数字化转型下大数据网络安全风险及防控对策

苑小军
山西赛盾网络安全测评技术有限公司，山西 太原 037000
DOI: 10.61369/TACS.2026070011

摘　　要： 2025 年我国数字经济规模突破 60 万亿元、占 GDP 比重超 45%，数据成了重要的生产要素，大数据技术在政务、金融、工业、医疗等领域应用越来越快，在释放数据要素价值、提高生产效率的同时，也暴露出一些不同于传统网络安全场景的特殊风险，给我国网络安全防护体系建设和数据治理带来了新的挑战。本文对数字化转型背景下的大数据网络安全风险进行梳理，提出相应的防控措施，为筑牢大数据安全防线提供一定的借鉴。
关 键 词： 数字化转型；数字经济；大数据网络安全风险；防控对策

Big Data Cybersecurity Risks and Prevention Countermeasures Under Digital Transformation

Yuan Xiaojun
Shanxi Saidun Network Security Evaluation Technology Co., Ltd., Taiyuan, Shanxi 037000

Abstract: In 2025, China's digital economy will exceed 60 trillion yuan in scale, accounting for more than 45% of GDP, making data an important production factor. Big data technology has been increasingly applied in fields such as government affairs, finance, industry, and medical care. While releasing the value of data factors and improving production efficiency, it has also exposed special risks different from traditional cybersecurity scenarios, bringing new challenges to the construction of China's cybersecurity protection system and data governance. This paper sorts out the big data cybersecurity risks under the background of digital transformation and proposes corresponding prevention and control measures, aiming to provide reference for building a solid line of defense for big data security.
Keywords: digital transformation; digital economy; big data cybersecurity risks; prevention and control countermeasures

引言

目前全球数字经济正在经历快速创新、深度渗透的发展阶段，我国先后出台了《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《“十四五”数字经济发展规划》等一系列政策法规，对数据安全治理和网络安全防护提出了明确要求，为推进数字化转型的有序进行奠定了坚实基础[1]。然而，随着各个领域数据采集、传输、存储、应用规模的不断扩大，数据流转环节越来越多，大数据平台的集中化存储特性使得海量数据成为网络攻击的主要对象。2025 年某头部电商平台因大数据平台漏洞导致 1.2 亿用户信息泄露，直接经济损失超 2.3 亿元。新的架构、新的场景下出现的安全漏洞也越来越多，传统的防护机制已经不能满足大数据动态运行的特点，安全风险发生的概率、影响范围和危害程度都在不断上升。如果不及时整理并解决大数据场景下出现的新安全问题，既会妨碍数据要素自由流动和价值实现，又会对企业的经营安全、用户的个人信息安全乃至国家网络空间主权安全造成威胁。因此，对数字化转型背景下的大数据网络安全的特殊风险进行系统地分析，建立适应大数据发展的安全防护体系，已经成为促进数字经济高质量发展所必须面对的重要问题。

一、数字化转型下大数据网络安全的核心独有风险

（一）数据全生命周期的系统性风险，因大数据属性被指数级放大

传统的数据场景中，风险一般只存在于存储或者应用这些单一环节当中，影响的范围也相对有限；但是大数据有着多源聚合、全链路流动、集中存储等特点，风险会沿着数据流转的链条进行传播扩散，任何一个环节的安全漏洞都会引起整个生命周期的连锁风险[2]。多场景大规模数据采集过程中存在过度收集、违规采集现象，据工信部 2025 年抽查结果，62% 的移动应用存在过度收集个人信息问题，其中 38% 的应用收集了与服务无关的生物识别信息，大量敏感个人信息、核心业务数据从源头上就埋下

Copyright © This Work is Licensed under A Commons Attribution-Non Commercial 4.0 International License.

了泄漏隐患，在传输环节，跨平台、跨机构的数据共享交换越来越多，开放链路增多大大提高了数据被拦截、窃取的可能性，在存储环节，海量数据集中到大数据平台之后，如果平台防护被突破，就会造成大规模数据批量泄露，危害程度远大于传统分散存储场景，在流通和应用环节，数据的二次加工、多方共享使得数据权属关系变得愈加复杂，违规流转、滥用敏感数据的行为也难以追查定位，从而进一步加大了全链路系统的系统性风险。

（二）攻击手段针对性升级，专门瞄准大数据架构漏洞

传统的网络攻击大多以窃取系统权限、破坏服务可用性为最终目的，而对大数据平台的攻击，其主要目的就是针对高价值的大数据原生架构漏洞进行攻击[3]。目前主流的大数据开源组件自身就存在着设计上的安全漏洞，部分开源组件没有设置完备的身份认证和权限控制，很容易被攻击者利用未授权访问漏洞直接获得数据访问权限；大数据平台一般使用分布式计算、多租户共用资源的架构，不同业务的数据存放在同一个集群里，攻击者可以利用侧信道攻击、节点间的通信漏洞来窃取跨租户的敏感数据，这些新型的攻击方式不能被传统的防护工具所识别和阻止。除此之外，大数据同人工智能技术相融合之后，攻击方可以借助人工智能算法去自动化地挖掘大数据平台中的潜在漏洞，从而批量产生出针对攻击脚本，这样攻击的效率以及隐蔽性就得到了极大提升，防御方对于攻击的发现与处理也变得更加困难。

