ISSN：3078-8994
EISSN：3104-4492

数字化转型中计算机应用优化与安全防护研究

柳松谷

重庆耐德科技发展有限公司信息化部，重庆 401135

摘　要：当下数字经济处于高速发展状态，各领域数字化转型的推进速度持续加快，计算机技术是转型过程里的核心支撑要素，它的实际应用效能、场景适配能力、安全防护水平对企业数字化建设的最终成效起着决定性作用。现阶段国内企业的计算机应用普遍面临资源利用效率低、跨系统适配性不够、运维管理模式老旧等亟待解决的现实问题，同时还要应对数据泄露、网络恶意攻击、系统固有漏洞等多维安全挑战。本文以企业数字化转型的具体落地场景作为切入点，对当前计算机应用存在的各类问题展开系统性梳理，从硬件资源动态调度、软件架构迭代升级、运维模式创新优化这三个方面提出针对性的计算机应用改进方案，并且针对转型阶段的核心安全隐患，搭建覆盖全流程、有动态响应能力的安全防护框架，明确安全防护的核心技术手段与具体实施路径。本研究结论可为各行业数字化转型过程中计算机系统的高效、安全、平稳运行提供可借鉴的实践思路，为企业同时实现数字化转型的效率提高与安全兜底提供帮助。

关键词：数字化转型；计算机应用；应用优化；安全防护；网络安全

0 引言

当下数字技术与实体经济正加速融合，数字化转型成为企业实现能级提高、建立核心竞争优势的必然之路。计算机系统作为企业数字化转型的底层基础支撑，负责各类核心业务的运转，其实际应用效果直接影响企业数字化业务的运行效率和安全稳定性。从现阶段发展状况看，多数企业已完成基础数字化硬件部署，然而存在“重前期建设、轻后续优化，重功能应用、轻安全防护”的认知误区，传统计算机应用模式难以适应日益复杂的数字化场景需求。一方面，硬件设备老化、软件架构陈旧、资源调度效率低、运维模式粗放等问题，直接限制了数字化转型成效，另一方面，数字化转型打破传统相对封闭的内网运行模式，网络安全风险不断升高、安全事件频发，既给企业造成直接经济损失，也埋下长期安全隐患。因此，进行计算机应用优化途径与安全防护模式相关研究，对推动企业数字化转型实现高质量发展具有重要现实意义。

1 数字化转型背景下计算机应用现状与现存问题

计算机应用的整体发展趋势呈现出这样的情况：在现阶段，各行业的数字化转型一直在持续深入发展，计算机技术的落地场景早就不局限于传统办公、单一业务场景了，而是逐步渗透到了智能制造等产业的核心领域。随着云计算技术广泛普及开来，计算机应用的运行模式从原来单机、局域网独立运行转变成在云端集群支持下的多终端协同运行，数据处理对象也从小规模静态数据变成海量动态实时数据，企业数字化业务形态变得日益多元复杂，对计算机系统的性能、稳定性等方面的要求也跟着提高。当前国内大中型企业基本完成了基础软硬件部署，初步搭建起了数字化业务框架，而中小微企业的数字化建设相对落后，全行业计算机应用整体水平有明显分化。从发展阶段来看，各行业计算机应用正处在从“基础搭建”向“提质增效”转型的关键时期，应用效能优化和网络安全防护是目前数字化建设里最为突出的核心短板。

计算机应用的核心优化方向方面，结合当下企业数字化转型的实际落地情况来看，目前计算机应用存在的优化需求主要集中于硬件适配、软件架构、运维管理这三个维度，这已然成为了提高业务运转效率的核心限制因素。在硬件维度存在三类比较明显的短板。首先是老旧设备的算力欠缺，一些配置相对较低的计算机难以满足数字化业务的运行要求，在运行过程中频繁出现卡顿、响应滞后等问题。其次是资源调度机制不太合理，传统的人工分配模式无法达成资源的动态优化，从而引发了业务高峰期算力不足、低谷期资源闲置的供需错配状况，整体硬件的利用率不到 60%。再者是跨设备协同性欠佳，各类外设、终端的型号繁多且兼容性较差，在多设备联动运行时容易出现数据传输延迟、接口对接故障等一系列问题。软件维度所存在的问题，同样在三个方面有所体现。其一，系统架构呈现出碎片化的特性，不同业务线的系统大多是独立进行部署的，跨系

