智慧校园背景下网络安全综合治理实践

李义
东北财经大学，辽宁 大连 116025

摘要：随着信息技术的迅猛进步，智慧校园作为教育领域的创新实践，正深刻改变着传统教育模式和管理范式。然而，伴随其带来的高效便捷，网络安全问题也愈发凸显。本文从智慧校园的定义和特点切入，深入探讨了网络安全在其中的重要性和作用，尤其是其在信息化进程中的基石地位。通过审视智慧校园网络安全治理的现存问题，揭露了管理、技术及数据安全层面的不足，并结合网络安全的前沿趋势，提出了一系列切实可行的治理策略和建议。接着，强调了构建健全网络安全体系与保障机制在智慧校园建设中的核心意义，这是确保教育信息化持续健康发展的关键。

关键词：智慧校园；网络安全；治理策略

Practice of Comprehensive Management of Network Security under the Background of Smart Campus

Li,Yi

Dongbei University of Finance and Economics, Dalian, Liaoning, 116025, China

Abstract: With the rapid progress of information technology, smart campus, as an innovative practice in the field of education, is profoundly changing the traditional education model and management paradigm. However, with its high efficiency and convenience, network security issues have become increasingly prominent. Starting from the definition and characteristics of smart campus, this paper discusses the importance and role of network security in it, especially its cornerstone position in the information process. By examining the existing problems of network security governance in smart campus, this paper exposes the deficiencies in management, technology and data security, and puts forward a series of feasible governance strategies and suggestions in combination with the frontier trend of network security. Then, it emphasizes the core significance of constructing and perfecting the network security system and guarantee mechanism in the construction of smart campus, which is the key to ensure the sustainable and healthy development of educational informatization.

Keywords: Smart campus; Network security; Governance strategy

DOI: 10.62639/sspfed04.20250101

引言

信息化浪潮的推动下，智慧校园以其独特的融合性，将现代信息技术与教育管理紧密结合，引领着全球教育发展的新方向。通过运用物联网、大数据、人工智能等尖端技术，智慧校园优化了教学与管理流程，更实现了教育资源的高效利用。但与此同时，其复杂的系统架构也带来了前所未有的网络安全挑战。在这样一个高度互联的环境中，确保师生信息的安全、保障教学数据的完整，已成为智慧校园发展中亟待解决的问题。

一、智慧校园的定义与特点

智慧校园是依托于信息化和数字化技术构建的现代教育环境，其通过互联网、大数据、物联网、人工智能等技术的深度融合，打破了传统校园的界限，实现了教学、管理、服务等各个环节的智能化。其核心特点在于数据的智能分析与应用、信息的共享与协同，以及基础设施的高效整合。这种环境为师生提供了更为便捷的学习和生活体验，也为学校管理者提供了强有力的决策支持，推动了教育模式的深刻变革。

二、智慧校园背景下网络安全综合治理存在的问题

（一）管理机制与责任体系的不足

在智慧校园的建设与运营中，网络安全管理机制常显不足。许多学校缺乏系统化、长远性的网络安全管理规划，导致管理层次松散、职责分工模糊。智慧校园的复杂性要求各部门间紧密协作，然而实际情况却是各部门各自为政，缺乏有效的跨部门沟通机制。这种分散管理模式在应对复杂网络攻击时显得尤为捉襟见肘，难以快速响应和协同解决问题。同时，责任体系的不明确也是一大治理难题。尽管部分高校已设立网络安全领导小组，但实际操作中责任界定模糊，无法形成有效的制度约束。特别是在应对突发事件时，由于缺乏明确的责任追究机制，事后问责与整改往往流于形式。这种管理体系的缺陷严重削弱了网络安全工作的执行力度和实效性，使得全校范

