# 大数据背景下信息通信网络安全管理策略

任平平
武汉华夏理工学院　湖北武汉　430223

**摘　要：**在大数据时代，信息通信网络已成为社会运转的核心基础设施，但其开放性、复杂性和数据密集性特征使其面临前所未有的安全挑战。本文从大数据背景下信息通信网络的安全现状出发，深入剖析硬件设施、网络攻击、内部威胁等核心安全问题，结合技术防护、管理机制、法律规制等维度提出系统性解决方案。通过分析中国电信量子加密、见微安全大模型等创新实践，以及国家网信办典型案例的警示作用，提出以技术创新为驱动、以制度完善为保障、以人才培养为支撑的三维防护体系，为构建安全可信的信息通信网络环境提供理论参考与实践路径。

**关键词：**大数据；信息通信网络；网络安全管理；量子加密；数据安全

## 前言

在信息技术高速发展的今天，大数据时代全面到来。大数据技术凭借强大的数据处理与分析能力给各行业都带来空前的机遇与挑战。在这种情况下，信息通信网络是大数据传输与存储的重要基础，因此网络的安全性就变得非常重要。信息通信网络安全问题不仅涉及个人信息保护、企业商业利益等问题，而且还涉及国家安全与社会稳定问题。但是在大数据环境中，信息通信网络所面临的许多安全问题是错综复杂的，常规的安全管理策略已很难适应现实的需要。所以，对大数据环境下信息通信网络安全管理策略进行深入研究具有十分现实的意义。

## 一、大数据背景下信息通信网络安全概述

大数据浪潮席卷而来，以信息通信网络为核心枢纽的数据流转安全形态正在发生深刻的变化。云端、边缘端和终端之间大量数据的高速流动不仅催生了智能决策和实时服务的创新应用，而且使得传统的安全边界变得越来越模糊——物理隔离失灵，攻击面呈指数级膨胀，威胁传播速度超过毫秒级。数据价值成倍增长，引来多方势力争夺，由黑客组织牟利攻击转向国家级APT，由勒索软件产业化扩散至供应链投毒隐蔽渗入，安全威胁由技术漏洞向系统性风险演化。与此同时，大数据的“4V”特性（海量、高速、多样、真实）对防护体系提出全新要求：PB级数据加密需突破性能瓶颈，非结构化数据检测需要跨模态分析能力，低质量数据隐蔽攻击需要智能识别技术，分布式架构安全协同需要统一管控平台等。基于这一背景，信息通信网络安全已经超越了单一技术范畴而成为集密码学、人工智能和量子通信于一体的交叉研究领域，其防护逻辑正由“被动防御”向“主动免疫”转变，通过建立涵盖数据全生命周期并贯穿云网边端的动态防御体系，在确保数据可用性、完整性和保密性的同时构筑数字经济稳健运行的基础。

## 二、大数据背景下信息通信网络面临的安全问题

### （一）信息通信硬件设施安全问题

信息通信硬件设施作为信息通信网络运行的根基，它的安全状况直接关系到整个网络是否能够安全地运行。在通信技术不断发展的背景下，通信设备的种类越来越多元，并且它们的构造、使用方式不尽相同，给通信网络安全管理工作带来了越来越大的难度。比如陈旧的通信设备会有硬件漏洞易被攻击者利用，造成数据泄露或者网络故障等。与此同时，部分公司为了降低成本，采用的电脑及操作系统也很陈旧，甚至有的采用了被淘汰的操作系统，从安全性上看，它们的表现很差，网络通信安全一旦发生问题，不能对来自外部的攻击做到有效预防和控制，就会导致核心数据和企业信息系统瘫痪的不同局面，这严重制约了企业未来的发展和经济效益的提高。另外，硬件设施物理损坏、自然灾害等都会造成数据丢失、网络中断。

### （二）网络攻击与病毒威胁

网络攻击以及病毒威胁正在变得越来越复杂和严重。“永恒之蓝”勒索病毒于2017年5月爆发，该病毒使用了NSA漏洞百出的“EternalBlue”漏洞攻击工具，并在Windows网络共享协议的帮助下迅速蔓延，开源平台及其他因素使得攻击门槛越来越低，其表现形式也变得越来越复杂和自动化。到2024年，勒索软件攻击成本极高，一名受害者支付了7500万美元；商业电子邮件诈骗

仅当年报告的21，442起事件就盗取27.7亿美元。这些袭击旨在盗取、篡改和破坏数据等。威胁涉及的人员范围很广，既有独当一面的黑客，也有条理清晰的网络罪犯，还有国家扶持的群体，其手段五花八门，涉及恶意软件攻击和社会工程诈骗。进入2025年，勒索病毒呈多样化、变种快速发展。重大数据泄露可能导致公众审视和其他后果，个体还可能面临身份失窃的风险，因此认清网络攻击的实质对于加强安全措施和防御风险具有重要意义。

