# 基于智慧校园建设的高校网络安全实践和管理探索

李 翔
无锡科技职业学院，江苏 无锡 214000

**摘　要：**随着高校信息化的高速发展，校园建设智慧化是高校信息化发展的必然趋势，智慧校园建设对高校来说强化了网络、业务以及资源等共享整合，提高了教育信息化管理水平，但网络安全方面暴露出的问题也成为了智慧校园建设发展的重要挑战。本文就智慧校园建设中网络安全相关情况展开研究，调查了高校网络安全现状，介绍了网络安全相关防护技术，提出目前高校网络安全存在的问题和不足，并给出了相应的网络安全技术和管理对策，确保智慧校园建设中高校网络的可控、可信和安全。

**关键词：**网络安全；智慧校园；校园网；安全管理

## 引言

高校网络安全稳定是高校信息化工作开展的前提和基础，也是高校开展智慧校园建设基本条件。随着信息网络的快速发展，各高校也在努力创建数字化标杆学校，一些新技术、新概念、新设备相互融合，尤其是云计算、人工智能、虚拟现实、大数据以及 5G 专网等技术在智慧校园建设中大量应用，给高校师生的教育和生活带来很大便利，但由于复杂的校园网络环境、庞大的设备存量以及错综的部门关系等因素，高校网络安全也存在着一定的安全隐患，网络空间安全，涉及国家安全，高校作为网络安全在教育系统的主要阵地，必须高度重视，发挥网络安全教育体系优势，提高自身网络安全防护和管理能力，加强网络安全技术队伍建设，赋能教育网络健康安全发展。

## 1 高校网络安全现状

在智慧校园建设不断深化的背景下，高校对网络信息资产的依赖程度显著提升，但与此同时，网络安全问题也日益凸显。首先，许多高校在管理众多网络设备、业务系统和应用平台时，存在权责不清的现象，导致部分信息资产闲置、失管，甚至未及时修复漏洞或更新补丁，这种管理缺位在发生网络安全事件时往往拖慢响应效率。其次，网络安全投入普遍缺乏前瞻性规划，偏重于硬件和平台建设，而忽视了对网络安全运维服务、设备更新与技术适配的同步投入，造成新旧设备难以兼容，服务功能难以协同。再者，不规范的网络安全运维流程也成为隐患，部分高校运维仍依赖经验主义，缺乏系统性的日志记录与审计机制，导致事件发生后难以追溯，影响问题处置的精准性与及时性。此外，网络安全人才队伍建设严重滞后，不少高校尚未设立专职岗位或配备专业人员，部分安全管理工作由非专业人员承担，难以胜任复杂网络环境下的防护与应对工作。与此同时，网络信息发布流程也存在短板，各单位通过自有平台发布内容时常绕过宣传部门和校级审核，导致信息准确性、导向性存在风险，甚至可能引发意识形态问题。总体来看，高校在智慧校园网络安全体系建设中仍面临资产管理混乱、投入结构失衡、流程操作松散、人员配置不足与信息发布审核机制缺失等一系列现实挑战，亟需从体制机制、资金配置、人才培养等多维度入手，推动高校网络安全体系向规范化、制度化和专业化方向发展。

## 2 高校智慧校园建设中网络安全相关技术

### 2.1 探针和态势感知技术

流量探针和网络安全态势感知技术是较新网络安全技术，流量探针主要通过捕获全网流量，通过记录和分析流量中源地址、目标地址、端口、数据内容等信息，对网络安全威胁进行预判。网络安全态势感知技术通过流量探针提供的相关威胁日志，比对本地或云端威胁特征库进行深度分析，针对不同类型的威胁信息结果进行分类整理，提供网络安全管理员全面和可靠的处理意见，也能自主联动其他网络安全设备执行安全处置。能够有效的提高网络安全防护能力，起到提早发现、提早干预，提早处置的作用。

### 2.2 防火墙技术

防火墙技术主要用于内网与外网之间，用于控制用

户访问内网与外网的权限，基于用户网络流量进行分析，通过防火墙相关安全策略的配置，可以有效控制外网与内网以及内网与内网中所有流量通讯的不安全访问，其技术原理是通过安全策略配置，检查所有通讯流量，对信任的IP、端口、范围或协议放行，不信任的进行阻断控制，以达到网络安全访问的效果。

