电子信息系统安全管理与保障措施

吴晓莹　侯晓林
中电伟恒（北京）科技发展有限公司天津分公司　天津　300308

摘　要：本文围绕电子信息系统安全管理与保障措施展开系统论述。首先，明确了电子信息系统安全以完整性、保密性、可用性为核心目标，阐述了其涵盖硬件、软件、数据、网络、人员的综合性安全体系特征。其次，从硬件设备安全隐患、软件与数据安全风险、人员操作与管理漏洞三个角度，分析了当前电子信息系统面临的主要安全威胁。在此基础上，提出了分级权限管理、日常运维制度完善、人员安全培训三项管理体系构建方案，以及硬件设备保障、软件与数据保障、网络与应急防护三项核心保障措施，为电子信息系统安全管理提供了系统性的技术路径与实施依据。

关键词：电子信息系统；系统安全；安全管理；措施

引言：电子信息系统已广泛应用于通信、工业控制、智能制造、医疗电子等领域，系统安全直接关系到数据资产保护与业务连续性保障。当前，电子信息系统面临的安全威胁日趋复杂化，硬件设备老化、软件漏洞频发、数据泄露风险突出、人员操作不规范等问题交织叠加，传统单一的安全防护手段已难以满足实际需求。构建覆盖硬件、软件、数据、网络、人员全要素的安全管理与保障体系，成为电子信息工程领域的迫切需求。本文围绕电子信息系统安全核心目标，系统梳理主要安全风险与隐患，提出安全管理体系构建方案及具体保障措施，为电子信息系统安全运行提供系统性参考。

1 电子信息系统安全核心概述

电子信息系统安全的核心目标是保障系统硬件设备、软件程序、网络通道及存储数据在运行全过程中的完整性、保密性与可用性，确保系统在常规运行状态及突发异常状态下，均能稳定开展数据处理、传输、存储与业务交互工作。电子信息系统安全的范畴区别于单一的设备维护或局部的故障排除，是一项涵盖硬件设备防护、软件程序安全、数据资源管控、网络环境监测、人员操作规范及运维管理制度的综合性安全体系，涉及系统运行的各个技术层面与管理环节[1]。

完整性是指系统中的数据与程序不被非法篡改、恶意损坏或意外丢失，各项数据记录保持真实有效，系统程序完整无缺失，确保数据处理结果与业务逻辑的一致性与可靠性。保密性是指核心数据、内部信息及敏感资源仅对经授权的用户与终端开放，严格杜绝非授权访问、非法窃取及信息泄露等安全事件的发生，保障信息资产在传输与存储各环节的安全可控。可用性是指系统能够随时响应正常的操作需求与业务指令，不会因硬件故障、网络攻击、软件漏洞等问题出现系统瘫痪、服务中断、响应卡顿或无法访问等情况，保障业务连续性与服务稳定性。

完整性、保密性与可用性三者相互关联、相辅相成，共同构成电子信息系统安全的核心评价标准，也是电子信息系统安全管理与保障工作的核心目标与实施依据。任何一方面的缺失均会导致系统安全体系出现重大漏洞，影响电子信息系统的整体运行效能与数据资产安全。

2 电子信息系统主要安全风险与隐患

2.1 硬件设备安全隐患

硬件设备是电子信息系统运行的物理基础，其运行状态直接决定系统的稳定性与可靠性。设备老化、选型不当、运维不到位、运行环境不适配等问题，均会引发不同程度的安全故障。（1）服务器、交换机、存储设备、终端电脑等核心硬件设备长期处于高负荷不间断运行状态，会出现硬件老化、性能衰减、零部件损耗等问题，极易导致设备死机、异常断电、数据读取失败等故障，直接造成系统运行中断与业务服务停滞。（2）部分设备部署环境不符合技术运行要求，机房温湿度控制失衡、防尘防潮措施缺失、线缆布局杂乱、供电系统不稳定，会加速硬件损坏进程，同时容易引发电路短路、设备过热等安全问题。此外，硬件设备缺乏定期检测与维护保养，闲置设备与老旧设备未及时更替，设备接口与线路存在破损、接触不良等隐患，均会成为电子信息系统安全运行的薄弱环节，增加系统故障发生概率[2]。

2.2 软件与数据安全风险

软件程序和数据资源是电子信息系统的核心价值载体，也是安全风险的高发区域。（1）在软件层面，系统自带程序、第三方应用软件存在开发漏洞、版本老旧、兼容冲突等问题，部分软件长期未更新补丁，存在大量可被利用的安全漏洞，极易被恶意程序入侵、植入木马

