信息化网络安全管理和防范探讨

蔡中葳
北京市智慧水务发展研究院　北京　101117

摘　要：信息化网络安全管理面临策略规划滞后、访问控制薄弱、数据保护不足及监测响应低效等问题。防范关键技术包括动态防御与边界防护、强化型访问认证、全生命周期数据防护及高效监测响应与恢复优化技术。管理实施路径为通过精准化安全培训提升意识、构建技术与管理协同机制、建立持续改进与安全评估体系。技术与管理协同施策，可提升网络安全防护能力，保障网络系统稳定运行与数据安全，支撑信息化健康发展。

关键词：网络安全管理；安全防范；数据防护；协同机制；持续改进

引言：信息化时代，网络应用渗透至各领域，网络安全重要性凸显。网络安全管理涉及策略规划、防护技术、实施路径等多方面，各环节紧密相连。有效的网络安全管理可预防安全事件，减少损失。当前网络安全存在策略滞后、访问控制薄弱等问题，相互关联放大风险。探讨网络安全管理与防范，对提升网络安全性、保障信息资产安全、推动信息化健康发展意义关键。

1 信息化网络安全管理存在的问题

1.1 网络安全策略与规划滞后

网络安全策略与规划的滞后，是制约网络安全防护效能的基础性问题。安全目标设定未能紧密贴合网络实际应用场景的动态变化，当业务系统升级或新增时，保护范围未能及时同步调整，致使部分新兴业务长期处于安全防护的真空地带[1]。风险评估缺乏动态更新机制，仍沿用传统框架应对新型网络威胁，对于云计算、物联网等新兴应用催生的风险点识别不足，难以全面预判潜在安全隐患。安全管理体系呈现碎片化特征，各部门基于自身需求独立制定安全策略，缺乏跨部门的统一协调与联动机制，形成一个个防护孤岛，无法形成合力抵御跨区域、跨系统的网络威胁。策略调整周期冗长，难以跟上网络攻击手段快速迭代的步伐，部分安全措施在落地实施时，其防护能力已落后于实际威胁形势，导致防护效果大幅削弱。这些问题相互叠加，使得网络安全防护体系难以应对复杂多变的安全挑战。

1.2 网络访问控制与身份认证薄弱

网络访问控制环节漏洞明显，用户权限分配缺乏精细化的动态管理，普遍存在权限过度授予的现象，对于非必要的访问权限未能及时回收，这在很大程度上增加了内部信息泄露的风险。访问控制机制对异常行为的识别灵敏度不高，面对非典型的访问模式，往往响应滞后，难以有效阻止持续性的未授权操作。身份认证方式较为单一，多数情况下仍依赖密码等传统手段，且密码管理松散，弱密码、密码复用等问题屡见不鲜，使得身份被冒用的风险显著升高。多因素认证技术在关键业务系统中的覆盖率较低，生物识别等先进认证技术的应用范围有限，导致整体身份认证体系的抗攻击能力较弱，难以有效应对复杂的网络攻击。

1.3 数据安全与隐私保护不足

数据全生命周期的安全防护存在诸多短板，是当前网络安全领域的突出问题。数据存储加密的覆盖率较低，部分敏感数据仍以明文形式保存，这无疑增加了数据泄露的风险。数据传输过程中的加密机制不完善，在跨网络进行数据流转时，极易被不法分子拦截窃取。隐私保护措施落实不到位，在数据收集环节，未明确告知用户信息的具体用途，数据处理过程中也缺乏有效的脱敏手段，导致个人信息与敏感商业数据的保护边界模糊不清[2]。数据访问审计机制不健全，无法完整记录数据的操作轨迹，难以追溯异常的数据访问行为，当数据发生泄露后，很难快速定位泄露源头。加密算法更新不及时，部分系统仍在使用安全性较低的老旧算法，其抗破解能力严重不足，难以保障数据的安全。这些问题与访问控制薄弱环节相互作用，加剧了数据安全风险的扩散。

1.4 安全监测与应急响应低效

安全监测体系存在较多覆盖盲区，对终端设备、边缘计算节点等的监测力度不够，难以全面、准确地掌握网络的整体安全状态。威胁检测技术对于新型攻击手段的识别能力有限，对隐藏在正常流量中的恶意代码识别率偏低，预警往往滞后于攻击的发生时间。入侵检测系统的误报率较高，大量的无效警报干扰了安全人员对真实威胁的判断，从而降低了响应效率。应急响应流程不完善，事件确认、影响评估、遏制措施、系统恢复等环

