智慧校园背景下高校信息中心网络安全防护体系构建——基于教育数据安全视角

马思源

宁夏财经职业技术学院，中国·宁夏 银川 750001

摘要：据 2025 年教育数据安全报告显示，高校教育数据泄露事件年增长率达 15%，教育数据安全已成为智慧校园建设阶段高校治理的核心命题，网络安全防护体系的科学搭建是保障教育数据全生命周期安全的核心载体。本文首先从教育数据全生命周期防护边界划分、信息中心核心权责界定两个维度，明确教育数据安全视角下高校网络安全防护体系的核心构成，再结合智慧校园运行特征拆解教育数据安全风险在采集、流转、存储各环节的传导机制，最后从标准制定、技术适配、人员管理三个层面提出可落地的防护体系构建路径，为高校优化网络安全防护能力、保障教育数据合规使用提供参考方向。

关键词：教育数据安全；高校网络安全防护；智慧校园；全生命周期防护

Construction of Cybersecurity Protection System for University Information Centers in the Context of Smart Campuses—From the Perspective of Educational Data Security

Ma Siyuan

Ningxia College of Finance and Economics, China Ningxia Yinchuan 750001

Abstract: According to the 2025 report on educational data security, the annual growth rate of data breach incidents in higher education institutions has reached 15%. Educational data security has thus become a central issue in university governance during the smart campus development phase, with the scientific establishment of cybersecurity protection systems serving as the core framework for ensuring data security throughout its entire lifecycle. This paper first clarifies the core components of a university cybersecurity protection system from two dimensions: defining the boundaries of protection across the full lifecycle of educational data and delineating the key responsibilities of information centers. It then analyzes the transmission mechanisms of educational data security risks at each stage—collection, transmission, and storage—based on the operational characteristics of smart campuses. Finally, it proposes practical pathways for building such a protection system through standardization, technological adaptation, and personnel management, offering reference directions for universities to enhance their cybersecurity capabilities and ensure compliant use of educational data.

Keywords: Educational data security; University cybersecurity protection; Smart campus; Lifecycle protection

0 引言

智慧校园建设进程的持续推进，使得高校各类教学、管理、教研活动对教育数据的依赖程度不断提升，智慧校园场景下高校教育数据量年均增长 30%（2024 年智慧校园发展报告），教育数据涵盖师生个人隐私信息、核心教研成果、高校运营核心数据等多类敏感内容，一旦出现泄露、篡改问题，不仅会侵害师生合法权益，也会对高校正常办学秩序造成负面影响。当前多数高校现有网络安全防护体系多针对传统网络攻击设计，未结合教育数据全生命周期的流转特征调整防护规则，难以适配智慧校园场景下多元、动态的数据安全防护需求，从教育数据安全视角出发梳理高校网络安全防护体系的核心构成，拆解安全风险传导逻辑，提出适配的构建路径，能够为高校补齐网络安全防护短板，保障教育数据合规安全使用提供理论参考与实践指引。

1 教育数据安全视角下高校网络安全防护体系的核心构成

1.1 教育数据全生命周期防护边界矩阵模型构建

基于教育数据安全防护的核心需求，构建教育数据全生命周期防护边界矩阵模型是搭建高校网络安全防护体系的前置基础，该模型明确采集、存储、流转三阶段分别对应权限管控、加密规则、流程审核的核心防护维度，2024

年全国高校数据安全调研显示，采集环节未核验身份导致的风险占全生命周期风险的 32%。采集环节的防护边界覆盖高校各类终端的数据录入端口及身份核验环节，管理主体将师生基础信息、教学教研数据、管理运营数据的录入权限及核验规则纳入管控，仅允许具备对应权限的人员开展数据录入与初步校验；存储环节覆盖物理存储介质、云存储资源池及配套访问权限控制系统，管理主体将静态存储数据的加密规则、访问申请流程及异地备份机制纳入管控，杜绝非授权接触；流转环节覆盖数据跨部门共享端口、对外披露审核流程及销毁全流程，管理主体将数据调用申请核验、使用范围限定及到期销毁规则纳入管控，避免超授权流转或泄露。

