 DOI: https://doi.org/10.12345/bdai.v6i1.23359

Analysis of the Current Situation and Countermeasures of Basic Software Supply Chain Security

Li Sun

Shizuoman (Shanghai) Medical Equipment Co., Ltd., Shanghai, 201108, China

Abstract

Basic software is not only the foundation for maintaining high-speed and smooth operation of computer systems, but also directly determines the level of digital infrastructure construction. Basic software, represented mainly by operating systems, databases, and middleware, forms an upstream industrial chain that directly affects downstream output scale and product efficiency. Basic software often has a long development cycle and requires significant investment. In the context of increasingly complex software supply chains, it is receiving more and more attention. At present, China's basic software industry is facing supply chain security risks while developing rapidly. Based on this, this article starts from the current situation of supply chain security and explores rational solutions to provide guarantees for the sustainable development of the basic software industry.

Keywords

basic software; Supply chain; Security status quo; Response strategy

基础软件供应链安全现状与应对策略解析

孙立

士卓曼（上海）医疗器械有限公司，中国·上海 201108

摘　要

基础软件不仅是维持计算机系统高速、平稳运行的基础，还直接决定数字化基础设施的建设水平。基础软件以操作系统、数据库和中间件为主要代表，形成上游产业链，直接影响下游产出规模和产品效益。基础软件往往研发周期较长，投入资金也较大，在软件供应链日益复杂的背景下，受到越来越多的关注。现阶段，我国的基础软件产业在快速发展的同时面临着供应链安全风险问题。基于此，本文从供应链安全现状出发，探究合理化的解决策略，以期为基础软件产业的可持续发展提供保障。

关键词

基础软件；供应链；安全现状；应对策略

1 引言

随着科学信息技术的不断发展，数字化时代到来，基础软件的安全问题不仅影响着人们的日常生活，对社会的平稳运行也具有关键影响。全球范围内软件供应链安全事件频发，以美国为首的多个国家进行技术垄断，导致全球软件供应链体系的不稳定性。基础软件是信息系统的核心组件，同时也是维持信息系统安全的关键，涵盖了操作系统、数据库、中间件、办公软件等多个方面 [1]。在软件供应链复杂化背景下，基础软件的发展受到越来越多国家的重视，基础软件的安全是国家综合实力和竞争力的体现，基础软件的供应链安全直接与软件产品以及服务的安全性、可靠性和可用性挂钩，同时影响着信息基础设施与网络安全的整体水平。然而现阶段，我国基础软件仍依赖于国外的技术供给，尤其是操作系统和数据库领域受开源软件的影响较深，导致我国基础软件的供应链存在安全风险与隐患。因此，当前软件产业的发展侧重点应需格外注意完善安全发展机制，着力解决现存问题，防范和化解供应链安全风险，提升基础软件开发的质量和水平。

【作者简介】孙立（1981–），男，中国上海人，本科，从事信息技术和数字系统管理研究。

2 基础软件的概念及发展

2.1 概念

基础软件是操作系统、数据库系统、中间件、语言处理系统（包括编译程序、解释程序和汇编程序）和办公软件（包括文字处理、电子表格、幻灯片以及一些初级图片处理程序）的统称。在信息系统中，基础软件起着基础性、平台性的作用，应用广泛并影响着信息安全。

2.2 发展

基础软件随着计算机和信息技术的发展而发展，早在

上世纪三四十年代数学家们便提出了计算机理论，1946 年出现了第一台电子计算机，其以 CPU 为中心，使用机器语言，但速度较慢、容量较小，停留在简单的数值计算。早期的程序控制是通过打孔纸袋编程，二十世纪 50 至 60 年代，编程语言才得以进一步发展，机器语言、汇编语言以及 Fortran 等高级语言的出现使得编程更加容易和高效。二十世纪 60 至 70 年代，操作系统和数据库出现，典型的操作系统有 FMS（FORTRAN Monitor System）和 IBSYS，为计算机提供了基本的管理和控制功能 [2]。第一个数据库管理系统是由通用电气公司开发的，为数据的存储、检索和管理奠定了基础。随着软件数量和需求增加，软件面临着开发与维护危机。1968 年，北大西洋公约组织的计算机科学家提出了“软件工程”的概念，旨在用系统化、规范化、数量化等工程原则和方法去进行软件的开发和维护。20 世纪 80 年代至今，中间件和办公软件兴起，随着应用软件需要在各种平台之间进行移植或支持多种应用系统，中间件应运而生，为软、硬件平台和应用系统之间提供可靠和高效的数据传递或转换；办公软件包括文字处理、电子表格、幻灯片以及初级图片处理程序等，办公软件的发展为人们的工作学习提供了诸多便利。

总而言之，基础软件的发展与时俱进，会随着计算机和信息技术的发展而不断发展，从早期编程语言到操作系统、数据库、中间件、办公软件的兴起，基础软件的功能越来越全面，对于信息系统的作用越来越重要。

