信息系统管理与网络通信安全分析

周 斌
江苏州维通信科技有限公司 江苏 扬州 225000

摘 要：在数字化进程加速推进的当下，信息系统与网络通信的安全稳定运行愈发关键。本文聚焦信息系统管理与网络通信安全，先阐述信息系统管理核心维度，包括构成要素、生命周期管理重点、安全需求嵌入机制及与网络通信安全协同关系；接着分析网络通信安全核心威胁与风险传导路径；随后构建信息系统管理视角下的安全管控体系；最后探讨协同优化路径，涵盖管理架构适配、技术融合、协同运维及迭代优化策略，为提升信息系统与网络通信安全水平提供全面参考。

关键词：信息系统管理；网络通信安全；安全管控体系；协同优化路径

引言：在数字化时代，信息系统与网络通信深度融入社会各领域，成为推动发展的关键力量。信息系统管理的高效与否，直接影响业务开展与决策制定；网络通信安全则关乎数据保密性、完整性和可用性，一旦遭受威胁，将带来巨大损失。然而，当前信息系统管理与网络通信安全面临诸多挑战，如安全威胁多样化、管理流程不完善等。因此，深入分析二者关系，构建科学有效的管控与优化体系，具有重要的现实意义。

1 信息系统管理的核心维度与安全适配逻辑

1.1 信息系统管理的核心构成要素

信息系统管理涵盖多个关键构成要素。硬件设施是信息系统的物质基础，包含10类主要设备，如服务器、存储设备、网络设备等，这些硬件的性能与稳定性直接影响系统的运行效率。软件系统则赋予硬件功能，从操作系统到各类应用软件，共同构建起信息系统的功能架构，其中操作系统有5种主流类型，各类应用软件更是多达100种以上[1]。数据资源作为信息系统的核心资产，其准确性、完整性和及时性至关重要，一般企业信息系统中数据量可达1000GB-10000GB不等。人员与组织是信息系统管理的关键力量，不同角色的人员如系统管理员、开发人员、用户等，在系统运行、维护和发展中发挥着独特作用，而合理的组织架构能确保各项管理任务有序开展，通常一个中型企业的信息系统管理团队人员数量在20-50人左右。

1.2 信息系统生命周期中的管理重点

在信息系统生命周期的不同阶段，管理重点各有侧重。规划阶段，需精准定位系统目标，与组织战略紧密结合，合理规划资源投入，一般规划周期为3-6个月。开发阶段，要严格把控软件质量，遵循规范的开发流程，确保系统功能符合需求，开发周期根据系统复杂程度在6-24个月不等。实施阶段，注重硬件设备的安装调试、软件的部署配置以及数据的迁移导入，保障系统顺利上线，实施周期通常为1-3个月。运行维护阶段，持续监控系统性能，及时处理故障，进行软件更新和硬件维护，保证系统稳定运行，维护成本一般占系统总成本的20%-30%。退役阶段，要做好数据备份与迁移，妥善处理硬件设备，避免信息泄露，退役周期约为1-2个月。

1.3 安全需求在信息系统管理中的嵌入机制

安全需求应深度融入信息系统管理全过程。在规划阶段，将安全目标纳入系统整体规划，评估潜在安全风险，制定相应安全策略，一般需识别10-20种潜在安全风险。开发阶段，采用安全编码规范，进行安全测试，从源头上减少安全漏洞，安全测试需覆盖80%-90%以上的代码。实施阶段，严格把控系统部署环境的安全性，确保网络通信加密、访问控制等安全措施到位，加密算法的密钥长度一般要求达到128-256位。运行维护阶段，持续监测安全威胁，及时更新安全补丁，加强人员安全培训，提升安全意识，每年安全培训次数不少于4次。

1.4 信息系统管理与网络通信安全的协同关系

信息系统管理与网络通信安全相互依存、相互促进。有效的信息系统管理为网络通信安全提供坚实基础，通过合理配置资源、规范人员操作，降低安全风险。网络通信安全保障信息系统管理的顺利实施，防止外部攻击和数据泄露，确保系统数据的保密性、完整性和可用性，共同推动信息系统稳定、高效运行。

2 网络通信安全的核心威胁与风险传导路径

2.1 网络通信链路层面的核心安全威胁

网络通信链路作为信息传输的通道，面临着诸多核心安全威胁。物理链路方面，自然灾害如地震、洪水等可能破坏通信线路，导致通信中断[2]。恶意破坏行为也不

容忽视，不法分子可能对光缆、基站等设施进行破坏，影响网络通信的正常开展。窃听攻击同样严峻，攻击者利用特殊设备截取链路中的信号，获取敏感信息，对个人隐私、企业机密乃至国家安全构成威胁。