病毒，导致程序篡改、系统失控。（2）日常使用中随意安装非正规软件、卸载系统核心程序、修改软件配置，也会造成软件运行异常、系统崩溃。在数据层面，风险主要集中在数据丢失、篡改和泄露三个方面。（3）数据存储未做好备份、存储设备故障、系统突发故障，会导致重要数据永久丢失；用户非授权操作、恶意篡改、病毒入侵，会造成数据失真、数据错乱，影响业务判定和数据使用；同时，数据传输过程未做加密处理、数据共享权限管控不严，会导致核心数据被非法窃取、外泄，造成数据资源损失。

2.3 人员操作与管理漏洞

人员操作不规范、管理机制不完善是引发电子信息系统安全问题的主要人为因素。（1）多数系统安全问题源于日常操作失误，操作人员安全意识薄弱，存在弱密码使用、密码随意泄露、离岗未锁屏、随意接入外接设备等不规范行为，大幅提升了系统被入侵、数据泄露的风险。同时，部分操作人员对系统功能、操作规范掌握不熟练，误操作核心程序、随意修改系统参数，会直接导致系统故障、数据损坏。（2）在管理层面，普遍存在权限管理混乱、岗位职责不清晰、运维记录不完整等问题。系统用户权限未按需分配，存在超权限操作、多人共用同一账号的情况，无法精准追溯操作记录；缺乏常态化的安全巡检、运维核查机制，各类潜在漏洞无法及时发现；运维工作无完整台账，故障处理、设备维护、系统更新无记录留存，出现安全问题后无法快速定位原因、开展溯源整改。

3 电子信息系统安全管理体系构建

3.1 建立分级权限管理机制

针对系统账号权限混乱、非授权操作频发等突出问题，需建立精细化的分级权限管理机制，实现权责对应、权限可控。按照岗位职能与工作需求对系统操作权限进行分级划分，设置超级管理员、运维管理员、普通操作人员等不同权限层级，严格遵循"最小权限原则"，仅为用户分配其岗位所需的最低操作权限，从制度层面杜绝超权限访问与越权操作行为。在账号管理方面，应规范账号使用标准，严格实行一人一号、专属专用制度，禁止账号共用、转借行为，定期梳理闲置账号与冗余账号并及时注销清理，消除账号管理盲区。同时，强制设置高强度账号密码，要求密码包含大小写字母、数字及特殊字符，定期更新密码，开启账号登录保护与异常登录提醒功能，对异地登录、频繁登录失败、非常规时段访问等异常行为进行实时预警与自动拦截，从源头管控人为操作风险，保障系统访问安全可控[3]。

3.2 完善日常运维管理制度

构建常态化、标准化的日常运维管理机制，规范系统运维全流程工作标准，规避运维漏洞。明确日常运维岗位职责，细化设备巡检、系统监测、漏洞排查、故障处理、数据备份等各项工作的操作流程和工作频次，确保运维工作有据可依、有序开展。建立每日巡检、每周排查、每月复盘的运维机制，每日监测系统运行状态、设备运行参数、网络传输情况，每周排查系统漏洞、软件隐患、线路故障，每月对系统运行数据、故障案例进行汇总复盘。同时，建立完整的运维台账管理制度，对设备维护、系统更新、漏洞修复、故障处理、权限调整等所有操作进行详细记录，留存操作时间、操作人员、操作内容、处理结果等信息，实现运维工作全程可追溯，提升运维管理的规范性和严谨性。

3.3 强化人员安全管控与培训

人员安全意识和操作能力是电子信息系统安全管理的核心要素，需常态化开展安全管控与技能培训，全面降低人为因素导致的系统安全风险。定期组织全员开展电子信息系统安全专项培训，培训内容涵盖规范操作流程、安全风险识别方法、病毒防范技术、数据保密要求及应急基础操作等模块，系统提升操作人员的安全防范意识与规范操作能力，从源头杜绝因操作失误引发的安全事件。同时，建立健全人员操作约束机制，明确系统操作禁忌事项与安全责任归属，将系统安全责任逐项落实到具体岗位与个人，强化全员安全责任意识。针对运维人员开展专项技能提升培训，重点围绕漏洞排查、故障处置、系统优化等专业方向，提升其快速响应与精准处理各类系统异常问题的能力，确保在突发安全事件中能够及时、有效地完成应急处置，筑牢人员安全防线。

