大规模信创操作系统替换研究与实践

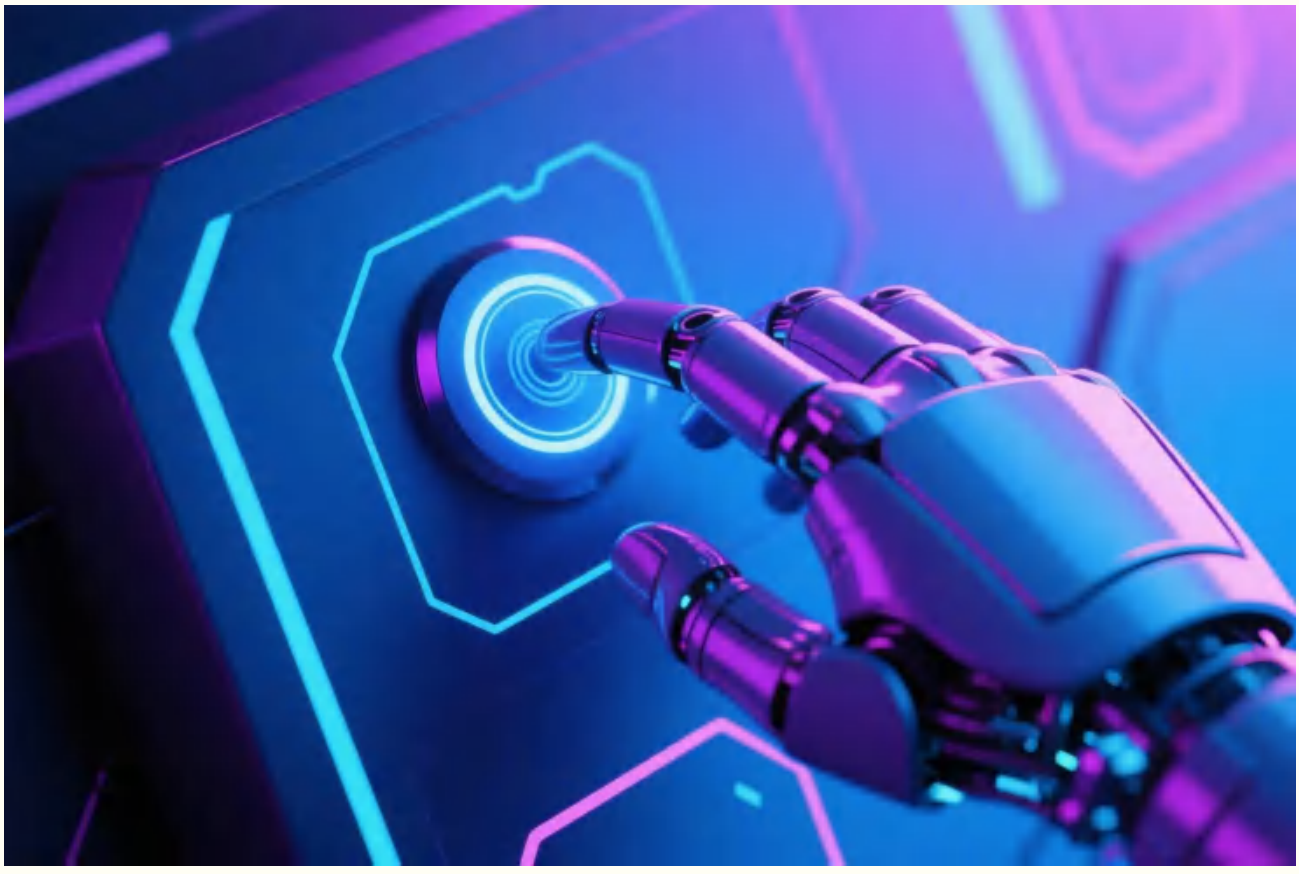
文◆中移动信息技术有限公司 李广博 班文娇 王 伟 杨 洪 阮 前 李 瑶

引言

在信息时代的大潮中，操作系统作为软件生态的基石，其重要性不言而喻。长期以来，我国在操作系统领域的对外依存度高，形成了对国际厂商的深度依赖[1]。这种依赖不仅构成了潜在的安全威胁，还阻碍了我国软件行业的自主创新步伐。随着全球信息化的加速推进，信息安全与科技自立自强已成为国家发展的核心议题，因此推动信创国产化操作系统的普及与应用成为我国实现科技自立自强的关键一环。