2.2 网络通信协议层面的安全隐患

网络通信协议是确保不同设备间正常通信的规则集合，但其中存在不少安全隐患。部分协议在设计时未充分考虑安全性，存在漏洞。例如，某些协议在身份认证环节不够严谨，攻击者可伪造身份接入网络，进行非法操作。数据加密机制不完善也是一大问题，一些协议采用较弱的加密算法，容易被破解，导致数据在传输过程中被窃取或篡改。此外，协议的兼容性问题可能引发安全风险，不同版本协议之间的交互可能出现异常，为攻击者提供可乘之机。

2.3 网络通信终端接入的安全风险点

网络通信终端接入网络时存在诸多安全风险点。终端设备自身可能存在漏洞，操作系统、应用程序的缺陷可能被攻击者利用，控制终端设备，进而窃取数据或发起进一步攻击。不安全的接入方式也是风险源，如使用公共无线网络时，若未采取加密措施，数据在传输过程中极易被截取。终端用户的安全意识淡薄同样带来风险，随意点击不明链接、下载未知文件等行为，可能导致终端感染恶意软件，引发安全事件。

2.4 安全威胁在网络通信环节的传导机制

安全威胁在网络通信环节的传导具有复杂性。攻击者从某一环节发起攻击后，可能利用网络通信的连通性，将威胁扩散至其他环节。例如，攻击者通过入侵终端设备获取用户凭证，进而利用这些凭证访问网络中的其他系统，造成更大范围的影响。在网络通信链路中，一个节点的安全漏洞可能成为攻击的突破口，攻击者借此渗透到整个网络，破坏通信的保密性、完整性和可用性，引发连锁反应，导致严重的安全后果。

3 信息系统管理视角下的网络通信安全管控体系

3.1 基于系统管理的网络通信安全策略构建

从信息系统管理视角出发构建网络通信安全策略，需紧密贴合系统整体架构与业务需求。要全面评估信息系统所承载业务的敏感程度与重要性，以此为依据确定不同层级的安全防护标准，划分3-5个安全防护层级[3]。对于核心业务数据传输，应采用高强度的加密算法，确保数据在通信过程中的保密性，加密算法强度不低于256位。同时，依据系统用户角色与权限，制定精细化的访问控制策略，严格限制用户对网络资源的访问范围，防止越权操作引发安全风险，访问控制策略规则数量不少于10条。此外，安全策略的构建还需考虑系统的扩展性与兼容性，确保在系统升级或引入新业务时，安全策略能够无缝适配，持续为网络通信提供有效保障。

3.2 信息系统资源调度中的安全管控措施

在信息系统资源调度过程中，安全管控是关键环节。硬件资源调度方面，需对服务器、存储设备等硬件的分配与使用进行严格监控，避免因资源过度集中或不合理分配导致单点故障，进而影响网络通信的稳定性。软件资源调度时，要确保所部署的软件来源可靠、版本合规，防止恶意软件或存在漏洞的软件进入系统，威胁网络通信安全。数据资源调度过程中，要实施严格的数据分类分级管理，根据数据敏感程度采取不同的传输与存储安全措施，保障数据在流动过程中的安全性。通过全方位的资源调度安全管控，降低因资源管理不善引发的网络通信安全风险。

3.3 网络通信安全态势的动态监测与响应机制

建立网络通信安全态势的动态监测与响应机制，是保障网络通信安全的重要手段。利用先进的监测技术，实时收集网络通信中的各类安全信息，包括流量异常、访问行为异常等。通过对这些信息的深度分析，及时发现潜在的安全威胁，准确评估安全态势。一旦检测到安全事件，迅速启动响应机制，根据预先制定的应急预案，采取相应的处置措施，如隔离受攻击设备、阻断异常流量等，防止安全威胁的进一步扩散。同时，对安全事件进行详细记录与分析，总结经验教训，不断完善监测与响应机制，提升网络通信安全防护能力。