（稿件编号：FED-25-1-17001）

作者简介：李义（1978-），女，汉族，辽宁大连人，东北财经大学，副教授，院党委副书记，本科学历，硕士学位，研究方向：主要从事党建、思政研究。

围内的统一协调与资源整合成为空谈，网络安全管理效果因此大打折扣。

（二）联动防御薄弱，安全产品整合欠缺

智慧校园作为信息技术的高度集成体，其安全防护的复杂性与多样性要求各类安全产品必须实现有效联动。但当前，众多智慧校园在网络安全方面存在显著问题：安全产品整合不足，联动防御能力薄弱。智慧校园通常涵盖防火墙、入侵检测系统、数据加密系统等多类安全产品，然而这些产品在设计和部署时往往未充分考虑整体协同作用，导致各自为战，缺乏联动。这种孤立性严重削弱了网络安全的整体防御力。例如，在应对复杂网络攻击时，单一防护措施难以识别和抵御多层次、跨系统的攻击，甚至可能引发不同安全系统间的冲突，影响整个校园网络的稳定。此外，许多智慧校园的网络安全体系仍处于“拼凑”状态，缺乏对安全产品的全面规划与深度整合，导致整体防御能力不足。同时，各部门根据自身需求采购的安全产品往往无法实现互联互通，存在兼容性问题，加剧了安全防护的难度。

（三）“数据孤岛”问题加剧，数据安全面临严峻挑战

随着智慧校园的全面数字化推进，数据在校园管理、教学和服务中的重要性日益凸显。然而，不同系统和部门在数据存储与使用上的割裂导致了“数据孤岛”现象的频发。这种现象阻碍了学校资源的共享与协同工作，更对数据安全构成了严重威胁。在智慧校园建设中，各类信息系统和应用程序由不同部门或单位分别负责，导致数据管理权限划分不清晰，系统间对接与信息共享困难重重。数据的孤立状态限制了智慧校园的整体效能发挥，还为网络攻击者提供了可乘之机。一旦系统被攻破，攻击者便可轻易获取大量敏感数据，造成严重后果。此外，“数据孤岛”还增加了数据安全防护的复杂性。各部门在数据安全防护标准、策略和技术手段上的不一致性导致在发生数据泄露、丢失或被篡改时难以追溯责任并采取有效修复措施。数据的分散存储与管理也加大了数据保护的难度和潜在风险。

（四）用户安全素养不均，防护意识亟待加强

网络安全是技术层面的对决，更是全校师生共同的责任。在智慧校园环境下，网络安全的保障深深依赖于每位师生的安全意识和行动。但遗憾的是，目前许多师生的网络安全素养仍有待提升，师生的防护意识相对薄弱。特别是学生群体，由于对网络潜在风险的认识不足，常在使用网络资源时暴露于安全隐患之中，如轻信不明链接、使用简单密码、随意分享个人信息等，这些行为无疑为网络攻击者提供了入侵的机会。同时，作为教师，其在智慧校园中的角色举足轻重，其网络安全意识和行为对整体校园网络安全具有直接影响。然而，不少教师在网络安全方面的知识储备有限，且未能充分意识到网络安全与教学工作间的紧密联系。由于缺乏必要的安全培训和知识普及，教师在日常工作中可能会忽略数据保护和隐私安全等关键环节，从而给学校的网络安全埋下隐患。

（五）安全保障投入不足，人才与资金双双匮乏

智慧校园的网络安全建设离不开充足的人力、物力和财力支持。但当前，许多学校在网络安全保障层面的投入显然不够，导致其网络安全防线相对脆弱。其中，网络安全人才的缺失尤为突出。智慧校园的建设和运维需要专业技能过硬的网络安全人才来保驾护航，但许多学校在这方面的人才储备明显不足。现有的网络安全团队往往以兼职人员为主，难以有效应对日益复杂多变的网络安全威胁。同时，资金短缺也是制约网络安全治理的重要因素之一。在智慧校园的建设过程中，学校往往更倾向于将资金投向硬件设备、教学资源和基础设施等方面，而忽视了网络安全这一基石。然而，网络安全的持续防护需要稳定的资金投入，特别是在技术迭代和安全设备更新方面。由于预算限制，许多学校无法及时跟进最新的安全技术和设备，导致其整体防护能力难以与时俱进，无法有效应对不断演变的安全威胁。