（三）传统安全技术体系全面失效，无法适配大数据运行特征

传统的网络安全体系是以边界防御为理念，用防火墙、入侵检测系统来构建内网边界，认为边界内部是可信的[4]。但是，在大数据环境下，网络边界已经完全消失，传统的技术体系存在着根本性的缺陷，不能处理大量的高并发流量，传统防火墙的最大吞吐量普遍在 10Gbps 以下，而当前主流大数据平台的峰值流量可达 50-100Gbps，导致传统设备漏检率高达 42%，造成检测卡顿、漏检严重；缺少了数据层面的防护能力，只关注网络层和系统层的攻击，不能识别出内部批量导出、多源非法融合等数据层面的异常；不能追踪到全域的数据流转，只能监控单一节点的状态，数据泄露之后很难快速找到泄露的节点；防护模式被动滞后，以事后响应为主，不能对海量数据异常访问进行事前预警。

（四）安全管理与合规体系滞后，难以应对海量数据治理难题

目前大多数企业和机构的安全管理仍然使用传统的、小数据场景下粗放式的机制，面对 PB 级的海量异构数据，不能对全量数据进行准确的分级分类梳理，核心敏感数据的存储位置、流转路径不能清楚掌握，数据访问权限也不能做到精细化配置，越权访问、内部数据违规流出等问题很难控制[5]。与此同时，伴随着我国数据安全领域法律法规体系不断完善，监管部门对于数据处理活动的合规要求也越来越细，2025 年全国市场监管部门共开出数据安全罚单 1173 张，罚款总额超 12 亿元，其中金融、医疗行业占比分别为 32% 和 28%。但是许多市场主体还没有建立起符合新规要求的合规管控流程，不能对数据采集、处理、共享各个环节的合规性进行持续审计，在合规检查、泄露溯源中也无法快速出具相应的合规记录，应对监管要求和风险处置的能力明显不足。

二、大数据网络安全的系统性防控对策

（一）构建大数据全生命周期原生安全防护体系

针对大数据全生命周期独有的风险，把安全能力嵌入到大数据架构当中，实现“数据在哪里，安全就在哪里”。数据采集阶段创建起多源数据接入统一认证体系，对所有的终端以及接口展开身份核验并加以安全加固，然后布置数据清洗设备，清除掉虚假数据和恶意数据，从源头保证数据品质[6]。数据传输环节用国密 SM4 算法对海量传输数据做端到端加密，创建起专门的安全传输通道，部署高性能流量清洗设备，可以对 PB 级流量实施实时检测并拦截恶意流量。数据存储阶段用分布式加密存储技术，对不同级别的数据采取不同的加密方式，核心敏感数据用硬件加密；按照零信任的思想创建细粒度的访问控制体系，实行“一人一权限、一数一授权”，阻止批量的数据无审批导出[7]。数据处理环节全部使用隐私计算技术，用联邦学习、差分隐私、同态加密等技术在不泄露原始数据的情况下进行多源数据的协同计算，从根本上解决数据融合泄露问题。数据销毁环节开发出分布式数据批量擦除工具，对所有的云节点以及物理介质上的数据副本实施彻底的擦除工作，并且还要借助第三方来检验数据是否可以被恢复。

（二）升级大数据原生安全技术体系

抛弃传统的边界防护技术，创建出适合于大数据架构的原生安全技术体系。一是部署大数据流量智能分析平台，用深度学习算法学习正常的海量数据访问、流转模式，精准识别出异常批量下载、跨域非法传输、数据投毒等攻击行为，实现秒级预警[8]。二是创建数据安全中台，把数据分类分级、全链路溯源、访问控制、审计日志等各方面功能集成起来，从而达到对整个数据统一管理的目的。利用数据水印技术给每一项数据加上唯一的标识，从而达到对数据泄露进行精确追踪的目的。三是加强大数据框架的安全加固，对 Hadoop、Spark、Flink 等主流的框架做安全配置工作，关闭不需要的端口和服务，开启 Kerberos 认证以及 Apache Ranger 权限管理，并且修补已有的漏洞。四是创建云边端协同防护体系，边缘节点上装轻量级安全探针，完成边缘数据的实时检测和防护，在云端搭建统一安全管理平台，达成云边端安全策略的同步和联动。五是严格按照网络安全等级保护和商用密码应用安全性评估的要求执行。按照网络安全等级保护条例和大数据平台等级保护 2.0 扩展要求，完成三级及以上大数据平台定级备案、建设整改、等级测评工作，主要加强数据安全计算环境、区域边界、通信网络安全防护。同步开展商用密码应用安全性评估（密评），对数据采集、传输、存储、处理全过程进行国密 SM2/SM3/SM4 算法的合规使用，保证大数据平台符合国家密码管理强制性要求。