信创操作系统作为国家信息技术创新的重要组成部分，承载着提升我国软件行业竞争力、保障国家信息安全的重任。尽管近年来信创操作系统已逐步崭露头角，但在大规模替换现网中存量的非信创操作系统时，面临的挑战不容小觑。这些挑战包括技术迁移的复杂性、业务连续性的保障、用户习惯的转变等，如何在确保业务系统连续性和稳定性的同时，实现信创操作系统的平稳替换，成为亟待解决的问题。

为了深入探讨信创操作系统的发展现状与未来趋势，剖析大规模替换的关键技术与策略，本



【作者简介】李广博（1988—），男，河北邢台人，本科，研究方向：云计算、自动化。

文旨在构建一套既能确保业务系统连续性和稳定性，又能兼顾安全性的替换方案。研究中，聚焦信创操作系统的实际应用，通过分析替换实施案例，评估替换效果，提炼出一系列有效策略。这些策略不仅涵盖技术层面的考量，还涉及业务流程的优化和安全风险的管控，为信创操作系统的推广和应用提供了实践指导。

1 信创操作系统现状与发展

1.1 国产操作系统的技术进展

自 21 世纪初以来，中国在国产操作系统的研发上取得了显著进展，其中最具代表性的是 OpenEuler、OpenAnolios、KylinOS、UOS、BCLinux 等操作系统 [2]。这些操作系统在内核设计、安全机制、用户体验以及兼容性方面进行了大量创新与改进，逐步缩小了与国际主流操作系统的差距。

在内核设计方面，中国国产操作系统多基于 Linux 内核进行二次开发，不仅保证了系统的稳定性和安全性，还充分利用了开源社区的丰富资源。例如，OpenEuler 操作系统采用了自主可控的安全可信内核，通过优化内核调度算法，显著提升了系统的响应速度和处理能力。

安全机制方面，国产操作系统在用户权限管理、数据加密、网络防护等方面进行了深度定制，以适应复杂多变的网络环境。KylinOS 以其严格的安全策略和先进的防火墙技术，在政府机构和军事领域得到了广泛应用，有效保障了国家信息安全。

用户体验方面，国产桌面操作系统也进行了诸多创新。KylinOS、UOS 操作系统界面设计人性化，操作流程简洁，支持多种办公软件和应用，极大地提高了工作效率。同时，为了满足用户个性化需求，还提供了丰富的主题和软件商店，使用户能够轻松定制属于自己的操作系统。

兼容性方面，国产操作系统通过引入兼容层技术，实现了对大量现有应用软件的支持，有效缓解了软件生态建设初期的兼容性问题。KylinOS、UOS 均支持 Wine 兼容层，能够运行大量基于 Windows 平台的应用程序，大幅提升了系统的实用性和普及率。

值得一提的是，国产操作系统在特定领域的应用上也取得了突破性进展。例如，在云计算领域，基于国产操作系统的云平台能够提供高效、稳定的服务；在移动设备和嵌入式系统领域，国产操作系统展现出了强大的适应性和生命力。

国产操作系统在技术进展方面取得了令人瞩目的成就，不仅提升了国家的信息安全水平，还为我国软件行业的自主创新注入了新的动力。然而，面对复杂多变的信息技术环境，国产操作系统仍需在技术、生态、市场推广等多方面持续努力，以实现更广泛的应用和更深入的发展。

1.2 信创生态与市场需求分析

信创生态的构建与市场需求的洞察是推动国产操作系统向前发展的双轮驱动 [3]。信创生态不仅涵盖了操作系统本身，还包括了硬件设备、应用软件、开发工具、服务支持以及教育培训等各环节的协同发展。一个完善且健康的信创生态，能够为用户提供全方位的技术支持和解决方案，从而提升用户满意度，加速国产操作系统的市场渗透。

硬件兼容性是构建信创生态的基石。随着国产 CPU、服务器、存储设备等硬件技术的不断突破，信创操作系统与国产硬件的兼容性得到了显著提升。例如，基于飞腾、龙芯、兆芯等国产 CPU 架构的服务器，与 OpenEuler、OpenAnolios、KylinOS、UOS、BCLinux 等操作系统实现了无缝对接，共同构建了安全可控的信息技术底座。

