ISSN: 2705- 1021 （P） 2661-4820 （O）

面向数字化转型的信息安全与数据安全保障机制研究

王鹏杰

中国电力科学研究院有限公司　北京　100192

摘　要：数字化转型作为社会发展的必然趋势，通过数据驱动、智能化、网络化和平台化等特征深刻影响各行业，但也带来了信息安全与数据安全的严峻挑战。本文旨在研究面向数字化转型的信息安全与数据安全保障机制，分析当前安全现状，构建涵盖技术层、管理层和法律层的多层次保障框架，并结合实际案例提出具体实施建议。研究发现，现有安全保障机制存在技术防护单一、管理机制不完善、法律法规滞后等问题，亟需构建协同防御体系。通过技术手段、管理策略和法律支撑的有机结合，形成全方位的安全保障机制，以应对复杂多变的网络安全威胁，确保数字化转型顺利进行。

关键词：数字化转型；信息安全；数据安全；保障机制；协同防御

引言

数字化转型已成为当今社会发展的必然趋势，其背景在于信息通信技术的迅猛发展和全球经济的高度融合。数字化转型通过数据驱动、智能化、网络化和平台化等特征，深刻改变各行业的业务模式和价值链。制造业通过智能制造提升效率，服务业借助数字化工具优化体验，金融业利用大数据增强风险管理，教育业则通过在线平台拓展教学边界。然而，数字化转型也带来了信息安全与数据安全的严峻挑战，如数据泄露风险增加、网络攻击手段复杂化和内部威胁加剧等。

在此背景下，构建完善的信息安全与数据安全保障机制显得尤为必要。这不仅关乎企业的生存与发展，更影响到社会的稳定和国家安全。本文旨在深入研究数字化转型过程中信息安全与数据安全保障的机制，探讨其面临的挑战和应对策略。研究内容包括分析当前信息安全与数据安全的现状，构建多层次、全方位的安全保障框架，并结合实际案例提出具体实施建议。

通过本研究，期望为企业在数字化转型过程中提供科学有效的安全保障方案，推动信息安全与数据安全领域的理论发展和实践应用。

1 数字化转型概述

数字化转型是指利用数字技术和信息通信技术，对传统业务模式、运营流程和价值链进行系统性改造的过程。其主要特征包括数据驱动、智能化、网络化和平台化。数据驱动强调数据在决策中的核心地位，智能化体现为人工智能和机器学习的广泛应用，网络化则指万物互联的态势，平台化则表现为多边市场的构建。

数字化转型对各行业产生了深远影响。制造业通过智能制造提升生产效率，服务业借助数字化工具优化客户体验，金融业利用大数据和区块链技术增强风险管理能力，教育行业则通过在线教育平台拓展教学边界。图 1 展示了数字化转型对各行业影响的示意图，从中可以看出，不同行业受数字化转型的影响程度存在显著差异。

然而，数字化转型也带来了信息安全与数据安全的严峻挑战。首先，数据泄露风险增加。随着数据量的激增和流动性的增强，数据泄露的可能性也随之上升。其次，网络攻击手段日益复杂。黑客利用先进的攻击技术，如勒索软件、钓鱼攻击等，对企业信息系统构成威胁。再次，内部威胁不容忽视。员工误操作或恶意行为可能导致敏感数据外泄。此外，法律法规滞后于技术发展，导致数据安全保障机制不健全。

在应对这些挑战时，构建完善的信息安全与数据安全保障机制至关重要。首先，应加强数据加密技术，确保数据在传输和存储过程中的安全性。其次，建立多层次的安全防护体系，包括防火墙、入侵检测系统和安全审计等。再次，提升员工安全意识，定期开展安全培训和演练。最后，完善法律法规，明确数据安全责任，强化监管力度。

综上所述，数字化转型在推动各行业发展的同时，也带来了信息安全与数据安全的挑战。构建科学有效的安全保障机制，是确保数字化转型顺利进行的关键。

2 信息安全与数据安全现状分析

当前，信息安全与数据安全已成为数字化转型过程中不可忽视的重要议题。随着数字技术的广泛应用，数据泄露和网络攻击事件频发，给企业和个人带来了巨大风险。据统计，近年来全球范围内的数据泄露事件数量呈上升趋势，涉及金融、医疗、教育等多个领域。表 1 展示了近年重大数据泄露事件的统计情况，从中可以看出，数据泄露事件的规模和影响范围不断扩大。