三、智慧校园背景下网络安全综合治理实践策略

（一）强化领导与制度构建，夯实网络安全基础

智慧校园网络安全治理体系中，加强领导和制度建设是基石。首要任务是构建健全的网络安全领导组织架构。学校应成立由校级领导主导的网络安全领导小组或委员会，汇聚信息技术、教学、后勤等相关部门力量，形成高效协同的工作机制。该领导小组需承担制定并实施网络安全策略的重任，明确各部门职责与人员分工，确保网络安全工作全面覆盖、全员参与。如此，网络安全便能从战略高度得到有力保障，有效防范管理断层和职责模糊的风险。与此同时，制度建设亦不可忽视。学校需结合自身实际，制定贴合需求的网络安全管理制度，涵盖信息安全管理、数据保护、访问控制及应急响应等关键环节。这些制度要满足日常安全管理需求，更要具备应对突发事件的能力，确保在安全事件发生时能够迅速、有序地做出响应。此外，网络安全制度还需与国家及行业法规保持衔接，确保合规性和时效性。学校应定期评估并修订相关制度，以适应不断变化的网络安全环境，保持制度的生命力和适应性。通过加强领导力量和完善制度建设，能够明确各方责任，提升网络安全工作的执行效率，更能在全校范围内营造共同参与、共同维护网络安全的良好氛围，为智慧校园的网络安全治理提供坚实保障。

（二）统一规划管理基础设施，夯实智慧校园网络安全基石

智慧校园网络安全的综合治理，离不开基础设施的统一建设与管理。面对多样化应用和复杂信息系统，校园网络必须具备高度协调性与统一

性。为此，学校应全局规划、统筹建设，以消除系统孤立、资源浪费及安全隐患。在建设初期，学校就需进行统筹规划，确保设备、终端和应用协同运行。实现校园网络集中管控，构建统一网络架构和数据平台，保障数据顺畅流通。这能减少因软硬件不兼容导致的安全漏洞，降低网络攻击传播风险，还能简化运维、提高资源利用率、节约成本，并增强网络服务可靠性。同时，统一管理有助于提升安全防护的全面性和针对性。学校可实时监控网络状态，及时发现潜在威胁。定期的安全审计和漏洞扫描则确保基础设施满足最新安全需求。此外，将智能设备、终端设备纳入统一管理体系，可避免设备安全问题成为网络攻击突破口。前瞻性考虑基础设施可扩展性和灵活性也至关重要，以应对新技术、新需求挑战。只有统一建设、高效管理，才能为智慧校园长期发展奠定坚实安全基础。

（三）全面加强安全防护举措

随着信息技术的不断进步，必须持续提升和创新网络安全防护措施。对于智慧校园而言，构建一个多层次、多维度的防御体系至关重要，其需要覆盖从物理层到应用层的所有方面。首先，物理安全是基石，学校必须严格确保网络设备、数据中心和服务器等设施的安全，防止未经许可的人员进入关键区域，从而避免硬件遭到损坏或被盗。同时，边界防护也至关重要，建立完善的防火墙和入侵检测与防御系统是必不可少的，这样可以实时监控网络流量，并迅速识别和防御网络攻击。在此基础之上，需要进一步加大数据中心的安全防护投入，实施严格的访问控制机制，以确保数据的安全存储与传输。重要数据必须进行加密处理，以防范数据泄露或篡改可能带来的严重后果。此外，学校还需构建完备的身份认证与访问权限管理体系，确保仅有授权人员能够访问敏感数据和系统，从而降低内外部威胁的风险。除了物理和边界防护，加强 IT 资产管理也是关键一环，必须确保所有设备和系统在其全生命周期内得到妥善管理。这包括详细记录设备的采购、配置、使用、维护及淘汰等信息，以保障设备的安全性和可靠性。同时，定期进行安全漏洞扫描，并及时修复已知漏洞，是防止黑客利用漏洞发动攻击的重要措施。