2.3 WEB 应用防火墙技术

WEB 应用防火墙简称 WAF，主要设置在外网与 WEB 服务器之间，用于检测外网用户访问 WEB 服务的相关特征行为，基于外网访问 WEB 服务的流量分析，通过与 WEB 应用防火墙的本地或云安全特征库进行比对，放行安全的 WEB 访问，阻断外网 WEB 扫描、攻击和渗透等安全威胁的一种技术。WEB 应用防火墙技术能够增强 WEB 服务器的安全性，针对 WEB 应用代码的一些缺陷或安全隐患能够针对性保护。

2.4 网络日志和网络行为审计技术

网络日志技术主要指用户的网络访问、数据通信、信息交互等操作利用日志审计服务器进行记录。网络行为管理技术指通过对所控网络用户的访问行为进行监测，并将网络用户所有网络相关操作行为进行记录的技术，网络行为管理技术还能够屏蔽一些涉黄、涉暴、涉赌和政治敏感等关键字搜索和访问。网络安全部门可以根据日志审计和网络行为管理的记录对发生的网络安全事件以及用户网络行为进行查询，达到事件溯源的要求。

**3 网络安全技术在高校智慧校园中的具体实践**

3.1 加大网络安全新设备、新技术投入

随着网络威胁和风险种类的不断迭代升级，高校在智慧校园建设中面对着各种攻击和威胁风险，亟需引入新型的安全设备和安全技术。如：部署网络安全态势感知平台、零信任体系架构、下一代防火墙等。通过新设备、新技术的投入，强化网络安全设备间的相互联动和配合，并通过云端特征对比技术，更加精准的识别和判断攻击类型，提升网络风险威胁防御能力。

3.2 优化网络安全设备安全策略配置

网络安全设备安全策略决定了防护的效果，高校网络设备种类丰富，策略复杂，容易因配置失误导致网络安全风险增加，需要优化网络安全设备策略配置来提高设备整体性能和能力。首先，可以通过对现有安全策略做梳理，保留有效策略，删除重复和无效的策略，并按照优先级提高重要安全策略的执行顺序，提升安全设备的防护能力和整体性能；其次，安全策略应遵循最小权限原则，针对必须的业务端口、IP 或者相关协议放行，阻断一切不必要的流量，达到网络安全防御的最佳效果。

3.3 加强全网网络会话、网络行为的日志审计和记录

由于设备、对象和用户的复杂性，产生的网络日志较多，涉及服务器、云桌面、网络和安全设备、终端等。加强记录全网网络会话和行为日志应尽可能做到日志采集的全覆盖，保证网络日志的存储时长的合规性；其次，应做好日志访问和查询审计的权限管理，避免内部人员导致的日志篡改，保证日志的权威性和有效性；另外，为方便日志查询和整理，应尽量保证日志格式的标准化和统一性，可采用如 syslog、snmp 等日志类型，针对敏感日志的存储应采用加密或遮码处理。网络会话、网络行为日志是用户访问网络产生使用痕迹的的重要凭据，在发生网络安全事件时能够通过日志记录和审计对事件快速溯源。

3.4 增强网络安全设备间联动，避免形成安全设备孤岛

目前，针对高校的网络攻击日益复杂，传统人工配置网络安全设备无论从效率上还是从准确度上都无法满足安全管理需求。传统安全设备一般缺乏有效的威胁信息共享和协同，存在安全防御延迟、防护能力弱和防护覆盖不全全面等现象。为提高网络设备整体防护效率，减少网络安全设备间孤岛效应，可采取设备联动处置网络安全威胁风险的方式，根据预设的网络安全防护模型、通过本地或云端的威胁风险特征库对高校全网流量进行监测，比对风险行为和特征，通过大数据分析和研判鉴别威胁类型，并分类推送给相应的网络安全设备处理。整个处置流程实现自动化和不同网络安全设备的联动，节省了网络安全事件处置时间，提高了风险处置效率。

3.5 提高远程运维的安全性，规范远程运维操作流程

高校智慧校园建设过程中，需要对大量业务系统、网络架构和操作系统进行远程运维，容易因远程运维权限配置、远程运维操作等问题增加网络安全风险。首先，远程运维人员通过远程桌面、SSH、VPN 等工具访问高校内部网络，应强化身份认证，妥善保管私有密钥，杜绝弱口令和未经授权访问的情况；其次，远程运维过程中，应当对数据和命令的传输进行加密，防止数据泄露；再次，应严