软件生态的繁荣是信创生态发展的关键。国产操作系统通过建立应用软件适配中心、开发者社区等平台，吸引了大量软件开发商和独立开发者参与其中。这些平台不仅提供了软件开发、测试、优化的环境，还鼓励开发者基于国产操作系统进行创新，丰富了软件库，提升了用户体验。例如，OpenEuler、OpenAnolios、KylinOS、UOS 操作系统建立了自己的软件商店，内置了办公、设计、编程等各类应用，满足了不同用户群体的需求。

服务支持与教育培训是信创生态不可或缺的组成部分。为了解决用户在使用国产操作系统过程中遇到的技术难题，建立了专业的技术支持团队和在线服务平台。同时，针对不同层次的用户，开设了线上线下结合的培训课程，帮助用户快速掌握操作系统的基本操作和高级应用。这不仅增强了用户对国产操作系统的信心，还培养了一批熟悉并支持国产操作系统的 IT 人才。

市场需求的洞察与响应能力是信创生态持续发展的动力。通过深入分析不同行业、不同领域的用户需求，国产操作系统厂商能够及时调整产品策略，推出符合市场需求的定制化解决方案。例如，针对金融、医疗、教育等行业，开发了专用版本的操作系统，满足了行业特定的安

全、稳定和功能需求。

信创生态构建与市场需求洞察，相辅相成，共同推动了国产操作系统的发展。未来，随着信创生态的不断完善和成熟，国产操作系统将能够更好地服务于国家的发展战略，为我国软件行业的自主创新和信息安全提供更强大的支撑。

2 大规模替换的关键技术与策略

2.1 业务系统连续性的保障机制

在大规模替换信创操作系统的过程中，业务系统的连续性是首要考虑的因素。为了确保替换过程中的业务不中断、数据不丢失，必须有一套完善的保障机制。本节将深入探讨如何在替换过程中保障业务系统的连续性，包括数据迁移策略、应用兼容性解决方案、测试与验证流程以及应急响应机制。

2.1.1 数据迁移策略

数据迁移是业务系统连续性保障的关键环节。在替换操作系统时，必须确保数据的完整迁移，避免数据丢失或损坏。为此，可以采取以下策略。

（1）增量备份与恢复。在迁移开始前，对业务系统进行全面的增量备份，确保所有数据、配置信息能够被准确无损地保存。迁移过程中，使用自动化的恢复工具，将备份数据快速恢复到新的操作系统上，减少业务中断时间。

（2）数据转换工具。针对不同格式的数据，开发或选用合适的数据转换工具，确保数据在不同操作系统间的格式兼容性，避免迁移过程中由于数据格式不匹配而导致的问题。

（3）数据验证。迁移完成后，实施严格的数据验证流程，通过数据比对、一致性检查等手段，确保迁移后的数据与原始数据完全一致，无任何遗漏或损坏。

2.1.2 应用兼容性解决方案

应用兼容性是影响业务系统连续性的另一个重要因素。确保现有应用在新的操作系统上能够正常运行，是替换过程中的重要任务。

（1）兼容性测试平台。构建兼容性测试平台，对所有关键应用进行预先测试，识别并解决应用在新操作系统上的兼容性问题。测试应涵盖功能测试、性能测试和稳定性测试，确保应用的全面兼容性。

（2）应用适配层。开发应用适配层或使用已有的中间件，如 Wine、Docker 等，以解决应用与操作系统之间的兼容性问题。适配层可以模拟应用所需的环境，使其在不同的操作系统上运行无异。

（3）应用迁移工具。使用自动化应用迁移工具，简化应用从旧操作系统到新操作系统迁移的过程，减少人工干预，提高迁移效率和成功率。例如，中国移动集团信息技术中心自研的信创操作系统智能管控平台，实现了非信创操作系统向信创操作系统无缝迁移，保障了业务系统的稳定性和高可用性，实现了操作系统自主可控。

