浅谈网络安全集中管控在医疗卫生信息系统安全管理中的重要性

章荣伟[1] 俞旭明[1] 曹 彦[*2]
（1. 杭州享量物联科技有限公司 浙江 杭州 310012）
（2. 浙江省疾病预防控制中心 浙江 杭州 310012）

【摘 要】本文提出了网络安全集中管控的模式，包括技术体系、运维体系和管理体系，并展示了其实施效果和影响，包括提高了医卫信息系统的运行安全、数据安全和网络安全，防范了漏洞利用、资产管理、数据泄露等风险，促进了医卫设备的智能化和数字化水平。本文对于提升医卫机构网络安全水平，促进医卫信息化发展，具有一定的价值和启示。

【关键词】网络安全；管理体系；医疗卫生信息化

Discussion on the importance of network security centralized control in the security management of medical health information system

Rongwei Zhang[1] Xuming Yu[1] Yan Cao[*2]
(1. Hangzhou Xiangliang iot Technology Co., LTD., Hangzhou,Zhejiang,310012)
(2. Zhejiang Center for Disease Control and Prevention, Hangzhou,Zhejiang,310012)

[Abstract]This article proposes the mode of medical health information security centralized management and control, including technical system, operation and maintenance system and management system, and shows its implementation effect and impact, including improving the operation security, data security and network security of medical health information system, preventing the risks of vulnerability exploitation, asset management, data leakage, etc., and promoting the intelligent and digital level of medical health equipment. This article has certain value and enlightenment for improving medical health institutions information security level and promoting medical health informatization development.

[Key words]Network security; Management system; Medical and health informatization

引言

网络安全是医疗卫生（以下简称医卫）信息系统的重要保障，但随着医卫信息化和互联网医疗的发展，医卫信息系统面临着更多的安全挑战。本文探讨了网络安全集中管控在提升医卫机构网络安全水平方面的作用和价值。网络安全集中管控是指对网络中的安全设备或安全组件进行统一管控的过程，可以提高网络安全管理的效率和效果，进行统一的管理，综合考虑安全性与业务连续性的要求。网络安全集中管控对于医卫信息系统的运行安全、数据安全和网络安全具有重要作用，也可以促进医卫信息系统与智能化医疗设备之间的协同与融合；网络安全集中管控在医卫信息系统网络安全管理中应该采用技术体系、运维体系和管理体系相结合的模式。

1 网络安全集中管控的发展

网络安全集中管控的目的是提高网络安全管理的效率和效果，实现对网络中的安全事件、安全策略、安全设备等的集中监测、分析、处理和管理，提高网络安全管理的效率和效果，实现对网络中的安全事件、安全策略、安全设备等的集中监测、分析、处理和管理。网络安全集中管控也是等保 2.0 在安全要求中明确提出的一个重要内容。

2 医卫网络安全集中管控的必要性与意义

医卫网络安全集中管控的必要性主要是为了保护医疗数据的安全，防止数据泄露、篡改、破坏等风险，维护医卫机构业务的正常运行和患者的隐私权益。

随着医疗信息化和互联网医疗的发展，医卫信息系统面临着更多的安全挑战，如网络攻击、程序漏洞、数据库脱库、科研数据流失、个人隐私泄漏等。医卫信息系统的安全性直接关系到医疗与卫生工作的正常运行，一旦网络瘫痪或数据丢失，将会给医卫机构带来巨大的灾难和难以弥补的损失，甚至危害国家安全。

为了构建完善的网络安全保障体系，需要从制度建设、技术措施、运维管理、风险评估、应急响应等方面进行规划和实施，遵循国家相关法律法规和标准要求，实现全生命周期的安全管理。医卫机构还需要加强网络安全意识培训，规范安全行为，完善各类人员安全责任制度，构筑全员安全堡垒，防范网络钓鱼、近源攻击等事件发生。

医卫网络安全集中管控的意义在于，对信息系统内的数据资源和用户权限进行统一管控，针对不同访问需

求，规范划分医护人员、行政人员、IT 信息人员、第三方运维人员等角色的权限，实现对医卫信息系统的全面监管和管理。同时，完善网络安全管理制度和提高职工网络安全意识的重要性也得到了明确。通过对安全防范技术、管理制度及措施、人员培训等方面的探索，实现医卫信息系统长期、有效的网络安全。集中管控可以有效地保障网络安全，防止数据泄露、篡改、丢失等情况的发生。同时，集中管控还可以提高医卫信息系统的运行效率，降低运维成本，为医卫信息化建设保驾护航。