（三）完善精细化大数据安全治理体系

就海量数据治理难题而言，创建起“技术加管理”的精细治理体系。一是用自动化数据分类分级的方法，用大模型技术来识别和分类大量的异构数据，准确率大于 90%，可以准确地识别出

 Copyright © This Work is Licensed under A Commons Attribution-Non Commercial 4.0 International License.

敏感数据并加以保护[9]。二是创建全链路数据流转审计机制，把数据从采集到销毁的每一个操作都完整地记录下来，即访问人员、操作时间、数据内容、流转路径等都要被完整地记录下来，从而达到“谁访问、谁操作、谁负责”的目的。三是加强内部人员管理，关闭普通员工的批量数据导出权限，核心数据批量调取必须经过两人审核并有全程录像；建立员工行为基线，对于异常的操作行为及时发出预警。三是开展常态化的大数据安全专项演练，模拟出大量的数据、大批量泄露、集群勒索攻击、供应链污染等真实的事故场景来提升运维人员的应急处置能力。

（四）强化合规建设与复合型人才培养

严格依照法律法规的要求来补齐合规建设管理和人才的不足。一是参照《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《关键信息基础设施安全保护条例》，制定企业大数据安全管理制度，对数据进行分类分级、跨域流转、出境安全评估等过程做出规定；把等级保护测评、密评结果当作合规审计的主要内容之一，定时展开专项合规审计，及时整改隐患[10]。二是创建多层次的人才培养体系。高校开设大数据安全相关专业，培养基础人才；企业同高校、安全厂商联合创建实训基地，培育实战型人才；实施在职人员专项培训，改善现有的运维人员大数据安全技能。三是发挥政府引导作用，创建大数据安全公共服务平台，给中小企业提供漏洞扫描、风险评估等服务，完善大数据安全标准体系，规范行业安全建设。

三、结语

大数据安全是数字化转型的底线，没有大数据安全，就没有数字经济的健康发展。大数据安全同传统的网络安全不同，它的主要矛盾就是海量多源数据的开放共享和安全防护能力不足之间的矛盾。传统的边界式防护已经不能应对系统性的风险了，必须改变安全的理念，由原来的“网络边界防护”转变为现在的“数据本身防护”，建立覆盖全生命周期的原生安全体系。随着大模型、量子计算等技术的发展，大数据安全也会出现新的问题。需要不断追踪技术发展动向，促使技术同管理以及合规深度整合起来，塑造起一个动态且全面覆盖、具备智能属性的大数据安全防护体系，从而让数据得以在安全的框架内自由流通，进而发挥出它所具有的巨大经济与社会潜力，为数字中国的创建筑牢根基。

参考文献

[1] 马志航 . 大数据时代下的计算机网络安全技术探析 [J]. 软件 ,2025,46(11):167-169.

[2] 王希喆 . 大数据云计算下网络安全技术实现的策略分析 [J]. 软件 ,2025,46(11):175-177.

[3] 李佳琦 . 网络安全态势感知技术提升企业可持续风险防控能力研究 [J]. 中国宽带 ,2025,21(12):91-93.

[4] 李成喜 . 数字化背景下提升网络安全建设的策略分析 [J]. 数字化传播 ,2025,(11):56-58.

[5] 胡红玲 . 大数据技术在计算机网络系统中的应用 [J]. 信息记录材料 ,2025,26(11):156-158.

[6] 齐菲 . 基于大数据分析的网络系统安全风险评估技术 [J]. 信息记录材料 ,2025,26(11):171-173.

[7] 李慧娟 . 大数据与人工智能技术融合系统在网络安全防御中的应用研究 [J]. 科技资讯 ,2025,23(20):52-54.

[8] 程荣森 , 赵鹏泽 . 大数据技术在网络安全风险检测中的运用研究 [J]. 科技资讯 ,2025,23(17):41-43.

[9] 赵浩达 . 基于大数据的计算机信息技术在网络安全中的应用 [J]. 流体测量与控制 ,2025,6(4):103-105.

[10] 李浒 , 王治国 , 张蓓 . 复合 CNN 下数据网络安全态势数字化感知方法 [J]. 电子设计工程 ,2025,33(7):150-154.

Copyright © This Work is Licensed under A Commons Attribution-Non Commercial 4.0 International License.