（四）大力提升用户安全素养

网络安全取决于技术手段，更在于广大师生的安全素养。在智慧校园环境下，用户的网络安全认知与行为对整体网络环境的安全至关重要。因此，学校必须多渠道提升师生的网络安全意识，引导师生树立正确的安全防护理念，并养成良好的网络安全习惯。为实现这一目标，学校应定期举办网络安全教育培训，全面讲解网络安全基础知识、常见网络威胁及有效的密码管理方法等。此类培训应覆盖全体师生，通过课堂讲授、线上课程、专题讲座等多种形式进行，以全面提升大家的安全防范意识。同时，建立完善的安全报告与反馈系统也势在必行，以鼓励师生积极参与网络安全管理。通过设立便捷的举报途径，确保师生能及时上报网络安全问题或隐患。学校需对所有报告进行审慎处理，并根据情况采取相应措施，从而营造全员参与的网络安全治理环境。此外，与外部安全专家的紧密合作亦不可或缺。定期邀请专家对校园网络安全状况进行评估指导，有助于学校及时发现并解决潜在安全问题，从而持续增强自身的网络安全防护能力，有效应对新型网络威胁。

（五）全面加强技术防御与应急响应

技术防御与应急响应是确保智慧校园网络安全的关键环节。面对不断变化的网络攻击手段，学校必须持续提升技术防御能力，以及时识别和抵御新兴威胁。为此，学校应加大对前沿网络安全技术的投入，部署先进的防火墙、入侵检测系统、入侵防御系统及网络行为分析等技术，构筑起多层次的防御体系。同时，建立完善的应急响应机制也至关重要。这意味着在网络安全事件发生时，学校能迅速反应，采取有效措施以降低事件影响并恢复系统正常运行。学校需制定周密的应急预案，明确各部门及岗位的应急职责，并定期进行演练以确保机制的有效性。预案应涵盖事件检测、初步分析、紧急处理及系统恢复等全流程，从而快速定位并解决问题，防止事态扩大。此外，提升应急处理能力还需加强跨部门协作与信息共享。通过建立跨部门的应急响应团队，整合技术、管理及安全等多方资源，形成强大的协同作战能力。这种多部门联动的模式能够确保学校在网络安全事件发生时迅速调动资源，高效应对。

四、结语

智慧校园建设是教育信息化发展的必然趋势，但随之而来的网络安全挑战亦不容忽视。随着技术的持续进步与应用场景的不断拓展，智慧校园的网络安全防护日益复杂，迫切需要在技术、管理及人员素养等方面进行全面提升。这些举措将增强校园网络的防御能力，也为教育行业的信息化安全管理提供了有益借鉴。展望未来，随着网络安全技术与管理模式的持续创新，智慧校园的网络安全防护体系将日臻完善，更好地满足数字化教育快速发展的需求。

参考文献：

[1] 张小雷 . 基于态势感知的高校网络安全实践探索 [J]. 网络安全技术与应用 , 2024, (11) :64-66.
[2] 王艳 . 数字校园网络安全防范体系构建思考 [J]. 网络安全技术与应用 , 2024, (11) :66-68.
[3] 杨芸 . 校园网安全漏洞全生命周期管理探讨 [J]. 网络安全技术与应用 , 2024, (11) :74-75.
[4] 陆富业 , 梁桂才 , 李玉荣 . 网络攻防演练中校园网络敏感信息的保护与应对 [J]. 网络安全技术与应用 , 2024, (11) :69-73.
[5] 许涛 . 校园网络安全与信息化建设的协同发展研究 [J]. 中国宽带 , 2024, 20(10) :103-105.