3 基础软件供应链安全现状

3.1 发达国家技术封锁，基础软件供应链面临挑战

现阶段发达国家实行技术封锁，不断强化数字鸿沟，封锁范围逐步扩展，不仅仅是高技术领域的封锁，基础研究领域也面临着越来越严重的封锁态势。尤其是以美国为首的发达国家，凭借其自身的信息技术优势，相继出台了一系列政策法规，对基础软硬件产品、技术等进行管制，严重影响基础软件供应链的完整性，严重威胁发展中国家的发展。因此，实现关键技术的自主可控是确保供应链安全的根本途径，只有具备自主创新能力并掌握核心技术，才能更好地地维护基础软件供应链安全。从国家层面而言，软件供应链的安全风险问题备受重视。为有效应对国内外软件供应链的安全挑战，近年来我国制定了一系列政策法规，旨在强化软件供应链的安全保障措施。例如，2020 年 10 月发布的《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》中，全面规划了“提升产业链供应链现代化水平”的任务，强调要坚持自主可控、安全高效的原则，针对不同行业制定供应链战略并进行精准施策，以推动全产业链的优化与升级 [3]。

3.2 开源模式渗透，基础软件源代码安全风险凸显

现阶段，GitHub、SourceForge 等代码托管平台已成为开发者首选的源代码共享平台。随着开源模式的不断发展，大多开发人员在接到研发任务时，往往会首先在共享平台上寻找功能相似或相近的代码，为研发工作提供参考。开源模式成为大势所趋，我国基础软件的发展也依赖于开源软件，但是，开源软件具有两面性，既具备开放、共同参与和自由传播的优点，同时又隐藏着安全隐患。安全隐患的产生可能与开源软件开发者的疏忽相关，也可能与恶意植入相关，更有一些恶意攻击者会制造含有隐蔽恶意功能的开源软件，并故意上传到代码托管平台，企图诱使软件研发人员使用这些带有恶意功能的软件。安全隐患的存在大大增加了基础软件供应链安全风险。与商业软件不同，开源软件在发现漏洞后，通常采用人工安装补丁的被动“拉取模式”[4]。如果基础软件的研发人员不定期对所使用的开源代码进行检查，那么这些安全隐患就会一直潜藏在基础软件的源代码之中。以数据库领域为例，MySQL 和 Oracle 是主流产品。然而，国内开发者中，仅有 7% 专注于数据库内核开发，而半数以上主要致力于业务开发。部分国产数据库产品通过吸收并二次开发国外 MySQL、PostgreSQL 等开源技术，存在“长期依赖进口，自主研发能力不足”的问题。据国家信息安全漏洞共享平台的数据显示，数据库领域共有 3031 条安全漏洞，其中开源数据库 MySQL 的安全漏洞占比高达 47.6%，位居榜首，这无疑进一步加剧了国产数据库产品的安全风险。

3.3 缺乏健全完善的供应链安全管理制度，进一步加剧供应链安全

当前，供应链安全标准在国内外均涵盖了供应链生命周期安全以及安全风险两大方面。从供应方和需求方两个视角出发，对供应链生命周期安全分别设定了安全要求，供应方需在软件产品或服务的开发、交付、运维等核心环节实施供应链安全管理，需求方则需要根据现有管理制度，进一步明确供应链管理制度的要求，构建供应商名录，并强化对采购环节的管理。 安全风险主要包括恶意篡改、仿冒伪造、供应中断、信息泄露、安全漏洞及其他安全威胁等六类。为了强化供应链安全管理，国内外已制定了一系列相关标准。举例来说，国外有 ISO/IEC 27036《信息技术安全技术供应商关系的信息安全》系列标准、ISO 28000《供应链安全管理体系规范》系列标准等；国内则有 GB/T 36637—2018《信息安全技术 ICT 供应链安全风险管理指南》、GB/T 32921—2016《信息安全技术信息技术产品供应方行为安全准则》等标准。同时，我国也正在修订与 ISO 28000 等同采用的国家标准《供应链安全管理体系 ISO 28000 实施指南》，旨在为基础软件企业自身的供应链安全管理提供指导 [5]。尽管市面上已有安证通、清科万道等商用的软件供应链安全管理平台，提供事前预防、事中处理、事后监测等安全管理机制，但部分基础软件企业在供应链安全管理上仍面临一些问题。首要问题是缺乏健全的供应链管理制度或体系，对产品开发、交付、运维等关键环节缺乏有效的管理手段。其次，

缺乏全面的供应商安全等级评估体系，导致供应链透明度不足，难以根据安全风险对所有供应商进行安全等级划分和精细化管理。此外，对开源代码安全性的重视不足，部分企业开源代码管理机制不完善，在开发过程中随意使用开源组件的现象较为普遍，进一步加剧了供应链管控安全风险。