表 1 近年重大数据泄露事件的统计情况

年份	事件名称	影响用户数（万人）	行业领域
2020	某金融公司数据泄露	500	金融
2021	某医疗平台数据泄露	300	医疗
2022	某教育机构数据泄露	400	教育

常见的网络安全威胁主要包括勒索软件攻击、钓鱼攻击、DDoS 攻击等。勒索软件通过加密用户数据，迫使受害者支付赎金，造成严重的经济损失。钓鱼攻击则通过伪装成合法机构，诱骗用户泄露敏感信息。DDoS 攻击通过大量请求瘫痪目标服务器，影响业务的正常运行。这些攻击手段不断演进，使得传统安全防护措施难以应对。

现有安全保障机制在应对复杂多变的网络安全威胁时，暴露出诸多不足。首先，技术防护手段单一，缺乏多层次、全方位的安全防护体系。许多企业仅依赖防火墙和杀毒软件，难以抵御高级持续性威胁（APT）。其次，安全管理机制不完善，内部威胁防范不足。员工安全意识薄弱，误操作或恶意行为导致数据泄露的风险较高。再次，法律法规滞后于技术发展，数据安全责任不明确，监管力度不足。

此外，数据流动性和共享性的增强，也增加了数据泄露的风险。在数字化转型过程中，数据在不同系统和平台间频繁流动，任何一个环节的薄弱都可能成为攻击的突破口。

综上所述，当前信息安全与数据安全面临严峻挑战，现有安全保障机制存在明显不足。需构建更加科学、完善的安全保障机制，以应对数字化转型带来的新风险。

3 信息安全与数据安全保障机制构建

在数字化转型背景下，构建全面、高效的信息安全与数据安全保障机制至关重要。本文提出一个多层次的保障机制框架，涵盖技术层、管理层和法律层，旨在形成协同防御体系。

首先，技术层是保障机制的基础，主要包括数据加密、访问控制等技术手段。数据加密技术通过将敏感信息转换为密文，防止未经授权的访问。访问控制技术则通过身份认证和权限管理，确保只有合法用户能够访问特定资源。这些技术手段相互补充，共同构建起多层次的技术防护体系。

其次，管理层是保障机制的核心，涉及安全策略制定、风险评估、应急响应和人员培训等方面。安全策略制定需结合实际情况，明确安全目标和具体措施。风险评估则通过定期识别评估潜在风险，制定针对防范措施。应急响应机制包括事件发现、报告、处置和恢复等环节，确保在发生时能够迅速响应，最小化损失。人员培训通过提高员工安全意识和技能，降低内部威胁。管理层通过系统化的管理流程，确保各项安全措施的有效落实。

再次，法律层为保障机制提供法律支撑，包括法律法规的制定与执行、数据隐私保护、安全责任追究等内容。法律法规的制定需与时俱进，明确数据安全责任和义务。数据隐私保护则通过立法保障个人数据的安全和隐私权。安全责任追究机制通过对违法行为的惩处，起到震慑作用。法律层通过完善的法律体系，为信息安全与数据安全提供坚实的法律保障。

各组成部分之间是相互协同，形成有机整体。技术层为管理层和法律层提供技术支撑，确保各项措施得以有效实施。管理层通过制定和执行安全策略，促进技术手段和法律规定的落实。法律层则为技术层和管理层提供法律依据，确保各项活动的合法合规。三者相互依存，共同构建起面向数字化转型的信息安全与数据安全保障机制。

通过上述分析，可以看出，面向数字化转型的信息安全与数据安全保障机制需综合考虑技术、管理和法律等多方面因素，形成协同防御体系，方能有效应对复杂多变的网络安全威胁，确保数字化转型顺利进行。

