浅谈网络安全和信息化形势下信息安全的应对措施

苗 森
新疆维吾尔自治区战略和应急物资保障服务中心（乌鲁木齐中央级救灾物资储备库） 新疆 乌鲁木齐 830000

摘 要：在全球数字化浪潮席卷之下，网络安全与信息化已成为国家发展的核心驱动力与战略高地。然而，这一进程也使得信息安全——作为网络空间的基石——面临着前所未有的复杂性与严峻性。攻击手段日益智能化、数据价值空前凸显、系统边界持续消融、供应链风险深度交织，共同构成了一个动态演化的高维威胁图景。本文聚焦于“信息安全”这一核心命题，深入剖析了在当前技术与社会双重变革背景下，信息安全所面临的主要挑战，并系统性地提出了一套以“数据为中心”、“智能为驱动”、“协同为支撑”、“法治为保障”的综合应对策略体系。该体系强调从被动响应转向主动免疫，从边界防护转向内生安全，从技术单点突破转向治理生态共建，旨在为构建一个自主可控、安全可信、韧性强大的国家信息安全屏障提供理论指引与实践路径。

关键词：信息安全；数据安全；内生安全；主动免疫；安全治理

引言

2026年，我们正处在一个由数据定义价值、由算法驱动决策、由连接重塑关系的时代。信息化的深度渗透，将物理世界与数字空间前所未有地融合在一起，极大地提升了社会生产力与生活便利性。然而，这种深度融合也意味着风险的同步放大。信息安全，即确保信息的机密性（Confidentiality）、完整性（Integrity）和可用性（Availability）——CIA三元组——不再仅仅是IT部门的技术议题，而是关乎国家安全、经济命脉、社会稳定和个人福祉的根本性问题。从国家级APT（高级持续性威胁）组织对关键基础设施的长期潜伏，到自动化工具对海量个人信息的精准窃取，再到供应链污染引发的系统性崩溃，信息安全威胁呈现出规模化、精准化、隐蔽化和武器化的显著特征。在此背景下，传统的、孤立的、静态的安全防护模式已显疲态。我们必须以全新的视角和系统性的思维，重新审视并构建适应新时代要求的信息安全应对措施。本文将围绕这一核心任务展开论述。

1 新形势下信息安全面临的核心挑战

1.1 数据成为首要攻击目标与核心防护对象

在数字经济范式下，数据已超越传统生产要素，成为最具战略价值的资产。无论是国家层面的战略情报、宏观经济数据，还是企业层面的核心知识产权、客户交易记录，抑或是公民个人的身份信息、生物特征、行为轨迹，都蕴含着巨大的经济与社会价值。这使得数据本身成为了攻击者的首要目标。攻击者不再满足于简单的系统瘫痪（拒绝服务攻击），而是致力于长期潜伏、静默窃取高价值数据，或通过篡改关键数据（如金融交易、医疗记录）来制造混乱、牟取暴利。因此，信息安全的重心必须从保护“系统”本身，向保护“系统中的数据”进行根本性转移。如何在数据的全生命周期内，确保其不被未授权访问、不被恶意篡改、并在需要时可靠可用，是当前最核心的挑战。

1.2 防御边界瓦解与攻击面无限泛化

云计算、移动计算、物联网（IoT）、边缘计算等技术的普及，彻底打破了传统企业网络清晰的物理边界。员工使用个人设备（BYOD）远程办公，业务应用部署在公有云或混合云环境，数以亿计的智能终端（从摄像头到工业控制器）直接接入互联网。这种“无边界”或“多边界”的网络架构，在提升效率的同时，也导致了攻击面的指数级扩张[1]。任何一个配置不当的云存储桶、一个存在固件漏洞的IoT设备、一个弱口令的远程访问接口，都可能成为攻击者入侵整个数字生态系统的入口。传统的、依赖防火墙和网络分段的“城堡与护城河”式防御模型，因其无法有效覆盖这些分散、动态、异构的接入点而失效。信息安全防护必须从关注“边界”转向关注“身份”和“数据流”，实现无处不在的细粒度控制。

1.3 人工智能赋能下的攻防对抗智能化升级

人工智能，特别是机器学习和生成式AI的飞速发展，正在深刻改变网络攻防的格局。一方面，攻击者利用AI可以实现攻击的自动化、规模化和智能化。例如，利用大语言模型（LLM）批量生成高度逼真的钓鱼邮件和社会工程学话术，成功率远超人工；利用强化学习算法自动探测网络漏洞并规划最优攻击路径；甚至开发出能够自主决策、规避检测的AI攻击代理（Agent）。另一方面，防御方也在积极应用AI技术，用于异常行为分析、恶意软件检测、自动化响应等。这使得攻防对抗不再是人与