**（三）内部安全威胁**

内部安全威胁如潜藏暗流的漩涡，在信息通信网络中持续侵蚀安全根基。部分员工受利益驱使，利用职务便利将核心数据拷贝至个人设备，通过暗网交易牟取暴利，某企业技术骨干窃取用户数据库后，导致数百万条个人信息流入黑市，引发大规模诈骗案件。更多威胁源于无意识行为，员工在公共场所连接伪造WiFi处理敏感文件，或误将含机密信息的邮件发送至错误地址，某金融机构员工因操作失误，将客户资产数据泄露至外部群组，造成重大声誉损失。此外，第三方合作方的管理疏漏亦成隐患，未严格审查的运维人员可能植入后门程序，某物流平台因外包团队权限管理失当，导致运输轨迹数据被篡改，引发供应链混乱。这些威胁往往因隐蔽性强、溯源困难而难以根治，需通过零信任架构限制内部访问权限，结合行为分析技术实时监测异常操作，将安全管控贯穿数据全生命周期。

## 三、大数据背景下信息通信网络安全管理策略

**（一）加强大数据技术的研发与应用**

强化大数据技术研发和应用可以从几个重要方面着手。在金融风控中，应重视数据驱动信用评估体系的建设，采用多源数据集成方式，使用API接口集成征信、交易和社交信息，打造全维度数据视图；利用机器学习算法进行优化，例如XGBoost、LightGBM模型与图神经网络相结合进行关联关系分析，增强对异常行为的识别能力；构建了实时反欺诈系统，并基于流处理技术进行秒级的交易行为监控和风险阈值的调节，如某银行推出的大数据风控平台，信用卡欺诈检测的准确率得到了极大提高。在智慧医疗方面，通过大数据辅助精准诊疗、融合病人全流程数据、优化手术排期、术后并发症报警等；采用关联规则挖掘技术对临床试验数据进行分析，加快药品研发的速度。然而为了解决数据标准化不充分、伦理风险大的问题，可以采用联邦学习的方法对多方数据进行联合建模，同时又能保护隐私。在智慧交通方面，将车联网数据进行融合，建立动态的交通态势图；使用强化学习调度算法对信号灯进行优化控制，并使用自动驾驶数据对迭代模型进行性能闭环。通过边缘计算和云协同以及区块链实现数据可信流通来解决实时性及数据可信的问题，从而缓解城市交通拥堵的问题。此外，大数据还可用于能源管理、制造业、农业、零售业等领域的优化升级，同时要应对数据孤岛、数据安全等挑战，推动大数据技术不断发展。

**（二）打造合理的数据中心体系**

布局设计时，应结合实际选用单层或者多层的数据中心。单层数据中心的布置规划方便，设备可以在一个层次上进行高效布置，降温、电源分配及电缆管理方便，易于维护，横向扩展更方便，尽管安全和火灾风险的管理更为简单和容易执行，但这需要更广阔的空间，在土地有限的城市环境中可能不是一个可行的选择，而且安全相关的外部成本也相对较高。而多层数据中心能够在较少的用地占用空间下增加数据容量，适合用地稀缺且价格昂贵的城市地区使用，可以实现垂直扩展以满足城市低延迟作业的要求，也可以执行具体到地板上的冷却区来优化能源的利用，但是垂直设计对冷却及电源系统要求较高，结构设计比较复杂，在维修及设备更换等方面具有较大的挑战。从位置上看，数据中心应该选择电力供给足够可靠、通讯迅速顺畅、交通便利的场所，而用水蒸发冷却方式进行制冷的数据中心则需要确保有足够的水源，同时应远离粉尘、油烟等有害气体及生产或者储存有腐蚀性、易燃和易爆物品的地方，避免有自然灾害隐患的地区、强振源和强噪声源及强电磁场的干扰等因素影响。能源和供电保障同样重要，双路市电的优先连接、柴油发电机及UPS的匹配、可再生能源绿电消纳的同步进行、“光伏加储能”等微电网的配置等都是为了减少能源消耗、提升能源效率的重要手段。除此之外，还需要遵循数据中心的设计规范、等保2.0标准、绿色数据中心的规范等合规性要求，并密切关注地方政策，例如“东数西算”的节点布局和可再生能源的补贴措施等。

**（三）严格访问控制**

为了确保信息系统的安全性，严格的访问控制显得尤为关键，特别是在如今的复杂网络背景下。访问控制需确保所有访问行为可审计，详细记录主体、客体、时间、操作、结果等信息，如记录“用户张三在2025–07–09 10：00试图移除文件A，但由于没有权限而未能成功”的日志，便于追溯问题，及时发现异常访问行为。访问控制在未来呈现智能化、自动化趋势，采用人工智

