电子信息技术在安全保障中的应用研究

朱瑞贺
（成武县应急管理保障和技术服务中心，山东省菏泽市成武县，274299）

摘要　为探明电子信息技术在安全保障中的应用方向，本文以电子信息技术的应用为主线，聚焦其在智能监控、身份认证、数据保护、应急指挥等关键场景的落地实践，系统剖析电子信息技术赋能安全管理的逻辑路径与内在机理，旨在为企业的安全管理、矿山或制造企业的安全生产提供安全保障，减少安全事故的发生。

关键词　电子信息技术；安全保障；应急响应

中图分类号：TP309　文献标识码：B
文章编号：1008-0899(2025)06-0074-02

在数字化浪潮席卷全球的今天，安全问题已从传统的物理边界防御演变为跨空间、跨维度的复杂挑战。无论是城市运行、工业生产，还是个人隐私、社会秩序，安全保障的需求正随着技术革新与风险形态的演变而急剧升级。电子信息技术作为现代社会的“神经系统”，凭借其智能化、网络化与数据驱动的核心特性，正深刻重构安全管理的逻辑与范式，从被动响应转向主动防御，从经验决策迈向精准预判，从孤立管控进化为全域协同[1]。因此，从智能监控与预警系统、身份认证与访问控制、数据安全与隐私保护和应急响应与指挥调度等方面对电子信息技术的应用进行总结和分析，对保障企业安全具有重要的作用和意义。

1　智能监控与预警系统

电子信息技术在智能监控与预警系统中通过AI算法、物联网和大数据分析的深度融合，显著提升了安全管理的实时性与精准度。基于人工智能中的人脸识别和行为分析等视频监控技术可自动识别异常行为或可疑目标，实现公共场所的主动防范；物联网传感器实时采集环境数据，动态监测火灾、泄漏等隐患并及时报警；智能分析平台则通过整合历史数据与实时信息，预测设备故障或交通拥堵等潜在风险，触发预警并辅助决策[2]。这一技术体系以自动化、全天候的监控模式，大幅降低了安全事故的发生概率，同时通过数据驱动的预警机制，为快速响应和风险防控提供了科学支撑。

2　身份认证与访问控制

电子信息技术在身份认证与访问控制领域构建了智能化安全防护体系，通过多维度技术手段有效防范身份冒用、权限滥用等风险。在身份认证环节，采用生物识别技术替代传统密码认证，基于指纹、虹膜、人脸等唯一性生物特征，结合高精度传感器和AI算法实现毫秒级精准核验。金融领域应用人脸识别技术完成用户与身份证照的实时比对，确保关键操作真实性。为强化防护，多因子认证技术将生物特征与动态密码（如短信验证码）、硬件令牌等要素结合，形成多重验证机制。企业核心系统采用“指纹识别+动态口令”双重认证，即使单一验证环节失效仍能保障系统安全。在权限管理方面，基于角色的访问控制（RBAC）和属性基加密（ABE）技术实现细粒度的权限分配，结合用户行为分析建立动态调整机制，有效防范内部威胁。这些技术共同构成了从身份核验到权限管理的全链条防护体系，显著提升了物理和数字空间的安全水平[3]。

在权限管理层面，基于角色的访问控制与动态权限调整技术成为关键。角色的访问控制通过预设角色分配权限，简化了大规模用户的权限管理流程；而动态权限技术则依托实时风险评估模型，根据用户行为动态调整权限等级。例如，当检测到某员工账户在非工作时间尝试访问敏感数据时，系统可自动冻结其权限并触发告警，有效防范内部威胁。

3　数据安全与隐私保护

作者简介：朱瑞贺（1987~），男，山东成武县人，本科，助理工程师，研究方向：电子信息技术。

电子信息技术在数据安全与隐私保护领域的应用，通过技术手段与制度设计的结合，构建了覆盖数据全生命周期的防护体系，成为应对数字化时代数据泄露、滥用及隐私侵权等风险的核心支撑。