3 医卫网络安全集中管控的原则与模式

在医卫信息化建设中，如何加强数据安全保护，有效实施数据全生命周期安全管理，夯实信息化发展的安全底线，是值得医卫机构管理者们思考的问题。医卫网络已经发展到智慧化的环境下，平台安全和数据安全成为关注重点。在信息化建设中必须加强网络安全防护工作，以完善的策略保护医卫网络的安全稳定运行。对医疗信息系统内的数据资源和用户权限进行统一管控，针对不同访问需求，规范划分医护人员、行政人员、IT 信息人员、第三方运维人员、医学科研人员等的访问权限；同时，对人员的数据访问行为进行全面审计，并对审计日志进行详细分析，生成审计报告。医卫网络安全集中管控的原则一般有：

统一性原则：安全集中管控应基于整体的网络安全策略，统一规划、设计和实施，确保各个安全要素的协调和一致性。

分层次原则：安全集中管控应根据安全等级和敏感程度将信息进行分层次管理和控制，以适应不同数据和系统的安全需求。

风险管理原则：安全集中管控应基于风险评估和威胁情报，采取针对性的安全措施，优先解决高风险和高威胁的安全问题。

合规性原则：安全集中管控应符合相关法律法规和标准要求，包括医卫网络安全相关的法规、上级部门和行业的标准、以及国家等保、关键基础设施和密评等要求。

审计与监控原则：安全集中管控应建立完善的审计机制和监控系统，对医卫信息系统的安全事件、访问行为和异常情况进行实时监测和记录。

医卫网络安全集中管控的模式包括：

技术体系模式：安全集中管控可以通过采用安全设备、防火墙、入侵检测系统、安全审计系统等技术手段，实现对医卫信息系统的统一管理和保护。

运维体系模式：安全集中管控应建立健全的运维流程和规范，包括日常维护、安全巡检、安全漏洞修复、事件响应等，确保信息系统的安全和稳定运行。

管理体系模式：安全集中管控应建立完善的组织机构和安全管理制度，包括人员安全责任制度、安全培训与考核机制、数据访问控制机制等，形成全员参与、全员负责的网络安全文化。

数据保护体系模式：安全集中管控应采用数据加密、备份与恢复、访问控制等措施，保护医卫的核心数据和敏感信息免受泄露和篡改。

4 医卫网络安全集中管控的效果与影响

医卫网络安全集中管控通过建立网络安全管理体系，对医卫机构内部的信息资产、数据流动、系统运行、网络访问等进行统一的规划、监控和保护，以防止信息泄露、篡改、破坏等安全风险的发生。

医卫网络安全集中管控的模式主要包括以下几个方面：

技术体系，涉及访问控制、完整性保护、系统和通信保护、物理与环境保护、检测与响应、备份与恢复等一系列技术方案；运维体系，包含流程和规范、日常维护、风险评估、行为管理、应急处置等；管理体系，包括组织机构、规章制度、人员安全、安全培训等。

医卫网络安全集中管控的模式要求医卫根据自身的业务需求、合规需求、威胁识别和风险评估，制定合理的安全规划和策略，建立数据管理委员会，加强监管和审计，实现网络安全的全生命周期管理。展示网络安全集中管控的实施效果和影响，包括提高医卫信息系统的运行安全、数据安全和网络安全，防范漏洞利用、资产管理、数据泄露等风险，促进医疗设备的智能化和数字化水平。

医卫网络安全集中管控的效果主要取决于以下几个方面：

医卫信息化建设的水平和规范，包括业务系统、质量管理体系、标准体系、人才梯队等；医卫网络安全设备的配置和使用，包括防火墙、VPN 设备、物理隔离设备、网闸设备、入侵检测设备和防毒墙；医卫网络安全管理的机制和措施，包括组织架构、制度落实、安全防范、管控意识和能力等；医卫网络安全素养的培养和提升，包括宣传教育、培训考核、数据保护和隐私保障等。

综合来看，医卫网络安全集中管控的效果需要各级各类医卫机构根据自身情况和国家标准，制定整体策略，完备系统，补足短板，创新模式，强化管理，提升能力，保障数据安全和患者利益。

5 医卫网络安全集中管控的价值与启示

医卫网络安全集中管控具有以下几个方面的价值：

统一管理与保护：通过网络安全集中管控，医卫机构可以实现对整个网络环境的统一管理和保护。这包括对网络设备、服务器、终端设备和应用系统的安

全配置、漏洞管理、访问控制等方面的统一管理，确保网络的整体安全性和稳定性。

提升安全防护能力：通过集中管控，医卫机构可以建立完善的网络安全防护体系，包括入侵检测与防御、威胁情报监测与应对、恶意代码检测与防范等。这可以大大提升医卫网络的安全防护能力，有效预防和抵御各类网络攻击和威胁。