人的较量，而演变为双方AI模型之间的深度博弈。防御方必须具备同等甚至更强的AI能力，才能在这场“智能化军备竞赛”中占据主动，否则将面临被降维打击的风险。

1.4 供应链安全风险呈现系统性与隐蔽性

现代信息系统是一个高度复杂的集成体，其构建严重依赖于全球化的软硬件供应链。从底层的芯片、固件，到操作系统、数据库，再到上层的应用软件和开源代码库，任何一个环节被植入后门或存在未知漏洞，都可能导致整个链条的失守。近年来频发的供应链攻击事件表明，攻击者正采取“擒贼先擒王”的策略，通过污染上游的开发工具、软件分发渠道或硬件制造环节，实现对下游海量用户的“批发式”攻击。这种攻击方式具有极强的隐蔽性和破坏力，因为被攻击的系统在其自身层面看起来完全正常。更严峻的是，地缘政治因素使得供应链安全问题愈发复杂，技术脱钩、标准割裂等趋势增加了构建可信、可控供应链的难度。信息安全防护必须向上游延伸，将供应商纳入统一的安全治理体系。

2 构建以数据为中心的信息安全综合应对策略

2.1 确立“以数据为中心”的安全防护范式

2.1.1 实施精细化的数据分类分级

这是所有数据安全工作的前提。组织必须首先对其拥有的全部数据资产进行全面盘点和梳理，依据数据的敏感程度、重要性以及泄露后可能造成的危害，建立科学、统一的分类分级标准。例如，可将数据分为公开、内部、秘密、机密、绝密等多个等级。

2.1.2 推行基于属性的动态访问控制（ABAC）

取代传统的、僵化的基于角色的访问控制（RBAC），采用ABAC模型。该模型根据用户的身份、设备状态、访问时间、地理位置、数据敏感级别等多种属性的实时组合，动态地决定是否授予访问权限。这能确保即使凭证被盗，攻击者也无法轻易访问高敏感数据[2]。具体实施中，可依托统一身份认证平台，集成终端安全状态评估（如是否安装最新补丁、是否启用磁盘加密），并将这些状态作为访问决策的关键因子，实现“人-设备-数据”三位一体的细粒度授权。

2.1.3 应用先进的数据保护技术

针对不同级别的数据，部署相应的保护技术。对于静态存储的数据，强制实施强加密，优先采用支持透明数据加密（TDE）的数据库，并将密钥交由硬件安全模块（HSM）或云KMS统一管理，杜绝密钥硬编码在应用代码中；对于传输中的数据，确保端到端加密，强制使用TLS 1.3协议，并禁用弱密码套件；对于使用中的数据，积极探索和应用隐私增强计算（Privacy-Enhancing Computation, PEC）技术，如联邦学习、安全多方计算（MPC）和同态加密，实现“数据可用不可见”，从根本上化解数据利用与安全保护之间的矛盾。在金融风控、医疗科研等场景中，可试点MPC技术，使多方在不共享原始数据的前提下联合建模。

2.2 构建智能驱动的主动免疫与纵深防御体系

2.2.1 拥抱“零信任”安全架构

零信任的核心思想是“永不信任，始终验证”。它假设网络内外都存在威胁，因此对每一次访问请求，无论来源，都必须进行严格的身份认证、设备健康检查和最小权限授权。这为无边界网络环境提供了坚实的安全基础。具体落地时，可部署零信任网络访问（ZTNA）网关，替代传统VPN，实现应用层的细粒度访问控制；同时，将多因素认证（MFA）作为所有高敏系统登录的强制要求。

2.2.2 部署内生安全与主动免疫机制

将安全能力内嵌于信息系统的设计、开发和运行全过程。通过在硬件、操作系统、应用等各层植入可信根（Root of Trust）和安全监控模块，使系统具备自我感知、自我诊断、自我修复的能力。一旦检测到异常行为或恶意代码，能够立即隔离、阻断并尝试恢复，如同生物体的免疫系统。例如，在服务器固件层启用TPM芯片提供硬件级可信启动；在容器化环境中，通过eBPF技术实现运行时行为监控，对异常进程调用（如非预期的文件写入或网络外联）实时告警并阻断。