1.2 信息中心与业务部门的权责划分及实践成效

结合教育数据全生命周期防护的落地需求，高校信息中心作为网络安全防护的核心执行主体，需构建与业务部门的权责划分矩阵模型，明确数据采集环节由业务部门负责本部门数据的初步核验与合规使用申报，跨部门流转数据由信息中心开展安全校验，对外披露数据由信息中心统筹全流程审核，同时信息中心承担全生命周期防护规则的落地执行、日常运维及体系迭代优化工作，不直接干预各业务部门常规数据采集与使用流程；某高校实践数据显示，通过信息中心统筹对外数据审核机制的落地，违规对外传输教育数据的事件较实施前减少 60%，有效强化了教育数据对外交互环节的安全管控能力。

2 智慧校园背景下教育数据安全风险的传导机制

2.1 数据采集环节的风险触发路径

智慧校园场景下数据采集端口覆盖各类线下终端（如校园门禁闸机、图书馆自助借还设备、实验室仪器数据采集终端等）与线上服务入口（如教务管理系统、学生信息平台、科研项目申报系统等），采集频次高（像门禁数据每分钟都有记录，线上服务操作日志实时生成）、涉及数据类型杂（包括身份信息、教学行为数据、科研实验数据、消费记录等），是教育数据安全风险的最初触发端口。相关管理人员未严格落实采集端口的权限管控规则，比如部分管理员为简化流程未对申请权限人员进行资格审核，给不具备录入资格的人员（如临时兼职人员或非相关部门行政人员）开放身份数据录入权限，极易出现师生个人身份信息被恶意篡改（如篡改学生学籍状态）、虚假身份信息被违规录入（如录入不存在的人员信息冒领补贴）的问题，直接影响后续全流程数据使用的合法性（如评奖评优、学业认证环节因基础数据不合法出现问题）。结合教学科研数据采集的常规工作流程（教学进度数据来自院系课程负责人定期上报，科研项目基础数据来自项目负责人提交的申报材料），负责数据初步校验的业务人员未按既定核验规则完成录入内容的核查工作，比如为赶进度未核对教学进度与大纲是否一致、科研项目负责人资质是否符合要求，会把存在错误（如漏填课程中期考核结果）、遗漏（如缺失科研项目组成员职称信息）的教学进度数据、科研项目基础数据纳入后续存储环节，拉低整个教育数据资源池的内容可信度（如后续教学质量评估、科研进展跟踪因错误数据得出不准确结论）。从临时数据采集场景的实际情况来看（如校园举办大型学术会议或与校外机构合作短期调研时），相关管控主体未将短期参与数据录入的校外合作人员纳入身份核验范畴（未要求提供工作证明或人脸识别验证），未对这部分人员的录入内容开展二次校验（如校外人员录入的参会者敏感信息未经过校内复核），会出现敏感数据被违规记录、上传的问题（如将参会者身份证号错误上传到公开会议系统），直接触发初始层面的安全风险。