2.1.3 测试与验证流程

测试与验证是确保业务系统连续性的必要步骤。通过系统化的测试，可以及早发现并解决潜在的问题，降低替换过程中的风险。

（1）环境搭建。在替换前，搭建与生产环境完全相同或相似的测试环境，用于模拟真实业务场景，进行测试和验证。

（2）多轮测试。进行多轮单元测试、集成测试和系统测试，确保替换过程中的每一个环节都经过充分验证，没有遗漏。

（3）用户验收测试。在内部测试完成后，邀请关键用户参与验收测试，通过实际操作验证替换后的系统是否满足业务需求，无任何功能或性能上的缺陷。

2.1.4 应急响应机制

尽管有周密的计划和预防措施，但在大规模替换过程中，仍会遇到不可预见的问题。因此，建立一套应急响应机制，对于保障业务系统连续性至关重要。

（1）快速回滚方案。制定快速回滚方案，确保在替换过程出现问题时，能够迅速将系统恢复到替换前的状态，减少业务中断时间。

（2）技术专家团队。组建由技术专家组成的支持团队，提供 7×24h 的技术支持，一旦出现紧急情况，能够立即响应，解决问题。

（3）通信计划。制定详细的通信计划，确保在替换过程中，所有相关方都能够及时获得信息、了解替换进度以及任何可能影响业务的变更。

通过实施上述策略和机制，可以大幅降低大规模替换信创操作系统过程中对业务系统连续性的影响，保障业务的平稳过渡，为后续的国产化替代工作奠定坚实的基础。

2.2 系统稳定性与兼容性提升策略

系统稳定性与兼容性是衡量

操作系统性能的关键指标，尤其在大规模替换非信创操作系统的过程中，这两点显得尤为重要。为了确保信创操作系统在替换后的稳定性以及与现有业务环境的兼容性，本节将重点探讨一系列提升策略，旨在构建一个既能满足业务需求，又能适应复杂环境的信创操作系统生态。

2.2.1 系统稳定性提升策略

（1）内核优化与安全加固。内核作为操作系统的核心，其稳定性直接影响着整个系统的运行状态。通过优化内核调度策略，提升资源分配效率，可以显著增强系统的稳定性和响应速度[4]。此外，实施严格的安全策略，如限制用户权限、启用防火墙和入侵检测系统，能有效防止潜在的系统崩溃和安全漏洞。

（2）自动化监控与故障预测。建立一套全面的自动化监控体系，实时监测系统运行状态，包括 CPU 使用率、内存占用、磁盘 I/O 等关键指标。利用大数据分析和机器学习技术，对监控数据进行深入分析，提前预测可能的故障点，及时采取预防措施，避免系统故障的发生。

（3）连续性集成与部署。采用持续集成（CI）和持续部署（CD）的开发模式，确保每一次代码变更都能经过严格测试，无误后自动部署到生产环境。这样不仅能提高开发效率，还能减少人为错误，保持系统的稳定运行。

2.2.2 兼容性提升策略

（1）构建兼容性测试框架。开发一套兼容性测试框架，用于测试信创操作系统与现有硬件、软件的兼容性。该框架应涵盖各种设备驱动、应用软件、网络协议等，确保在替换后，业务系统能够无缝运行。

（2）应用虚拟化与容器化。利用虚拟化技术，如虚拟机或容器，可以为特定应用创建独立的运行环境，解决直接硬件兼容性问题。通过容器化，可以在信创操作系统上运行原本为其他操作系统设计的应用，同时保证业务的连续性和系统的稳定性。

（3）应用程序接口（API）标准化。制定统一的应用程序接口标准，确保在不同操作系统之间，应用软件能够通过标准接口进行通信和数据交换，从而提高跨平台的兼容性。例如，采用 POSIX 标准，使应用能够在多种 UNIX 和类 UNIX 系统上运行，而无需修改。

（4）用户反馈与迭代优化。建立用户反馈机制，收集用户在使用信创操作系统过程中遇到的兼容性问题，及时进行调整和优化。通过持续迭代，逐步提升系统的兼容性，满足更多用户的需求。

通过上述策略的实施，可以显著提升信创操作系统的稳定性与兼容性，为大规模替换工作提供坚实的保障。这不仅有助于提升业务系统的运行效率，还能增强用户对国产操作系统的信心，促进信创生态的健康发展[5]。

2.3 安全性增强与风险防控措施

在大规模替换信创操作系统的过程中，安全性增强与风险防控是不可忽视的环节。面对复杂的网络环境和潜在的安全威胁，必须采取一系列措施，确保替换过程中的数据安全、系统安全以及业务安全。本节将深入探讨如何在大规模替换中增强安全性以及实施有效的风险防控措施。