4 电子信息系统安全保障措施

4.1 硬件设备安全保障

硬件设备安全保障需落实全周期防护策略，从运行环境优化、维护机制建设、物理隔离防护三个层面保障物理设备的稳定运行。（1）优化设备运行环境是硬件安全的基础环节。应规范机房与设备间的环境管理标准，严格调控温湿度参数至适宜范围，落实防尘、防潮、防静电、防电磁干扰措施，整理线缆布局并规范走线，杜绝线路老化、短路、挤压等安全隐患。同时配备不间断供电设备与稳压装置，避免断电、电压波动对系统运行造成影响。（2）建立硬件设备定期检测维护机制是保障设备持续稳定运行的关键措施。应定期对服务器、交换机、终端设备、存储设备进行全面检测，清理设备积尘、检测零部件运行状态、排查线路连接故障，及时更

换老化、损坏及性能不足的硬件设备，避免因设备故障引发系统安全问题。（3）做好硬件设备防护隔离是物理安全的重要保障。核心服务器、存储设备应单独部署于专用区域，避免与普通终端设备混用，定期检查设备接口安全状态，关闭闲置无用接口，防止外部设备非法接入，从物理层面构建硬件设备安全防线[4]。

4.2 软件与数据安全保障

软件与数据安全保障需从软件防护和数据保护两个维度全方位强化，杜绝软件漏洞利用与数据安全事件的发生。（1）在软件防护方面，应定期对操作系统、应用软件进行更新升级，及时修复已知漏洞与补丁缺陷，优化软件运行兼容性，杜绝漏洞被恶意利用。严格规范软件安装与使用标准，禁止安装非正规来源及存在未知风险的软件，定期查杀系统病毒、清理恶意程序、卸载冗余软件，保障软件系统纯净、稳定运行。同时，锁定系统核心配置权限，禁止非授权人员随意修改程序参数与系统设置，避免因配置变更导致软件运行异常。（2）在数据安全方面，应建立多重数据备份机制，采用本地备份与异地备份相结合的双重模式，定期对核心业务数据、系统配置数据进行完整备份，并定期测试备份数据的可用性，防止数据丢失或损坏。对系统传输与存储的核心数据实施加密处理，规避数据在传输、存储过程中的泄露风险。同时，严格管控数据共享、导出、传输权限，完整记录数据操作轨迹，杜绝私自导出、外传核心数据的行为，保障数据资源全生命周期的安全可控。

4.3 网络与应急防护保障

强化网络环境防护，搭建安全稳定的网络运行体系，同时完善应急处置机制，提升风险应对能力。（1）在网络防护上，部署防火墙、入侵检测、流量监控等防护工具，实时监测网络访问行为、网络流量状态，精准拦截恶意访问、攻击扫描、非法入侵行为，过滤风险网络流量。划分网络安全区域，将核心业务系统与普通办公网络进行隔离，避免单一区域网络风险扩散，减少网络攻击、病毒蔓延带来的系统损害。同时，定期优化网络架构，排查网络卡顿、延迟、断连等问题，保障网络传输稳定。（2）在应急保障方面，结合系统常见安全风险，制定完善的应急处置预案，明确系统瘫痪、数据异常、病毒入侵、网络攻击等各类突发问题的处置流程、处置步骤和责任人。定期开展应急演练，提升运维人员突发故障处置能力，确保出现安全问题时，能够快速响应、及时止损，最大限度降低安全事故造成的损失。同时，建立系统运行实时监测机制，全天候监控系统状态，实现安全隐患早发现、早处理[5]。

结束语

电子信息系统安全管理是一项涉及硬件设备、软件程序、数据资源、网络环境及人员操作的系统性工程。本文从安全核心概述出发，系统分析了硬件设备、软件数据、人员操作三大维度的安全风险与隐患，并从分级权限管理、日常运维制度、人员安全培训三个层面构建了安全管理体系，同时提出了硬件保障、软件与数据保障、网络与应急防护三项核心保障措施。研究表明，电子信息系统安全需坚持技术防护与管理制度并重，从物理层面、系统层面、管理层面构建多层次安全防线，才能有效保障系统的完整性、保密性与可用性。未来，随着电子信息系统应用场景的持续拓展，安全管理需持续迭代优化，不断提升风险防控能力与应急响应水平。

参考文献

[1]支开来.智能控制技术在电子信息系统中的优化与改进[J].集成电路应用,2024,41(04):318-319.

[2]刘涛.数字信号处理系统在电子信息工程中的应用[J].集成电路应用,2024,41(04):378-380.

[3]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,(03):128-129.

[4]侯祥,赵岩,徐明远.电子信息工程技术的应用与安全防护方案[J].电子世界,2022,(01):208-209.

[5]郑文凯.基于大数据分析的电子信息智能化数据处理系统研究[J].网络安全和信息化,2025,(05):107-109.