格限制远程运维人员的操作权限、人员数量等，开启 IP 或 MAC 地址的白名单模式，限制远程运维访问操作的来源，减少远程运维方式的暴露面。另外应当做好远程运维的日志记录，定期对远程运维人员操作做合规性审计。

**4 高校智慧校园建设中网络安全管理探索**

随着智慧校园的加速推进，高校面临的网络安全风险持续升级。为保障信息系统稳定运行，构建系统化、规范化的管理机制显得尤为关键。

4.1 完善规章制度，落实安全责任

建立健全网络安全规章制度，是高校开展网络治理的基础。高校应结合自身业务架构，制定涵盖网络接入、账号权限、数据管理、安全审计等内容的管理细则，并明确二级部门网络安全责任，实行安全考核与奖惩机制。依据《网络安全法》等法规，对不同级别的信息资产进行分级管理，推动管理流程从“临时应对”向“常态规范”转变。

4.2 加强宣传教育，提升安全意识

高校用户群体庞大，安全意识参差不齐。可通过专题讲座、知识竞赛、宣传月等方式，定期开展网络安全宣传活动。将安全教育纳入学生课程体系，强化如防诈骗、防泄密、数据备份等基础知识。对教职工组织定期培训，明确信息发布、账户管理等操作规范，营造“人人重安全”的氛围。

4.3 构建安全平台，实现集中管理

高校信息系统复杂，需建设统一的网络安全综合管理平台，对网络资产、风险事件、权限日志等实现集中管理。平台应具备漏洞预警、策略审计、行为记录等功能，并支持多部门间的协同处置。通过平台数据可视化管理，提升安全工作效率，确保问题可追溯、处置有反馈。

4.4 推进等级保护，夯实合规基线

高校应依据国家等级保护要求，对教务、科研、财务等系统定级备案，并完成差异化防护。等级保护能帮助高校明确系统风险等级、制定防护策略，避免“一刀切”式投入浪费。同时，等级保护测评报告也作为信息化项目验收和管理合规的重要依据，是落实法定责任的重要抓手。

4.5 强化应急演练，提升响应能力

应急演练是检验管理制度和处置能力的关键措施。高校应定期开展模拟演练，涵盖数据泄露、网络攻击、舆情处置等常见场景。演练应覆盖技术处置、信息报告、恢复流程等环节，确保各级人员熟悉职责与流程。演练结束后，及时总结问题并修订应急预案，不断提升实战水平。

4.6 建设专业队伍，强化技术支撑

网络安全需要专业技术人员支撑。高校应设立独立岗位或科室，配备专职安全管理人员；加强在职培训，提升技术运维水平；依托专业优势设立实训基地，构建“教师 + 学生 + 企业”联合培养机制。同时，通过产教融合、项目合作等形式，引入企业力量参与高校安全工作，形成多层次、可持续的人才保障体系。

**5 结论**

高校在智慧校园建设过程中，风险和机遇并存，特别是网络安全建设方面，高校不仅面对日益增长的复杂网络安全形势，也经历着网络安全威协和风险的持续升级，对高校网络安全的防护要求越来越高。高校通过合理规划网络安全防御架构、加大网络安全设备投入、提高用户整体网络安全素养、优化网络安全管理和决策、提升网络安全专业人才队伍技术能力，能够更好的为高校安全服务。

**参考文献：**

[1] 宋雨泽 . 新时代青少年网络信息安全教育机制构建研究 [J]. 福建轻纺 , 2024,(05).

[2] 陈艳 . 高校智慧校园建设的探索与研究 [J]. 网络安全技术与应用 ,2025,(04):96-98.

[3] 田文君 , 王罕 . 智慧校园网络安全运营体系的构建 [J]. 办公自动化 ,2025,30(06):37-39.

[4] 郭晋勇 . “智慧校园”理念下网络安全与数据安全监测预警体系的设计与建立 [J]. 九江学院学报 ( 自然科学版 ),2024,39(04):65-69.

[5] 杜伟 . 智慧校园下网络安全一体化平台建设研究 [J]. 中阿科技论坛 ( 中英文 ),2024,(09):93-97.

[6] 李海蓉 . 智慧校园建设中无线网络安全问题探究 [J]. 网络空间安全 ,2024,15(04):284-287+294.

[7] 杨志杰 , 丁国平 , 潘敏 . 智慧校园通信网络安全通信资源智能分配方法 [J]. 长江信息通信 ,2024,37(09):181-183.