# 智慧校园网络环境中的数据安全问题及应对策略分析

耿亚涛
（郑州电力职业技术学院　河南郑州　451450）

【摘　要】随着我国高校信息化技术的飞速发展，教育信息化2.0逐步向教育信息化3.0迈进。智慧校园的建设离不开网络的支持，但随之而来的是日益突出的数据安全问题。本文通过对目前我国智慧校园网络环境中的数据安全问题的研究分析，提出了几点相应的应对策略，希望有助于促进完善高校智慧校园的建设。

【关键词】智慧校园；网络环境；数据安全；应对策略

**DOI:** 10.18686/jyfzyj.v2i12.33069

## 1 智慧校园概述

智慧校园指的是工作、学习和生活都处于以网络为基础的智慧化环境中，在这个环境里，任何人都能很方便地得到资源，获取想要的服务。其三个核心特征是：①提供以人物角色为基础的个性化智能感知环境和综合服务；②将信息技术全面融入校园生活的方方面面；③通过智慧化平台为学校提供一个与外部世界进行交流和感知的接口。由此可见，智慧校园建设的基础是网络校园的建设，这就意味着有线网络与无线网络覆盖是必不可少的。

## 2 我国目前智慧校园网络环境中的数据安全现状分析

### 2.1 用户管理不规范

智慧校园网络环境中的用户对网络的认识程度和数据安全的重视程度不一，甚至大部分用户都没有养成良好的使用校园网络的习惯，这就可能会引发网络数据安全问题。此外，校园网络中很大一部分病毒是由于移动存储设备交叉感染造成的，但许多用户没有建立足够的安全防御意识，在使用移动存储设备时不会查杀病毒和定期对自己的电脑进行病毒库升级杀毒，以保障设备的安全性。

### 2.2 网络架构不完善

智慧校园的建设并不是一成不变的，通常会随着新的信息技术、科学技术和要求的出现而不断更新，这就会导致在网络安全建设的过程中缺少整体性规划。且不能对重要的数据进行备份和异地容灾备份，并对重要的数据系统进行定级备案等保测评。这就意味着，当发生网络数据安全事件时，相关的管理人员可能没有办法及时发现问题的根源，从而给学校造成一定程度上的损失。

### 2.3 防御手段不全面

数据表明，我国一直以来都频繁出现针对校园网络的恶意攻击事件。例如，我国多所大学校园网在 2017 年的全球最大勒索软件攻击事件中中招，这是因为教育网对国内曾多次出现利用 445 端口传播的蠕虫病毒并无限制，因此高校成为不法分子进行网络攻击的重灾区。当时正值毕业论文季，这波网络攻击给学生们的学习资料和个人数据造成严重的损失。造成攻击的主要原因是很多学校由于安全防护手段不全面，导致管理人员对于潜在的威胁难以及时察觉。

### 2.4 全网资产数据不清

想要通过一种防护方案去解决所有的安全防护问题，这是不可能实现的，也就是说，网络数据安全的防护需要具有针对性。这就要求相关技术人员在最开始进行安全体系建设时，就必须要将全网所有需要被防护的资产纳入其中。但实际上，我国目前很多高校管理部门并没有对全网资产信息进行详细地统计，在此前提之下主动的安全防护就无从谈起，只能进行被动的安全事件处理，而且经常无法责任到人，导致最终无法对出现的安全问题进行及时处理。

### 2.5 管理难度大

首先，我国很多高校的二级学院都有单独的管理网站和系统，但是对于相关工作人员的权利和责任的分工又不够明确，这就会给管理工作造成更大的困难。其次，一些高校早期的资料都是进行纸质备案的，相较于电子版备案，纸质备案的管理所需要耗费的人工和时间都更多，这就意味着一旦发生紧急的数据安全问题就无法迅速准确地对事件进行处理，对相关责任人进行追责。最后，部分高校的二级学院还存在十分严重的私自搭建管理网站和系统的现象，但是自身的监管力度又有所缺乏，这就很容易导致出现问题时很难对网站和系统进行检测。上述种种问题，都会对学校产生负面影响。

### 2.6 缺乏有效的安全管理体系

安全管理体系由软件和硬件两个部分组成。所谓软件是指思想、制度和管理等；所谓硬件是指技术、设备等。就硬件来说，我国大部分高校目前都多多少少引进了相应的安全产品，以加强自身的校园网络数据安全系数，但是自身依然缺乏了“软件”防护，这就会导致安全产品成为一种摆设。

### 2.7 安全人员数量不足，待遇差

我国大部分高校都更侧重于引进和培养教学和科研人员，而把网络信息安全者归于教育辅助部门，用人方式也多是以人事代理或者临时工为主，这就造成了网络信息安全者相对于教师来说，在工资收入和社会地位等方面都更低一些，这不但无法发挥工作人员的积极性，也会导致人才流失。