2.3.1 数据安全防护

数据安全是信创操作系统替换中的首要安全问题。在替换过程中，数据面临泄露、篡改或丢失的风险。为了保护数据安全，可以从以下几个方面入手。

（1）加密技术应用。在数据传输和存储过程中，采用先进的加密技术，如 AES、RSA 等，确保数据在传输过程中的安全性，防止未授权访问和数据泄露。

（2）访问控制策略。实施严格的访问控制策略，包括基于角色的访问控制（RBAC）和最小权限原则，确保只有授权用户才能访问特定数据，减少数据泄露的风险。

（3）数据备份与恢复计划。制定详细的数据备份与恢复计划，定期进行数据备份，并确保备份数据的安全存储。在数据丢失或系统故障时，能够迅速恢复，减少业务中断时间。

2.3.2 系统安全加固

系统安全是保证业务连续性的基石。在大规模替换信创操作系统时，应采取以下措施，增强系统安全性。

（1）安全配置与补丁管理。对信创操作系统进行安全配置，关闭不必要的服务和端口，减少攻击面。定期更新操作系统和应用程序的补丁，修复已知的安全漏洞，降低被攻击的风险。

（2）入侵检测与防御系统。部署入侵检测系统（IDS）和入侵防御系统（IPS），实时监测网络流量，识别并阻止潜在的攻击行为，保护系统免受恶意软件和网络攻击。

（3）安全审计与日志分析。实施安全审计，记录系统和网络的所有操作，定期分析日志，及时发现异常行为，对潜在的安全威胁进行预警和响应。

2.3.3 业务安全与连续性

在确保数据和系统安全的同时，业务安全和连续性同样重要。为了保证替换过程中的业务安全，可以采取以下措施。

（1）业务影响分析。在替换前进行业务影响分析，评估替换过程对业务连续性的影响，制定相应的风险缓解计划。

（2）业务恢复计划。建立业务恢复计划，包括灾难恢复和业务连续性计划，确保在遇到突发事件时，能够快速恢复业务运营，减少经济损失。

（3）用户培训与意识提升。对用户进行安全培训，提高其对网络安全威胁的意识，教育用户识别和防范网络钓鱼、恶意软件等安全风险，减少人为因素导致的安全事件。

2.3.4 风险防控措施

为了有效防控替换过程中可能遇到的风险，实施以下措施。

（1）风险评估与管理。在替换前进行全面的风险评估，识别潜在的风险点，制定风险防控策略。持续监测风险变化，及时调整防控措施。

（2）多层防御体系。构建多层防御体系，包括网络边界防护、应用层防火墙、数据库审计等，形成纵深防御，提高系统的整体安全性。

（3）应急响应机制。建立应急响应机制，包括安全事件响应流程、人员培训和演练，确保在发生安全事件时，能够迅速响应，将损失降至最低。

通过实施上述安全性增强与风险防控措施，可以显著提升大规模替换信创操作系统的安全性，确保业务的连续性和稳定性，为信创操作系统的广泛应用奠定坚实的基础。这不仅有助于提升国家的信息安全水平，还是推动信创产业健康发展的重要保障。

3 替换实施案例与效果评价

3.1 关键行业替换实践

在信创操作系统的大规模替换实践中，关键行业成为探索与应用的前沿阵地[6]。这些行业包括政府、金融、电信、能源和教育等，它们对系统的稳定性、安全性和业务连续性有着极高的要求，因此其替换实践具有重要示范意义和研究价值。

3.1.1 政府机构的替换实践

政府机构作为信创操作系统的首批用户，其替换实践具有标杆作用。以某省级政府为例，该政府在推进信创操作系统替换过程中，首先进行了全面的业务系统评估，识别了关键业务流程和应用软件。其次，构建了测试环境，进行了多轮的系统兼容性和稳定性测试，确保替换后的系统能够平稳运行。最后，在替换过

程中，政府机构还加强了数据安全防护，采用了加密技术、访问控制和数据备份策略，确保了政务数据的安全。通过这一系列的准备和实施，政府机构成功完成了信创操作系统的替换，不仅提升了系统的安全性，还促进了政务流程的优化和效率的提升[7]。