在数据安全领域，电子信息技术以加密技术为基石，结合分布式存储、入侵检测与隐私计算，形成“传输-存储-使用”全流程防护链。传输环节采用非对称与对称加密算法，确保数据在公共网络中的机密性；存储环节通过同态加密或可信执行环境实现数据“可用不可见”，例如医疗研究机构可在加密状态下分析患者数据，避免原始信息暴露。此外，区块链技术通过分布式账本与哈希链结构，为数据完整性提供保障，应用于电子合同、供应链溯源等场景，确保记录不可篡改[4]。

隐私保护层面，匿名化与脱敏技术通过模糊个体特征或添加噪声，降低数据关联风险。例如，在用户行为分析中，平台可利用差分隐私技术向数据集注入随机噪声，使统计结果无法回溯至特定个人。同时，零知识证明等密码学方案允许验证方在不获取原始数据的情况下确认其真实性。

在主动防御方面，入侵检测系统与AI驱动的威胁感知成为关键。基于机器学习的入侵检测系统可实时分析网络流量模式，识别病毒攻击、勒索软件等异常行为，并联动防火墙进行阻断。

4　应急响应与指挥调度

电子信息技术在应急响应与指挥调度中的应用，通过融合高速通信、智能分析与可视化技术，构建了从灾情感知到资源调度的全流程数字化体系，显著提升了突发事件的响应速度、决策科学性与救援协同效率。其核心在于利用5G、物联网、地理信息系统（geographic information system，GIS）及虚拟现实等技术，打通“数据采集-信息整合-指挥决策-行动执行”的闭环链路，实现对复杂应急场景的快速感知、精准研判与动态优化[5]。

4.1　技术实现

5G通信技术凭借高带宽、低延迟的特性，为无人机、智能机器人等终端设备提供了实时数据传输能力，例如在火灾现场，无人机可通过5G网络将高清影像与热力图实时回传至指挥中心，辅助救援人员快速定位火源与受困者；GIS则整合卫星遥感、道路网络与人口分布等多源数据，通过空间分析与可视化建模，动态规划最优救援路径并评估灾害影响范围，如在洪涝灾害中，GIS平台可结合实时水位数据预测淹没区域，指导人员疏散与物资投放。同时，虚拟现实与数字孪生技术通过构建高仿真应急场景，支持多部门协同演练与预案推演，例如模拟化工厂泄漏事故时，指挥人员可在虚拟环境中测试不同处置方案的效果，优化应急流程并降低实战风险[6]。

4.2　面临的挑战

当前技术应用仍面临多重挑战：①通信基础设施的覆盖与稳定性制约了极端环境下的应急响应能力，如地震导致基站损毁时，依赖传统通信网络的指挥系统可能陷入瘫痪。②多源数据融合与标准化存在瓶颈，不同部门的数据格式、更新频率差异导致信息整合效率低下，可能延误决策窗口。③技术成本与普及度不平衡，欠发达地区或中小型机构往往难以承担高端设备的部署费用，形成应急能力鸿沟。此外，智能化算法的可靠性仍需验证，例如AI对灾害趋势的预测可能因训练数据偏差而产生误判，过度依赖技术工具可能削弱人工决策的灵活性。

5　结语

电子信息技术对安全管理的重构，本质是一场关于“信任”的革命，技术既在解构传统的人工审核信任机制，也在重建区块链的可追溯性等更高维度的信任体系。这一进程中，电子技术既是风险感知的“神经末梢”，也是决策执行的“智慧大脑”，更是连接物理空间与数字空间的“韧性纽带”。

参考文献

[1]　李龙飞.电子信息技术在网络安全中的应用[J].电子技术,2024(5):266-267.

[2]　武明斐.电子信息技术在安全保障管理中的应用[J].集成电路应用,2023(4):327-329.

[3]　杨立营.浅析电子信息技术在企业安全管理中的应用[J].中外企业家,2019(34):51.

[4]　陆颖.电子信息技术在企业安全管理中的应用分析[J].无线互联科技,2019,16(14):138-139.

[5]　盛俊.电子信息技术在网络安全中的应用研究[J].网络安全技术与应用,2022(3):128-129.

[6]　王晓庆.电子信息技术在企业安全管理中的应用分析[J].中外企业家,2020,(14):80.