2.2.3 建设AI赋能的安全运营中心（SOC）

利用大数据和AI技术，构建下一代智能SOC。它能够对来自全网的海量安全日志、网络流量、终端行为等数据进行实时关联分析，精准识别已知和未知威胁。通过安全编排、自动化与响应（SOAR）平台，将分析结果自动转化为标准化的响应动作，极大提升安全事件的处置效率和准确性，形成“预测-防护-检测-响应-自愈”的闭环[3]。例如，当EDR检测到某终端有可疑的PowerShell脚本执行行为，SOC可自动触发剧本（Playbook）：隔离主机、冻结账户、提取内存镜像、通知安全分析师——整个过程可在数秒内完成。

2.3 强化全链条的供应链与第三方风险管理

2.3.1 建立供应商安全准入与评估机制

在引入任何第三方产品或服务前，必须对其进行严格的安全评估，包括代码审计、漏洞扫描、安全开发生命周期（SDL）成熟度审查等。明确要求供应商提供软件物料清单（SBOM），以便清晰掌握其产品的组件构成和潜在风险。评估应覆盖开源组件（如Log4j类漏洞）、许可证合规性及历史漏洞修复时效，并将结果作为采购决

策的关键权重项。

2.3.2 实施持续的供应链安全监控

安全管控不应止于采购环节。应与关键供应商建立持续的安全沟通机制，要求其及时通报新发现的漏洞和安全事件。利用自动化工具，对已部署的第三方软件进行持续的漏洞监测和合规性检查[4]。可接入国家漏洞库（CNNVD）或商业威胁情报平台，设置自动化告警规则，一旦所用组件出现高危CVE，立即触发应急响应流程。

2.3.3 推动构建可信的国产化生态

在关键领域，应大力扶持和发展自主可控的软硬件产业，逐步构建一个安全、可靠、透明的本土化供应链体系，从源头上降低因外部依赖带来的系统性风险。在政务、能源、金融等行业，优先选用通过国家等保三级及以上认证的国产数据库、操作系统和中间件，并参与行业信创联盟，共同制定安全标准。

2.4 夯实法治、人才与文化三位一体的治理根基

2.4.1 完善信息安全法治与合规体系

严格遵循《网络安全法》、《数据安全法》、《个人信息保护法》等法律法规的要求，将合规性内化为组织的基本运营准则。建立健全内部数据安全管理制度和操作规程，明确各岗位的安全职责，并定期进行合规审计。特别要落实数据出境安全评估、个人信息影响评估（PIA）等法定程序，并留存完整记录以备监管检查。

2.4.2 破解信息安全人才瓶颈

信息安全的竞争归根结底是人才的竞争。必须加大投入，通过高等教育改革、职业培训、实战演练等多种途径，培养既精通密码学、攻防技术等硬核技能，又具备风险管理、合规治理等软实力的复合型人才。同时，建立有竞争力的薪酬和职业发展通道，吸引和留住顶尖人才。可设立内部红蓝对抗实验室，定期组织CTF竞赛或攻防演练；与高校共建“网络空间安全学院”，定向培养人才；鼓励员工考取CISSP、CISP-DSG等权威认证。

2.4.3 培育全员参与的安全文化

再先进的技术也无法完全弥补人为疏忽带来的风险。必须将信息安全意识教育常态化、场景化，覆盖组织内的每一位成员。通过定期的、贴近实际工作场景的培训和模拟演练（如钓鱼邮件测试），让安全规范深入人心，转化为自觉行动，真正筑牢信息安全的第一道也是最后一道防线。

3 结语

在网络安全与信息化深度融合的新时代，信息安全已上升为一项关乎全局的战略性、基础性工程。其所面临的挑战是多维度、深层次且不断演进的。应对之道，绝非依赖单一技术或孤立举措，而在于构建一个以“数据”为核心、以“智能”为引擎、以“协同”为纽带、以“法治”为基石的综合性、动态化、自适应的安全治理体系。这一体系要求我们转变观念，从被动防御走向主动免疫；聚焦核心，将数据资产置于防护的中心；开放协同，整合内外部资源形成合力；固本培元，通过法治、人才和文化筑牢根基。唯有如此，我们才能在波谲云诡的数字浪潮中，牢牢守住信息安全的底线，为国家的长治久安、经济的繁荣发展和人民的幸福安康构筑起坚不可摧的数字长城。

参考文献

[1]丘业.信息化背景下计算机网络信息安全防护策略分析[J].信息与电脑,2025,37(06):90-92.

[2]李凡.探析企业信息化建设中的网络信息安全[J].网络安全技术与应用,2024,(03):88-90.

[3]吴保安.如何做好网络信息化时代信息安全保密工作[J].网络安全技术与应用,2022,(08):101-103.

[4]李长挺.信息化背景下计算机网络信息安全防护策略[J].电子世界,2022,(01):146-147.