3.1.2 金融行业的替换实践

金融行业因其业务的敏感性和复杂性，对信创操作系统的替换提出了更高的要求。银行、保险和证券等金融机构，在替换过程中重点考虑了系统的交易处理能力和数据安全性。其采用了虚拟化和容器化技术，确保了金融应用在信创操作系统上的稳定运行。同时，金融机构还加强了安全审计和风险防控，实施了全面的入侵检测和防御机制，有效保护了金融数据和客户信息的安全。此外，金融行业还注重用户体验的提升，通过优化用户界面和提供定制化的培训，加快了用户对新操作系统的适应，保证了业务的连续性。

3.1.3 电信行业的替换实践

电信行业作为信息技术服务的关键提供者，其信创操作系统替换实践对整体网络稳定性和服务质量有着重大影响。在替换过程中，电信运营商着重于网络设备的兼容性和系统的高可用性。其引入了冗余设计和故障切换机制，确保了网络服务的连续性。同时，电信行业还加强了网络安全防护，通过实施防火墙、入侵检测系统和加密通信，增强了网络的抗攻击能力。此外，电信运营商还通过建立用户反馈机制，持续优化系统性能，提高了网络服务质量。

3.1.4 能源行业的替换实践

能源行业尤其是电力和石油等关键基础设施，对信创操作系统的替换提出了严格的安全性和稳定性要求。在替换实践中，能源企业注重工业控制系统（ICS）的兼容性和安全性。其采用了定制化的操作系统版本，确保了工业应用的稳定运行。同时，能源行业还加强了现场设备的安全防护，实施了物理隔离和访问控制，有效防止了外部攻击对生产系统的影响。通过这些措施，能源行业成功实现了信创操作系统的替换，不仅提升了系统的安全性，还促进了数字化转型和智能化运维的进展。

3.1.5 教育行业的替换实践

教育行业在信创操作系统替换过程中，重视了教学资源的兼容性和用户体验的提升。学校和教育机构通过建立应用软件适配中心，有效解决了教学软件在新操作系统上的兼容性问题。同时，教育行业还加强了技术支持和用户培训，通过提供在线课程和面对面培训，加快了师生对信创操作系统的适应。此外，教育行业还通过建立软件生态，吸引了更多开发者参与，丰富了教育软件库，提升了教学效率和质量。

通过上述关键行业替换实践的分析可知，信创操作系统的替换不仅消除了操作系统供应链风险，还促进了行业数字化转型和智能化升级。这些实践为信创操作系统的广泛推广和应用提供了宝贵的经验和案例，为我国信息技术发展的自主创新和信息安全保障奠定了坚实的基础。

3.2 实施效果与用户反馈分析

在对关键行业进行信创操作系统的大规模替换后，实施效果的评估与用户反馈分析成为衡量替换方案成功与否的重要标准。通过对政府、金融、电信、能源和教育等领域替换实践的深入研究，可以从系统稳定性、业务连续性、安全性增强以及用户体验提升等多个维度，全面评估替换实施的效果，并分析用户对新操作系统的接受程度和反馈意见。

3.3 系统稳定性与业务连续性

替换实施后，系统稳定性得到了显著提升。关键行业通过采用优化的内核调度策略、自动化监控与故障预测机制以及持续集成与部署的开发模式，有效保障了业务系统的平稳运行。在业务连续性方面，通过实施数据迁移策略、应用兼容性解决方案、测试与验证流程以及应急响应机制[8]，关键行业成功实现了业务的无缝过渡，确保了业务的连续性和数据的安全性。

（1）安全性增强。安全性增强是大规模替换信创操作系统的重要目标。关键行业通过实施数据安全防护策略、系统安全加固措施以及业务安全与连续性的保障机制，显著提升了系统的安全性。加密技术、访问控制、安全配置与补丁管理等措施的应用，有效防止了数据泄露和系统攻击，构建了多层防御体系，为业务安全提供了坚实的保障。

（2）用户体验提升。用户体验是衡量替换成功与否的关键因素。关键行业在替换过程中，注重提升用户的操作便利性和应用兼容性。通过优化用户界面、提供定制化培训、建立应用软件适配中心以及丰富软件库，关键行业有效提升了用户对信创操作系统的接受度和满意度。此外，建立用户反馈机制，收集和分析用户意见，为后续系统优化和升级提供了宝贵的参考。