节缺乏明确、规范的标准化步骤，当安全事件发生时，各部门之间容易出现协同不畅、应对混乱的情况，延误了最佳的处置时机。系统恢复机制不健全，数据备份策略执行不到位，部分关键数据的备份不及时，或者备份介质的安全性不足，这在很大程度上影响了安全事件发生后的快速恢复能力，可能导致业务中断时间延长。这类问题的存在，使得前期安全防护措施的效果难以充分发挥。

2 信息化网络安全问题的防范关键技术

2.1 动态防御与边界防护技术

针对网络安全策略与规划滞后问题，动态防御技术可实现安全策略的实时适配。通过构建弹性安全架构，将网络安全策略与业务系统升级同步联动，当新增业务上线时，自动扩展防护范围并调整策略参数，消除安全防护真空地带[3]。采用智能化风险评估引擎，整合云计算、物联网等新兴应用的威胁特征库，动态更新风险评估维度，精准识别新型风险点。建立跨部门的安全策略协同平台，打破防护孤岛，实现安全策略的集中管控与统一调度，确保各部门防护措施形成合力。引入威胁情报共享机制，缩短策略调整周期，使安全措施能快速匹配攻击手段的迭代速度，通过实时推送的威胁情报，自动优化防护规则，提升防护时效性。动态防御系统还可通过模拟攻击演练，持续检验策略有效性，在业务场景变化前提前预置防护规则，避免因策略滞后产生新的安全漏洞。其与后续访问控制技术形成联动，为权限管理提供基础安全环境。

2.2 访问控制与身份认证强化技术

为解决网络访问控制与身份认证薄弱问题，采用基于角色的动态权限管理技术，根据用户实时业务需求自动分配最小必要权限，并定期扫描权限冗余，及时回收非必要访问权限，从源头降低内部信息泄露风险。部署行为基线分析系统，建立用户访问行为模型，对偏离基线的非典型访问模式实时预警并自动拦截，提升异常行为识别的灵敏度。构建多因素认证体系，在密码基础上融合生物识别、硬件令牌等技术，针对关键业务系统强制启用多因素认证，通过密码强度检测工具杜绝弱密码、密码复用现象。推广无密码认证技术，利用生物特征或设备指纹替代传统密码，进一步提升身份认证的抗攻击能力，确保身份信息不被冒用[4]。访问控制技术还可与业务流程深度绑定，根据业务节点自动切换权限等级，在完成特定操作后即时收回临时权限，形成动态闭环管控。该技术承接动态防御的安全环境，为数据防护筑牢访问防线。

2.3 数据全生命周期安全防护技术

针对数据安全与隐私保护不足的问题，构建数据全生命周期加密体系，在数据存储环节采用透明加密技术，实现敏感数据自动加密存储；传输过程中部署量子密钥分发或TLS1.3等高强度加密协议，防止数据在跨网络流转时被拦截窃取。建立隐私保护合规管理平台，在数据收集阶段明确告知用户信息用途并获取授权，处理过程中自动应用数据脱敏技术，根据数据类型动态调整脱敏规则，清晰界定个人信息与敏感商业数据的保护边界。部署数据操作审计系统，全程记录数据访问、修改、删除等操作轨迹，通过区块链技术确保审计日志不可篡改，当发生数据泄露时，可快速追溯操作源头。建立加密算法动态升级机制，定期评估算法安全性，自动替换老旧算法，引入AES-256、RSA-2048等高强度加密标准，提升数据抗破解能力。数据防护技术还可根据数据敏感度动态调整保护强度，对核心数据实施多重加密与访问隔离，确保高价值信息资产的绝对安全。此技术依托访问控制的权限管理，为监测响应提供数据安全基础。

2.4 监测响应与恢复优化技术

为提升安全监测与应急响应效率，构建全维度监测网络，覆盖终端设备、边缘计算节点及云端资源，通过轻量级探针实时采集全网安全数据，实现安全状态的全面感知[5]。采用机器学习驱动的威胁检测引擎，深度分析正常流量中的隐藏恶意代码，结合沙箱动态行为分析技术，提升新型攻击手段的识别率，缩短预警滞后时间。优化入侵检测系统的智能降噪算法，通过关联分析过滤无效警报，将误报率控制在合理范围，使安全人员聚焦真实威胁。制定标准化应急响应流程，明确事件确认、影响评估、遏制措施、系统恢复等环节的操作规范，建立跨部门协同响应机制，通过应急指挥平台实现各部门的实时联动与高效协作。构建智能数据备份与恢复系统，采用增量备份结合异地容灾技术，确保关键数据备份的及时性与安全性，通过自动化恢复脚本，缩短安全事件后的业务中断时间。监测响应技术衔接数据防护的安全状态，形成完整的技术防护闭环。

