 480.

7 龙思哲，吴震天，刘洋. RPA 机器人辅助医院数据统计工作的应用探讨 [J]. 当代医学，2021，27（27）：189 – 191.

8 郝伶俐. 医院财务管理信息化建设的现状及发展对策 [J]. 财会学习，2018（34）：74.

9 刘琪. 医院改革背景下医用耗材管理的困难与对策 [J]. 中国市场，2017（15）：201，203.

10 刘丹丹. 医院高危药物管理和风险防范分析 [J]. 饮食保健，2019，6（3）：274.

11 陈侠李，郑建中，王晶，等. 社会医疗保险背景下住院者过度索赔影响因素分析 [J]. 中国农村卫生事业管理，2016，36（6）：693 – 696.

12 黄伟亚，成建梅. 财务机器人的落地与挑战 [J]. 企业管理，2020（10）：103 – 105.