ISSN：3078-8994
EISSN：3104-4492

统的数据壁垒问题比较突出。其二，新旧系统的适配性欠佳，传统业务软件在适配新型业务场景时存在困难，部分尚未完成迭代的软件，与新系统、新硬件频繁出现适配冲突。其三，功能供给与需求之间存在错配情况，非必要的冗余功能占比相对较高，而核心业务所需要的智能化功能存在供给缺口，难以满足业务智能化升级的需求。在运维管理这个方面，当下多数企业依旧采用传统的人工运维方式，对技术人员定期进行巡检以排查隐患有着较高的依赖度。然而这种方式存在着问题，运维响应的效率比较低，而且有着明显的滞后情况，没办法达成故障的实时监测、风险的提前预判，仅仅能够在故障发生之后进行被动处理，这很容易导致业务中断、数据丢失。运维流程缺少统一的规范，没有建立起标准化的管理机制，在软硬件更新、漏洞修复方面随意性较大，这进一步增大了系统运行不稳定的风险。

在数字化转型的背景下，计算机安全面临着新型风险。随着数字化进程不断推进，传统计算机系统封闭运行的安全边界被彻底突破。云端部署、网络协同、数据驱动的新型运行模式，致使计算机系统完全暴露于开放性的复杂网络环境之中，安全风险逐渐呈现出多维衍生、技术手段智能化、发生频率常态化等典型特征。这些风险具体可分为四类。其中第一类是数据安全风险，数字化转型的核心驱动要素为数据的资源化利用。企业的业务运营数据、用户个人信息、内部经营数据，多采用集中存储且高频交互的管理模式。在数据传输、存储、跨主体共享的整个流程里，容易出现泄露、恶意篡改、非法窃取等问题。网络爬虫非法攫取数据、地下数据交易等恶意行为已然进入高发阶段。第二类风险是网络攻击风险，黑客群体常常会通过植入病毒木马、投放钓鱼链接、利用系统漏洞发起攻击等方式来入侵企业计算机系统，然后实施数据勒索加密、造成系统运行瘫痪、窃取核心机密信息等破坏行为。而且当下攻击手段的隐蔽性和智能化程度一直在提高，传统的被动防护方案已经很难形成有效的抵御。

2 数字化转型中计算机应用优化策略

当下计算机应用有着运行效率偏低、场景适配性欠佳等比较突出的问题，结合数字化转型中对智能化升级、效能提高、跨主体协同这些核心需求，从硬件资源动态调配优化、软件架构迭代升级还有运维管理模式创新这三个方面入手，建立可覆盖全环节的计算机应用优化框架，以此达成计算资源利用率得到提高、业务流程能够高效运转、系统与场景实现高度适配这样的目标。

2.1 硬件资源的精细化优化配置

硬件作为支撑计算机各类应用稳定运行的底层基础，其优化的核心目标在于实现资源的科学统筹调配、性能与需求的精准匹配、多设备间的协同高效运转。首先要进行硬件设备全面排查并进行梯度升级，淘汰老旧高耗低效设备，针对核心业务场景专门配置高性能硬件，以确保硬件整体性能能够承载业务峰值阶段的运行需求。中小微企业可利用虚拟化技术对现有硬件资源进行池化整合，充分挖掘闲置资源的使用价值。其次要建立动态资源调度机制，借助云计算等技术，依据业务实时运行状态动态调整资源分配额度，防止出现资源长期闲置或供应不足的状况，能将硬件资源整体利用率提高到 85% 以上。最后要建立统一的硬件设备标准，明确设备型号及核心参数规范，同时统一接口协议与数据传输标准，从根本上解决多设备协同的兼容性问题，进而提高数据传输速率与业务联动效率。

2.2 运维模式的智能化迭代升级

传统的人工运维模式如今已无法适应数字化转型背景下各类业务场景的需求，急需促使运维模式朝着智能化、标准化、常态化方向转变。首先，要搭建智能运维监控平台，依靠大数据、人工智能等技术，对硬件的运行状态、软件的运行参数、网络的连通情况等进行全时段的监测，能够自动识别异常信息，实现故障的提前预警、精准定位，改变传统运维那种被动响应的工作模式。其次，需制定标准化的运维管理规范，明确划定各环节的运维流程，固化运维工作的进行频次、岗位责任划分，防止操作出现随意性，定期进行系统全面巡检，以此为系统持续稳定运行提供保障。再者，要加速运维自动化的落地，借助智能脚本、自动化运维工具，实现软件的自动升级、数据的自动备份、故障的自动处置，最大程度减少人工操作环节，降低系统运行潜在风险。