3.4 信息系统管理流程对安全管控的支撑作用

科学合理的信息系统管理流程能够为网络通信安全管控提供有力支撑。在系统规划阶段，将安全需求纳入整体规划，明确安全目标与指标，为后续的安全管控工作指明方向。开发阶段，遵循安全开发流程，进行安全编码、安全测试等工作，从源头上减少系统漏洞，降低网络通信安全风险。运行维护阶段，建立规范的系统维护流程，定期进行安全检查、漏洞修复与系统升级，确保系统始终处于安全稳定的运行状态。通过各阶段管理流程的紧密衔接与协同运作，形成全方位、全过程的安全管控体系，有效保障网络通信安全。

4 信息系统与网络通信安全的协同优化路径

4.1 信息系统管理架构的安全适配优化方向

信息系统管理架构的安全适配优化需从多维度展开[4]。在组织架构层面，应设立专门的安全管理部门或岗位，明确职责分工，确保安全管理工作贯穿于信息系统的规划、开发、运行与维护各阶段，安全管理部门人员

数量根据企业规模在5-20人左右。同时，打破部门壁垒，促进不同部门间的信息共享与协作，形成安全管理的合力，部门间信息共享频率每周不少于3-5次。在技术架构方面，采用分层、模块化的设计理念，将安全功能模块嵌入到信息系统的各个层次中，实现安全防护的深度集成。例如，在网络层部署防火墙、入侵检测系统等安全设备，防火墙数量根据网络规模在2-10台不等；在应用层实施身份认证、访问控制等安全机制，身份认证方式种类可达5-10种。此外，还应关注管理架构的灵活性与可扩展性，以便能够快速适应不断变化的安全威胁和业务需求，管理架构调整周期为每年1-2次。

4.2 网络通信安全技术与信息系统管理的融合应用

网络通信安全技术与信息系统管理的融合是提升整体安全性的关键。将加密技术应用于数据传输过程，确保信息在通信链路中的保密性。无论是采用对称加密算法还是非对称加密算法，都需根据数据的敏感程度和传输环境进行合理选择。身份认证技术则用于验证用户身份的合法性，防止非法用户接入信息系统。通过结合多因素认证方式，如密码、指纹、动态令牌等，提高身份认证的准确性和可靠性。访问控制技术依据用户的角色和权限，限制对信息系统资源的访问，避免越权操作。将这些安全技术与信息系统管理流程紧密结合，实现安全策略的自动化执行和动态调整。

4.3 安全导向下的信息系统与网络通信协同运维模式

建立安全导向的协同运维模式，能够及时发现和解决潜在的安全问题。制定统一的运维标准和规范，明确信息系统与网络通信设备的运维流程和操作要求。通过集中监控平台，实时收集系统和网络的运行状态信息，包括设备性能、网络流量、安全事件等。对收集到的信息进行分析和评估，及时发现异常情况并发出预警。一旦发生安全事件，迅速启动应急响应机制，组织相关人员进行协同处置，快速恢复系统和网络的正常运行。同时，定期对运维工作进行总结和反思，不断优化运维模式，提高安全运维水平。

4.4 长期安全保障下的系统与网络迭代优化策略

为实现长期的安全保障，需制定系统与网络的迭代优化策略。定期对信息系统和网络通信设备进行安全评估，识别存在的安全漏洞和风险隐患。根据评估结果，制定针对性的优化方案，对系统和网络进行升级改造。在升级过程中，充分考虑安全因素，确保新引入的技术和设备与现有系统兼容且具备更高的安全性。同时，关注安全技术的发展趋势，及时引入先进的安全理念和技术手段，提升系统和网络的整体安全防护能力。通过持续的迭代优化，使信息系统和网络通信始终保持良好的安全状态，适应不断变化的安全挑战。

结束语

信息系统管理与网络通信安全紧密相连、相互影响。通过优化管理架构、融合安全技术、建立协同运维模式以及实施迭代优化策略，可有效提升信息系统与网络通信的整体安全性。在实际应用中，需根据具体情况灵活运用这些方法，持续关注安全动态，不断调整和完善安全策略，确保信息系统与网络通信在安全稳定的环境中运行，为各领域的数字化发展提供坚实保障。

参考文献

[1]李宁,李丽.网络通信安全与信息系统管理的安全分析[J].通信电源技术,2022,39(11):101-103.

[2]张杨武.网络通信安全与信息系统管理研究[J].IT经理世界,2024(4):83-85.

[3]王腾.网络通信与信息系统的安全管理措施[J].信息与电脑,2024,36(6):212-214.

[4]李世凯.网络通信安全与信息系统管理的安全分析[J].网络安全技术与应用,2022(7):164-165.