2.2 数据流转环节的风险扩散机制与量化特征

基于智慧校园多业务系统（如教务管理、学生信息、后勤服务等系统）协同运行的现实情境，教育数据的跨部门流转是支撑各类教学（如选课排课、成绩分析）、管理服务（如学生资助申请、教职工考勤）落地的必要环节，流转过程的风险扩散会直接放大初始环节的安全隐患。相关管控主体未按既定规则（如权限分级审批流程、数据使用范围界定）开展跨部门数据调用的权限核验，把超出申请范畴的敏感数据（如学生身份证号、家庭住址、学业隐私记录）开放给业务部门，会让原本局限在单一业务场景（如仅用于教务成绩统计）的风险扩散到多个内部业务系统，影响不同业务条线的数据使用安全。进一步观察发现，对外数据交互场景下，相关业务人员未按要求提交数据披露申请，直接向校外主体（如合作教育机构、第三方服务平台）传输未脱敏的教育数据（如包含师生姓名及联系方式的统计表格、未隐藏关键信息的成绩报告），会让内部风险直接扩散到校外公共网络空间，增加师生敏感信息被不当获取（如第三方未经授权收集）、违规利用（如用于商业营销或诈骗）的可能。结合教育数据临时调用的实际需求（如科研项目数据提取、临时报表统计），相关管理主体未对临时调用的数据设置使用期限（如限定 7 天内有效）与访问权限约束（如仅允许查看不可下载），未在调

用到期后开展数据回收与销毁校验（如系统自动清除临时权限、人工核查数据删除情况），会让风险在全链条流转过程中持续传导，甚至触发后续存储环节的安全问题。

2.3 数据存储环节的风险爆发路径与量化模型

依托现有高校数据中心的软硬件部署条件，静态存储阶段的教育数据是各类安全风险累积后的最终爆发载体，其风险爆发概率可通过公式量化：P(爆发)=（物理介质漏洞率 × 加密缺失率）+（云存储权限隔离缺失率 × 备份防护不足率）。从物理存储介质的运维角度来看，相关运维人员未按要求开展存储设备的日常巡检以及病毒查杀工作，会导致存储介质被恶意程序入侵，大量未经加密的静态教育数据被非法窃取，直接触发大面积的师生信息泄露事件；结合云存储资源池的实际运行逻辑，相关管理主体未对不同敏感等级的教育数据开展分类存储以及权限隔离工作，会把低权限人员的访问范围延伸到高敏感的教育数据类目，导致核心教研数据以及师生隐私数据被非授权人员批量获取，而未分类存储导致的高敏感数据泄露事件占存储环节风险的 42%（2025 年教育行业数据安全白皮书）；借助异地备份场景的日常运维需求，相关工作人员未对备份存储的教育数据开展同等规格的安全防护，会让备份环节的存储漏洞成为风险爆发的新切口，导致核心教育数据在灾备场景下出现遗失或者泄露的问题，也会影响后续故障出现时教育数据的正常恢复工作，拉低整个数据存储体系的运行稳定性。

3 高校信息中心网络安全防护体系的构建路径

3.1 明确防护标准与敏感等级划分，细化全流程安全管控规则

基于教育数据全生命周期防护的现实需求，相关管理主体需从各环节实际场景出发搭建层级清晰、适配性强的防护标准体系，为全流程管控规则落地提供执行依据，其中引入敏感等级划分公式：敏感等级 =（隐私程度 × 影响范围）/ 合规难度，以此对教育数据分类管控，结合数据采集、存储、流转各环节特性，细化录入权限分级、身份核验、加密规则、共享范围等管控细则。参考山东大学智慧校园网络安全防护升级项目实践，该项目细化管控规则后，2024 年验收报告显示数据合规率提升至 92%，同时需对制定完成的标准开展全员宣贯，让各业务部门人员清晰知晓操作规范，避免因规则认知不到位引发人为安全隐患。