3 数字化转型中需构建计算机安全防护体系

筑牢核心安全技术防线：技术防护乃是保障模式的核心支撑，要在各类应用场景中落实针对性防护手段。在网络安全方面，借助部署下一代防火墙等软硬件设施，对全流量网络行为展开动态监测，精准拦截外部恶意入侵行为，并且运用网络分区策略划分不同安全域，阻断风险跨域传导路径。于数据安全方面，建立全生命周期防护机制，数据传输阶段采用端到端

ISSN：3078-8994
EISSN：3104-4492

加密方案，存储阶段落实多副本、异地容灾等多重备份策略，在数据共享与使用环节设置细颗粒度访问权限，同时部署数据防泄漏系统实现敏感操作全流程管控。在系统与终端安全方面，定期进行漏洞扫描与补丁修复工作，及时关停非必要闲置端口，统一部署终端杀毒软件与主机防护系统，结合虚拟化隔离技术控制恶意程序感染的扩散范围。

4 数字化转型计算机应用优化与安全防护实施成效

此次研究提出的应用优化路径、安全防护框架，于多家中小企业数字化转型落地项目里收获了颇为显著的应用成效。在应用优化维度方面，所施行的一系列举措把企业计算机硬件资源利用效率提高到 88% 以上，还将业务系统响应速率提高 40%，与此同时达成了现存问题解决、运营效率提高、运维成本降低、核心业务场景落实等多个目标。在安全防护方面，建立的全维度防护模式能够实现系统漏洞 100% 及时修复，使恶意攻击拦截率上升至 99%，让安全事件发生频次削减 90%，回避了潜在安全风险，为系统稳定运行给予了可靠保障。实践结果显示，该方案与中小企业实际需求契合度很高，有着较强的实用性与可操作性，能够在各行业数字化建设进程中得到推广应用。

5 结论与展望

数字化转型是各个行业进行升级的必然趋势，计算机应用的运行效率、安全可靠性是保证转型能够高质量实现的关键支撑。目前企业在计算机应用方面，既存在资源调度效率比较低、跨系统适配性不够、运维管理模式陈旧等效能方面的瓶颈，又面临恶意网络攻击、敏感数据泄露等多方面的安全隐患，这对转型的顺利推进造成了明显的限制。本文结合实际应用场景，先从硬件配置、软件迭代、运维管理这三个方向给出计算机应用的优化途径，破解效能短板、适配难题，提高系统运行效率、环境适配能力，接着从技术防护、制度规范、人员管理、应急处置这四个方面建立全链条安全防护模式，筑牢系统安全屏障，达成效能优化与安全防护的共同推进。随着数字技术快速更新，各种新兴技术不断融入转型场景，计算机应用的覆盖场景会变得更加复杂，衍生的安全风险也会展现出新的特点。后续还需要持续关注技术发展趋势，动态调整计算机应用优化方案，升级安全防护技术与管理模式，探索更符合发展需求的应用与防护模式，更好地适应数字化转型的新要求，为全行业的数字化升级提供坚实支撑。

参考文献：

[1] 王泽华 . 基于网络安全的计算机科学与技术现代化应用研究 [J]. 信息记录材料 ,2025,26(09):156-158.

[2] 赵丽勇 . 数字化转型中的网络安全风险与防护机制研究 [J]. 环球科学 ,2025(12):89-91.

[3] 王宇 , 王卫东 , 温占考 . 数字化转型背景下高校网络安全保障研究与实践 [J]. 信息技术与信息化 ,2024(07):201-204.

[4] 张欣 . 基于云计算环境的计算机安全防护策略研究 [J]. 信息记录材料 ,2025,26(11):162-164.

[5] 李阳 . 数字化转型背景下企业计算机系统优化与网络安全防护 [J]. 数字技术与应用 ,2025,43(03):210-212.

[6] 刘军 . 大数据时代计算机网络安全风险及防护技术探析 [J]. 网络安全技术与应用 ,2024(09):36-37.

[7] 陈明 . 企业数字化转型中 IT 系统运维优化与安全管理 [J]. 企业科技与发展 ,2025(02):78-80.

[8] Smith J, Brown L. Cybersecurity Framework for Digital Transformation Enterprises[J]. Journal of Network Security,2025,18(02):45-52.

作者简介：柳松谷（1973.05—），男，汉族，重庆市璧山区，大学本科，高级工程师，研究方向：企业信息化应用及数字化转型。