能、机器学习等技术对用户行为进行自动识别、对访问权限进行动态调节，增强安全性。同时遵循零信任安全模型，对用户在内部网络中的认证与权限审查均不予默认信任。执行最小权限原则，只赋予用户执行任务的最低权限，以减少潜在安全风险。某大型电力公司在实践中通过构建以角色为中心的访问控制系统来明确员工的责任与权限，并与双因素身份验证技术相结合来提高系统的安全性。并定期对访问日志进行分析，对不正常的访问进行及时处理。为了确保访问控制的有效执行，需要全面考虑不同用户群体的安全需求，确认所有的系统资产，确保信息分类和授权策略是一致的，满足相关的法律法规要求，并持续更新维护策略。

**（四）做好黑客防范，完善防范机制**

搞好黑客防范、健全防范机制，是确保网络安全的重点。了解黑客攻击核心技术，建立配套防范体系是关键。黑客往往利用系统或者网络漏洞采取横向移动、数据窃取或者破坏的方式进行攻击，可以清理痕迹来掩盖攻击行为，攻击方式多种多样，例如假冒电话套取资料，使用恶意软件对系统进行控制或者破坏等。要对付这些袭击，就需要建立一个多层次、主动式防范体系。在基础防护上，实行网络隔离，利用防火墙、VLAN技术实现关键业务系统和外部网络的分离；执行访问控制、遵守最小权限原则、严禁管理员账户的误用、启用MFA以加强账户安全；设置自动化补丁更新机制对已知的漏洞进行及时修补。也可以通过蜜罐技术、部署虚假系统引诱黑客、搜集攻击手法等手段来提高防御策略。数据安全加固方面，实现敏感数据加密传输和存储、关键数据定期备份以及恢复流程有效性验证。另外，增强用户及企业对网络安全的认知与教育是必不可少的，宣传网络安全知识与技术，增强辨别网络信息、避免误操作遭受打击的能力。

**（五）加强网络法律法规的制定**

强化网络法律法规制定，是维护网络空间秩序、保障公众权益至关重要的措施。在互联网技术日益发达的今天，网络空间已经成为国家治理中的一个崭新领域，而网络法律的颁布与实施则为网络行为的制定提供了明确的规范，它可以有效地打击网络犯罪及侵权行为、维护网络空间秩序和稳定等。但是，目前的传统法律框架正面临着新的考验，由于网络技术的不断进步，现行的网络法律框架难以与之同步，对于网络犯罪的管理和跨国互联网活动的执法权限也存在一定的限制。因此，立法部门有责任制定与时代发展相适应的法律规定，以确保网络安全得到有效的维护和公众权益得到保障，同时也要防止公众面临不当起诉的风险。为了适应数字时代发展的需要，我国网络法律应不断完善与健全，如修订传统刑法、增设有关以信息网络犯罪作为惩罚对象的条款等。另外，司法技术需要改进与完善、投资需要增加、高素质司法人才的培养、打击与防范网络犯罪的技术支持与人才保障也需要加强。今后，伴随着大数据、云计算以及人工智能的运用，我国将会建立起更加完备的网络法律体系，更好地保障公民个人信息安全与隐私，规范互联网企业行为、促进公平竞争、为发展数字经济提供法治保障等方面进行研究。

## 结论

大数据背景下的信息通信网络安全管理是一场持久战，需技术、管理、法律三管齐下。通过研发量子加密、AI安全等核心技术，构建“云网边端”协同防御体系；通过优化数据中心架构、实施零信任访问控制，提升系统内生安全能力；通过完善法律法规、加强国际合作，营造法治化网络空间。唯有如此，方能在享受大数据红利的同时，筑牢国家网络安全屏障，为数字经济发展保驾护航。未来，随着6G、数字孪生等新技术的融合应用，网络安全管理将面临更多挑战，但只要坚持创新驱动、系统治理，必能开创安全可控的数字化新未来。

## 参考文献

[1] 王鹤馨. 大数据背景下信息通信网络安全管理策略研究 [J]. 电子元器件与信息技术，2024，8（09）：141-143+147.

[2] 张利. 大数据背景下网络信息安全管理问题及优化策略研究 [J]. 市场瞭望，2024，（17）：169-171.

[3] 狄敏. 大数据下计算机信息技术在网络安全中的作用分析 [J]. 科技视界，2024，14（19）：32-35.

[4] 景李. 大数据背景下信息通信网络安全管理策略研究 [J]. 信息与电脑（理论版），2024，36（11）：208-211.

[5] 邱丹青. 大数据背景下信息通信网络安全管理措施探讨 [J]. 中国新通信，2023，25（23）：10-12.