## 3 智慧校园网络环境中的数据安全问题的应对策略

针对智慧校园建设中可能存在的数据安全风险，广大高校应该采取相应的应对策略，以保障智慧校园的建设进度。本文探讨出的措施具体如下。

### 3.1 构建健全的网络安全体系

建设智慧校园网络数据安全防护体系并不是一个简单的工程，其涉及技术、人员、法治规定等多个方面，并且需要以各个高校自身的网络运行实际为依据。在建设智慧校园网络安全体系时，应该针对每一层都采取具有针对性的安全保护策略，这样才能在整体上提高数据的安全性和传输可靠性。例如，通过数据加密、数据清理等技术和措施对数据层进行安全保护，对重要的文件和数据进行备份。以达到提高信息的安全性和确保智能设备正常运行的目的。除此之外，还可以从强化系统对风险因素的预测入手，例如，设立安全状态感知设备，利用感知设备还可以及时对校园网络运行过程中产生的数据和安全信息进行采集，然后通过对这些数据和安全信息的分析将智能设备的 bug 和用户访问行为等情况转化成数据信号，进而根据数据的反馈及时发出预警信号和制定风险防护方案。与此同时，设置相应的技术人员和管理制度，以确保各项技术及策略在安全体系运行过程中能够得到有效落实，并逐步完善系统安全功能。

### 3.2 保障智能设施安全稳定运行

智慧校园的建设需要一个统一的平台，而确保这个平台的安全稳定运行对于保障网络数据安全而言至关重要。通常来说，包括要减少类似于地震、火灾等不可抗力因素对软件资源和硬件设备的损坏以及外力干扰对智能设备系统的不利影响。这就要求在搭建或者选择智能设备时要注意服务器的可靠性和扩展性，同时设置不间断电源，以确保系统能够一直稳定运行；在设计校园网络中心交换机时，要同时兼顾网络之间的有效连接问题和局域网划分问题，这样才能避免由于网络问题而造成的通信障碍问题；在选择网络数据的存储设备时，要考虑设备的稳定性和性能，这样不仅能保障数据储存的完整性，还能有效提高数据的安全性。

### 3.3 确保数据信息安全

所谓数据信息安全是指将网络数据信息储存在学校的可控制范围以内，如果将所有的网络数据都储存在服务器中，无异于将所有的鸡蛋都放进一个篮子里，提高了数据安全的危险系数。从访问控制、数据隔离、数据加密等多个角度去思考如何确保智慧校园网络数据的安全，才能真正达到保障网络数据安全的目的。首先，实施数据隔离。虚拟化的数据库隐藏着大量的安全隐患，因此要根据实际的应用要求对网络数据采取相应的隔离措施，这就需要对校园网络数据进行分类处理。其次，要对访问控制给予足够的重视。即利用数据加密技术对于用户的数据访问权限进行明确的界定，每一名用户只有在输入了用户名和密码后才能使用智慧设备，而且可查询的信息根据用户身份的不同也有不同的限制。这就要求学校要建立一个对用户进行身份认证的平台，这不仅能够保障网络数据的安全以及数据访问的有序开展，还能强化对用户的管理。最后，还要加大对数据加密的重视，因为通过数据加密能够有效提高用户个人数据的安全性，保证数据不会被非法分子盗取，以避免由于个人数据泄露而造成的损失，尤其是隐私数据，一旦泄露带来的后果是不可预估的。除此之外，由于智慧校园的网络数据储存在共享设备中，一旦出现数据残留的问题就会极大程度地增加网络数据的安全隐患，因此工作人员要及时对数据进行清理，以避免发生私自搭建的问题。

### 3.4 提高校园网络安全防护能力

一方面，高校都应该建立一套安全系数较高的网络安全防护体系。例如，注重边界防护，具体来说就是根据办公区域、学习区域以及其他区域的具体安全防护需求来制定具有针对性的访问策略，从而对整个校园网络进行全面控制。另一方面，要充分利用防火墙技术。在实施安全防护策略时，可以将交换机端口和防火墙进行有机结合，对于重点防护区域可以设置访问权限，进行隔离保护，并且要对重要的数据进行备份和异地容灾备份，对重要的数据系统进行定级备案等保测评，以保证重要数据安全。

### 3.5 培养专业技术人才队伍

加大对计算机操作人员的安全培训力度，定期开展网络安全知识培训，并且加大对保管核心数据人员的网络数据安全培训力度，加强计算机信息安全的防护措施。

## 4 结语

我国目前正处于信息化技术快速发展的过程中，我国教育部于 2018 年 4 月 13 日正式提出《教育信息化 2.0 行动计划》，促进了教育信息化的发展。行动计划中指出要实现从专用资源向大资源转变；从提升学生信息技术应用能力、向提升信息技术素养转变；从应用融合发展，向创新融合发展转变。建设智慧校园不仅是顺应社会发展的潮流，也是更好满足师生各方面需求的趋势，这就对各个学校搭建智慧校园数据安全防护体系提出了更高的要求。综上所述，学校要做好以下几点：首先，构建网络安全体系，从各个层面抑制网络数据安全问题的发生；其次，确保智能设施安全运行，从而保障网络数据的完整性；再次，确保数据信息的安全，从源头上降低威胁网络数据安全的隐患；最后，提高校园网络的安全防护能力，以便在发现网络数据存在安全隐患时能够及时进行处理。

**作者简介：**耿亚涛（1978.9—），男，河南郑州人，工程师，研究方向：计算机信息管理，计算机信息安全，计算机网络技术等。

## 【参考文献】

[1] 段忠祥. 智慧校园网络环境中的数据安全问题及应对策略 [J]. 网络安全技术与应用，2019（03）：61+74.
[2] 刘岳山. “互联网 +”环境下智慧校园数据安全治理 [J]. 网络安全技术与应用，2020（06）：105-106.