3 信息化网络安全问题的管理实施路径

3.1 安全培训与意识提升

结合网络安全管理存在的问题，安全培训需针对性强化人员对动态权限管理、多因素认证等技术的理解，重点培训钓鱼邮件识别中与身份冒用相关的特征，以及数据加密存储的基本操作规范，帮助人员掌握防范权限滥用与数据泄露的具体方法。培训形式增加沉浸式模拟

演练，还原权限过度授予导致的信息泄露、弱密码被破解等真实场景，让人员实践中熟悉应急处理流程，提升应对实际威胁的能力。在安全文化培养中，突出最小权限原则动态认证等核心理念，通过案例宣传展示访问控制失效、数据保护不足引发的安全事件，强化人员对关键安全环节的重视，推动人员主动报告权限异常、数据泄露等隐患，形成全员参与的安全防护氛围。培训内容需随网络安全形势更新，纳入新兴威胁的识别方法，确保人员掌握的防护技能与实际需求相符[6]。这种培训模式能为技术与管理协同奠定认知基础，让人员理解协同机制的必要性。培训过程中可结合实际发生的安全事件案例，让人员直观感受安全管理各环节的关联性。

3.2 技术与管理协同机制

针对各环节安全问题，建立技术落地与管理制度的双向映射机制，将动态防御、权限管理等技术要求转化为可执行的管理规范，明确技术参数的管理阈值，例如权限审计的频率、数据加密强度的标准等，确保技术措施按预期发挥作用。技术部署前需通过安全管理委员会审核，重点评估技术对访问控制、数据保护等问题的解决能力；技术运行中自动生成管理报表，为权限优化、加密策略调整等管理决策提供数据支撑。打破部门壁垒，由安全部门牵头建立技术-管理-业务协同工作组，定期召开安全态势分析会，共享权限异常日志、数据泄露预警等信息，针对访问控制薄弱、数据防护不足等问题制定联合整改方案，确保技术优化与管理改进同步推进，形成闭环管理。通过规范的协同流程，让技术应用与管理要求深度融合，覆盖网络安全的各个环节。该机制承接安全培训的认知成果，为持续改进提供实施框架。协同过程中需注重各部门职责的清晰划分，确保每个环节都有明确的责任主体。

3.3 持续改进与安全评估

为解决各类安全问题的长效改进，构建常态化安全评估体系，定期开展渗透测试模拟新型攻击手段，验证动态防御、访问控制等技术的有效性；通过配置审计工具全面检查安全策略与权限配置，找出管理流程中的漏洞。采用漏洞扫描与威胁狩猎相结合的方式，重点检测权限管理系统、数据加密模块等关键环节的薄弱点，优先修复可能导致信息泄露、身份冒用的高危漏洞[7]。安全评估报告需量化分析当前安全状态与目标的差距，例如权限冗余率、数据加密覆盖率等指标，明确改进优先级。建立安全策略动态优化机制，根据评估结果调整动态防御规则、权限分配模型及数据加密策略，结合网络环境变化实时更新防护措施，确保安全管理始终适配业务发展与威胁演变，形成持续改进的良性循环。通过定期评估与及时调整，让安全管理措施不断完善，应对网络安全的各类挑战。这种持续改进模式依托技术与管理协同的成果，反哺安全培训内容的更新迭代。评估结果需及时反馈至相关部门，作为下一阶段工作调整的重要依据。

结束语

信息化网络安全管理和防范是长期且复杂的系统工程。从管理内容、防护技术到实施路径，各环节紧密相连。动态防御、访问控制强化等技术，结合培训提升、协同机制构建等路径，形成防护体系。面对变化的网络安全形势，持续探索创新，融合先进理念、技术与管理实践，构建动态、智能、高效的防护网，可保障信息化发展稳定前行。

参考文献

[1]董雅,卢金垌.计算机信息化管理发展与网络安全防范措施[J].电脑采购,2023(15):23-25.

[2]郝付东.市政工程经济管理信息化存在的风险及防范措施分析探讨[J].文渊（高中版）,2023(11):649-651.

[3]王彦霖,孙骞.信息管理技术在网络安全中的应用研究[J].中国公共安全,2024(11):157-159.

[4]黄华莲.大数据时代建筑企业会计信息化管理的存在问题和对策研究[J].发展改革理论与实践,2023,39(23):88-90.

[5]杨豫.网络安全威胁和网络监管对策探讨[J].科技视界,2023(5):113-116.

[6]鲁慧菊.信息化网络安全管理及防范对策研究[J].中国科技纵横,2023(15):74-76.

[7]任建档,胡青.谈金融企业会计信息化网络安全风险的防范[J].中国商界(下半月),2009,(10):159.