（3）用户反馈分析。根据用户反馈，信创操作系统在稳定性、安全性和用户体验方面得到了广泛认可。用户普遍反映新操作系统在日常操作中更加流畅，系统响应速度得到了提升。在安全性方面，用户对数据加密、访问控制和入侵检测等功能表示满意，认为这些措施有效保护了业务数据和用户信息的安全。同时，用户对应用软件的兼容性和操作界面的优化表示赞赏，认为这些改进显著提升了工作效率和操作体验。

然而，用户反馈中也提到了一些挑战和改进建议。部分用户反映在替换初期遇到了软件兼容性问题，需要更多的时间和资源进行适配。此外，对于部分非技术背景的用户，系统迁移过程中的操作流程和术语解释需要更加清晰和详细。用户还建议增加更多行业专用软件的支持，以满足特定业务需求。

通过综合评估替换实施效果和深入分析用户反馈，信创操作系统的替换在提升系统稳定性、业务连续性和安全性方面取得了显著成效，同时也促进了用户体验的提升。然而，为了进一步优化替换方案，增强用户满意度，还需要在软件兼容性、操作流程的简化和行业应用支持等方面不断努力和改进。这些反馈和建议将为未来大规模替换提供宝贵的参考，推动信创操作系统向更加成熟和完善的阶段发展。

结语

本文深入探讨了大规模替换信创操作系统的关键技术与策略，通过对关键行业替换实践的案例分析和效果评价，验证了替换方案的可行性和有效性。研究发现，通过保障业务系统连续性、提升系统稳定性和兼容性、增强安全性与风险防控以及重视用户体验提升，信创操作系统的替换不仅能够满足业务需求，确保系统的平稳过渡，还能显著提升系统的安全性，促进用户对新操作系统的接受度。此外，政府、金融、电信、能源和教育等关键行业在替换实践中的成功经验，为信创操作系统的广泛应用提供了宝贵案例，为我国软件行业的自主创新和信息安全保障奠定了坚实基础。

展望未来，信创操作系统的普及和应用将呈现以下趋势。一是技术融合与创新加速。随着 5G、云计算、大数据、人工智能等新技术的融合应用，信创操作系统将面临更多技术挑战和创新机遇，需要在技术兼容性、性能优化、安全策略等方面持续创新，以适应信息技术的快速发展。二是生态建设与应用丰富。为了进一步提升信创操作系统的市场竞争力，必须加强生态建设，吸引更多的软件开发商和独立开发者参与，丰富应用软件库，提升用户满意度，促进信创生态的成熟和繁荣。三是国际合作与标准制定，在全球化的背景下，加强与国际技术社区的交流合作，参与国际标准的制定，将有助于提升信创操作系统的国际影响力，促进技术的开放共享和互操作性。四是人才培养与教育推广，为应对技术迭代和市场变化，需要加大人才培养力度，建立多层次、多领域的培训体系，提高 IT 人才的技能水平，同时加强信创操作系统的教育推广，提升公众对国产操作系统的认知和使用率。总之，未来信创操作系统将不仅服务于国内市场需求，还将走向世界，展示中国信息技术创新的能力和风采。

引用

[1] 王美娟,林美丽,刘如月,等.PK体系对国家信息安全的意义案例研究——以天津海河教育园区南开学校开展信息科技课堂教学为例[J].实验教学与仪器,2023,40(5):119-121.

[2] 林然.操作系统:信创核心环节国产替代空间广阔[J].股市动态分析,2023(5):52-53.

[3] 贾雲博.开源Linux自研操作系统在信创产业中的应用研究[J].产业创新研究,2023(20):93-95.

[4] 贵重,李艳,李云翔,等.国产操作系统发展及分析[J].电信工程技术与标准化,2023,36(6):76-80.

[5] 王继伟,庄培锋,黄榕,等.基于全栈国产化平台的医院信创改造与全场景应用[J].中国数字医学,2024,19(4):17-22.

[6] 李森,刘先群.基于国产操作系统对开源软件编译方法的研究与应用[J].计算机应用文摘,2023,39(11):48-53.

[7] 陈飚,李兴新,侯玉华.面向政企移动办公的信创云手机产品解决方案[J].邮电设计技术,2023(8):5-8.

[8] 王丽芳,武瑞娟,樊彩霞.操作系统中进程同步与互斥思政教学设计[J].计算机时代,2021(6):102-105+109.