敏感信息保护：医卫信息系统处理的数据中包含大量的敏感信息，如公民的个人身份信息、病历资料、医疗研究数据等。通过网络安全集中管控，可以采取有效的加密、访问控制、数据备份与恢复等措施，保护这些敏感信息的安全，防止泄露和滥用。

快速响应与事件管理：医卫网络安全集中管控可以建立实时监测和事件响应机制，及时发现和应对网络安全事件和威胁。通过集中收集和分析安全事件的日志和信息，可以快速定位问题、采取相应措施，并进行安全事件的溯源和调查，提高应对网络安全事件的效率和准确性。

合规与法规要求：随着医疗行业对信息安全的要求越来越高，网络安全集中管控可以帮助医卫信息系统满足相关的合规与法规要求。通过统一的安全策略和控制措施，确保医卫信息系统的合规性，遵循医卫信息安全相关的法律法规和行业标准，保护医卫机构和病人的权益。

医卫网络安全集中管控的价值在于提供统一管理和保护、提升安全防护能力、敏感信息保护、快速响应与事件管理以及满足合规与法规要求，从而确保医卫信息系统的安全性、可靠性和可持续发展。

医卫网络安全集中管控给我们带来以下一些启示：

重视网络安全：医卫网络安全集中管控的实施表明，各级医卫机构对网络安全问题的重视程度正在提高。医卫机构应意识到网络安全对于保护敏感数据、维护公民与病人权益和确保医卫服务的连续性至关重要。

统一规划和管理：通过集中管控，医卫机构能够统一规划和管理网络安全措施，包括安全策略、安全配置、漏洞管理等。这提醒我们，在建设和管理医卫信息系统时，需要采取整体、统一的方法来确保网络安全的一致性和有效性。

多层次的安全防护：医卫网络安全集中管控的实施需要考虑多个层面的安全防护，如网络设备、服务器、终端设备和应用系统等。这提示我们，仅仅依靠单一的安全防护措施是不够的，需要在多个层次上采取综合的安全措施来提高网络安全性。

实时监测和响应：医卫网络安全集中管控强调实时监测和事件响应的重要性。这提醒我们，在网络安全管理中，应建立及时的安全监测和事件响应机制，能够快速发现和应对安全事件，降低潜在风险和损失。

持续改进和合规：医卫网络安全集中管控的实施需要不断改进和满足合规要求。这告诉我们，网络安全工作是一个持续的过程，需要跟随技术的发展和法规的更新，不断改进安全措施和适应新的威胁。

总的来说，医卫网络安全集中管控是重视网络安全、统一规划和管理、多层次的安全防护、实时监测和响应以及持续改进和合规。这些启示对于其他行业和组织来说也具有普适的价值，有助于提高网络安全的水平和保护敏感信息的安全。

结束语

医卫网络安全是保障医卫工作正常运行和患者隐私权益的重要保障。随着医卫信息化和互联网医疗的发展，医卫信息系统面临更多的安全挑战。网络安全集中管控作为一种统一管理网络安全设备和安全组件的方法，对提升医卫网络安全水平具有重要作用和价值。

针对网络安全集中管控的模式和方法，本文提出了技术体系、运维体系和管理体系相结合的模式。技术体系包括访问控制、完整性保护、系统和通信保护等技术方案；运维体系包括流程和规范、日常维护、风险评估、应急处置等；管理体系包括组织机构、规章制度、人员安全和安全培训等。这些模式和方法可以帮助医卫机构实现对信息系统的全面监管和管理，确保医卫网络安全的全生命周期管理。

然而，医卫网络安全集中管控的效果需要加强信息化建设的水平和规范，合理配置和使用安全设备，建立完善的安全管理机制和措施，培养和提升人员的网络安全素养。只有综合考虑技术、运维和管理等方面的因素，全面推进医卫网络安全集中管控，才能有效保障医卫网络安全，防范安全风险的发生。

综上所述，网络安全集中管控在医卫网络安全管理中具有重要作用和价值。通过采取适当的模式和方法，医卫机构可以提升自身的网络安全水平，保障医卫工作的正常运行和公民、患者的隐私权益。

参考文献：

[1] 王非，谷敏，高晓娟．医院信息网络系统安全策略与维护 [J]《江苏科技信息》2011,03(28-29)

[2] 王政理，衢州医保“云”信息系统赋能医保治理体系 [J].《中国医疗保险》2021,07（39-42）

作者简介：

章荣伟（1983.4- ）男，汉族，浙江杭州人，大学本科，技术总监，一直从事网络空间安全运营及管理。

通讯作者：曹彦（1977.8- ）男，汉族，大学本科，高级工程师，一直从事研究信息化应用。