4 案例分析

在数字化转型过程中，企业如何有效实施信息安全与数据安全保障机制，成为业界关注的焦点。以某知名金融科技企业为例，该企业在数字化转型中采取了多层次的安全保障措施，取得了显著成效。首先，在技术层面，该企业部署了先进的数据加密技术，确保敏感信息在传输和存储过程中的安全性。同时，通过严格的访问控制机制，实现了对用户身份的精准认证和权限的精细化管理，有效防止了未经授权的访问。此外，入侵检测系统和态势感知技术的应用，使其

能够实时监测网络环境，及时发现并应对潜在威胁。

在管理层面上，该企业制定了全面的安全策略，涵盖数据管理、系统维护和应急响应等多个方面。通过定期的风险评估，及时识别和化解潜在风险，确保系统的稳定运行。此外，企业高度重视人员培训，通过定期举办安全意识和技能培训，提升了员工的整体安全素养。

在法律层面，该企业严格遵守相关法律法规，确保数据处理的合法合规。通过建立健全的数据隐私保护机制，保障了用户数据的隐私安全。同时，明确的安全责任追究制度，对内部违规行为进行了有效震慑。

通过上述措施，该企业在数字化转型中实现了信息安全与数据安全的双重保障，提升了企业的整体竞争力和市场信任度。其成功经验表明，构建多层次、全方位的安全保障机制，是企业在数字化转型中确保信息安全与数据安全的关键。

5 保障机制实施建议

在数字化转型背景下，企业实施信息安全与数据安全保障机制的具体建议尤为重要。首先，技术层面应采用先进的数据加密技术，确保敏感信息在传输和存储过程中的安全。同时，严格的访问控制机制和实时的入侵检测系统是不可或缺的，前者通过精准认证和权限管理防止未授权访问，后者则能及时发现并应对潜在威胁。

在管理层面，企业需制定全面的安全策略，涵盖数据管理、系统维护和应急响应等多个方面。定期的风险评估有助于及时识别和化解潜在风险，而高效的应急响应机制则能在安全事件发生时迅速启动应急预案，最大限度减少损失。

对于不同规模和类型的企业，上述措施需根据实际情况进行调整。大型企业可建立更为复杂的安全体系，而中小型企业则应侧重于成本效益较高的解决方案。政策支持在此过程中扮演关键角色，政府应出台相关法规和政策，为企业提供指导和资源支持。

人才培养同样至关重要。企业应定期举办安全意识和技能培训，提升员工的安全素养。高校和研究机构也应加强信息安全相关专业的建设，培养专业人才，为企业提供持续的人才支持。

综上所述，构建多层次、全方位的安全保障机制，结合政策支持和人才培养，是企业在数字化转型中确保信息安全与数据安全的关键路径。

6 结论与展望

本研究深入探讨了数字化转型过程中信息安全与数据安全保障机制的构建，分析了当前安全现状及面临的挑战，并提出了多层次、全方位的保障框架。未来研究可进一步探索新兴技术在安全保障中的应用。同时，需关注法律法规的完善与国际化接轨，强化跨行业、跨地域的安全协作机制。此外，加强安全文化建设，提升全民安全意识，亦是未来研究的重要方向。通过持续的理论创新与实践探索，有望构建更加坚实的信息安全与数据安全保障体系，助力数字化转型稳健发展。

参考文献：

[1] 陈鹏 , 何英强 . 数字化转型、动态能力和企业双元创新 [J]. 湖北科技学院学报 ,2025,45(04):32-41.

[2] 闫严 . 云电脑平台数据传输的信息安全保护技术研究 [J]. 产业创新研究 ,2025(12):91-93.

[3] 赵丽莉 , 王鹏 . 公共数据开放中企业数据安全风险及其治理研究 [J/OL]. 重庆邮电大学学报 (社会科学版),1-17[2025-07-09].http://kns.cnki.net/kcms/detail/50.1180.c.20250630.1437.004.html.

[4] 马嘉良 . 大数据助力建工多媒体通信的通信安全保障机制研究 [J]. 中国宽带 ,2025,21(08):49-51.

[5] 裴辰晔 . 电力系统网络安全中的多层协同防御模型分析 [J]. 电子技术 ,2024,53(12):240-241.

作者简介：王鹏杰（1993—），男，汉，山西朔州，中国电力科学研究院有限公司，大学专科，无，网络安全。