4 基础软件供应链安全应对策略

4.1 健全完善法规政策制度和供应链安全管理长效机制

相关主管部门应加强对基础软件供应链的安全监管力度，健全完善相关的法规制度，强化顶层规划和宏观指导，明确基础软件供应链的发展方向和策略，同时，鼓励地方政府出台相应的政策措施，为基础软件供应链的安全应对工作提供资金和政策支持，并加强对行业内重点企业及基础软件供应商的供应链安全检查。为促进基础软件供应链的安全发展，需要建立国家级或者行业级的安全风险分析平台，以激励国内科研机构和软件企业及时报告基础软件面临的威胁与问题，加强风险信息的共享。此外，鼓励并支持第三方测评机构、企业及高校等研发针对基础软件供应链安全风险的评测标准，明确评测的具体维度与科学方法，并积极推动团体标准、行业标准的制定与广泛宣传[6]。最后，还需要加强对基础软件各环节的指导和规范化管理，引导基础软件企业优化安全管理措施，构建详尽的软件物料清单，确保用户能够清晰掌握所采购应用中的组件构成，从而精准识别与解决安全与合规问题，为基础软件供应链的安全发展提供坚实保障。

4.2 提升产品质量与技术水平，弥补供应链安全风险缺陷

软件产品服务提供商需要增强安全责任意识，对软件供应链安全管理进行系统性规划，梳理并整合产品中应用的开源软件及组件，实现统一高效管理。基础软件供应商应在企业内部构建健全的软件供应链管理架构，设立产品风险管控与漏洞响应体系，并制定相应管理规范，为软件供应链的分析、管理、审计及修复工作提供内部指导和支持。应侧重于产品安全开发的全流程，为每一环节设置安全保障措施，并主动实施全生命周期的风险审查与评估，以有效预防许可证争议、供应中断等风险。同时，应积极开展基础软件组件分析以及缺陷智能检测技术的研发，力求突破软件供应链安全状态检测技术的效率与准确性瓶颈。此外，需不断强化研发与管理团队的培训，持续提升团队的专业能力和产品质量。同时加大关键核心技术的自主研发投入，严格控制自主开发代码的质量，以提升基础软件产品的自主可控能力。

4.3 提升用户单位基础软件安全意识，降低安全风险问题

用户单位需要加强对基础软件代码安全重要性的认识，持续监测基础软件及供应链使用情况，编制详尽的基础软件资产清单，并严格规范软件的安装、升级、使用及卸载等全生命周期管理环节。同时，用户单位应构建供应商审核机制，强化对供应商产品的安全审核，对所使用产品的供应链安全水平进行全面评估。在采购商用软件过程中，用户单位应与供应商签署协议，明确要求其提供涵盖开源组件在内的第三方组件清单，以此确保产品来源的可靠性，并尽可能降低许可证纠纷及供应中断的风险。此外，还需构建一个涵盖事前预防、事中监控、事后处置的基础软件供应链安全防护体系，增强对基础软件供应链安全事件的防范、检测及应对能力，防止安全事件带来严重后果[7]。同时，用户单位还需及时关注并更新厂商发布的升级或补丁信息，防止因升级滞后而产生安全缺陷被恶意使用的风险。

4.4 运用加密技术，强化基础软件供应链安全防护

在基础软件供应链安全的发展进程中，科技化的信息加密与身份验证技术对于供应链安全具有至关重要的作用，不仅能够提升用户信任度，还能有效保障软件数据的安全，为各行业的技术创新提供有力支撑。同时为适应当前的发展环境，需要更新安全理念，实现加密技术在数据传输中的应用，可以采用密文形式对数据进行加密，从而有效防止信息外泄，保护整个基础软件供应链的相关数据安全。通过身份验证，还可以防止未授权的访问，结合行为、环境等多方因素，实现智能化的验证机制。

5 结语

近年来，基础软件供应链安全问题越来越受到重视和广泛关注，就基础软件供应链安全现状来说，其不仅受到国外技术垄断的影响，还受到自身缺乏健全管理制度的约束。基于现存风险挑战，需要从政策制度、产品质量、技术创新、用户单位、加密技术等多个方面采取安全应对，针对基础软件供应链的安全现状，采取相应的应对策略，进一步为我国基础软件供应链的安全发展提供保障。

参考文献

[1] 张蕾,闻书韵.基础软件供应链安全现状分析与对策建议[J].信息安全研究,2024,10(8):780-784.

[2] 叶剑飞,冯承基,王晓周,等.基础电信企业软件供应链安全风险识别与技术研究[J]. 电信工程技术与标准化,2024,37(2):16-19.

[3] 李祉岐,郭晨萌,汤文玉,等.关键信息基础设施软件供应链风险分析及应对方法研究[J].信息安全研究,2024,10(9):833-839.

[4] 何跃鹰,刘中金,邢燕祯,等.加强软件供应链安全实践,提升关键信息基础设施韧性[J].中国信息安全,2024(7):16-21.

[5] 洪晟,易哲凯.开源软件供应链安全展望[J].工业信息安全,2024(1):13-18.

[6] 毛天宇,王星宇,常瑞,等.面向Java语言生态的软件供应链安全分析技术[J]. 软件学报,2023,34(6):2628-2640.

[7] 零家勇.勒索软件攻击冲击下的软件供应链安全风险分析[J].网络安全和信息化,2022(12):117-119.