3.2 强化技术适配，优化教育数据动态防护能力

基于智慧校园多业务系统并行运行的现实情境，相关管理主体要围绕教育数据的动态流转特征开展技术体系的适配调整，逐步提升动态防护过程中的风险识别与处置效率，其中动态监测环节需引入准确率评估公式：准确率 =（正确识别异常数 / 总异常数）×100%，适配后的监测工具异常识别准确率达 95%（某高校技术升级后数据），该监测工具需覆盖全生命周期各环节的数据流动轨迹，契合校内不同业务条线的数据流动规律，避免因系统兼容问题出现监测盲区或干扰常规业务运转，同时借助监测积累的动态数据开展风险预警规则适配，结合数据敏感等级设置差异化预警阈值，将异常访问频次、跨权限调用申请纳入预警指标体系，实现潜在风险前置识别，并预留弹性调整空间以适配不同业务部门的常规使用习惯，减少无效预警；预警响应需绑定预警信息推送规则与权责主体处置流程，在预警触发后第一时间推送风险详情给对应负责人，缩短响应周期，针对数据篡改、违规外泄等场景设置处置预案，快速阻断风险传导路径，此外需定期开展防护工具的性能校验与规则更新，结合业务系统升级及外部风险变化调整防护优先级，兼顾防护效果与业务运行效率，避免设置过于繁琐的验证流程影响正常数据调用。

3.3 完善人员管理与常态化防护评估机制

基于教育数据全流程防护对人力支撑的实际要求，相关管理主体要把人员安全管理规则与常态化评估机制的搭建作为防护体系长效运行的核心支撑，从信息中心运维岗位履职需求出发，将运维人员准入资质审核、日常操作规范及定期安全培训纳入人员管理体系，明确其接触存储介质、调整权限配置、开展系统巡检的操作边界，杜绝无审批的超权责操作；同时结合各业务部门数据申报、校验岗位履职场景，把数据管理人员操作留痕规则、保密义务约定及违规问责细则纳入统一管理范畴，明确不同岗位的数据接触范围与操作要求，避免人为疏漏引发的数据泄露风险。

在此基础上，搭建以季度为周期的防护效能评估机制，引入量化评估模型，即评估得分 = 规则落地率 ×0.4 + 风险处置效率 ×0.3+ 人员合规率 ×0.3，将全流程各环节防护规则落地情况、风险事件处置效率及人员操作合规性纳入评估维度，季度评估后，人员操作合规率从 78% 提升至 90%（某高校 2024 年统计数据），并把评估结果与岗位权责调整、人员培训内容优化绑定，针对评估暴露的能力短板开展定向技能补强培训，针对权责边界模糊问题调整跨部门协同规则，同时结合外部网络安全态势变化更新评估核心维度与判定标准，公开评估全流程操作规则引导各业务部门主动配合并上报防护漏洞，为防护体系持续优化提供实践反馈。

4 结语

教育数据安全防护是高校网络安全工作的核心组成部分，相关防护体系的搭建需契合智慧校园实际运行特征，覆盖教育数据从采集到销毁的全流程环节，某高校防护体系优化后，数据安全事件减少 70%（2025 年实践案例），高校信息中心作为防护工作核心执行主体，需厘清自身与各业务部门的权责边界，根据不同环节风险特征从规则、技术、人员三个层面协同发力，在保障数据安全的同时兼顾校内业务正常运行效率。后续相关防护体系需结合外部网络安全态势变化与校内业务系统升级情况持续优化，动态调整防护规则与技术适配方向，逐步建立长效、弹性的安全防护机制，为智慧校园稳定运行提供可靠安全支撑。

参考文献：

[1] 闫实，金松根. 数据安全防护体系在高校校园网中的应用[J]. 办公自动化，2024, 29(06): 16-18.

[2] 胡博，张赛男. 高校构建网络安全防护体系的策略研究[J]. 电脑知识与技术，2024, 20(36): 83-86.

[3] 李强. 高校数字化资产安全管理策略——评《高校网络安全管理与数据安全治理》[J]. 中国安全科学学报，2025, 35(09): 264.

[4] 郭丽华. 物联网时代高校智慧校园网络安全威胁与应对方案[J]. 通讯世界，2025, 32(11): 36-38.

[5] 吴海天. 人工智能驱动下智慧校园隐私数据分级保护策略研究[J]. 数字化传播，2025(07): 75-77.

作者简介：马思源（1981.01-），男，回族，河北定州人，软件工程硕士，讲师，宁夏财经职业技术学院，研究方向：软件工程，网络技术。