面向信息系统的 ICT 供应链保护策略研究

张 恒
公安部第三研究所 北京 100000

摘 要：在全球数字化转型不断加速的背景下，信息通信技术（ICT）供应链的安全性已成为影响国家安全、社会稳定和企业持续发展的关键因素。近年来，供应链攻击呈现出从单点渗透到全链条渗透的趋势，攻击目标涵盖软件、硬件及服务的全生命周期环节。本文以信息系统为研究对象，分析 ICT 供应链在开发、采购、获取、交付、运维及废止等阶段可能面临的安全风险，提出了一套面向信息系统的 ICT 供应链全生命周期保护策略。

关键词：信息通信技术；供应链；供应链攻击；全生命周期；保护策略

引言

近年来，全球 ICT 产业链高度全球化与分工协作的特征愈发显著，信息系统所依赖的软件、硬件、服务往往跨越多个国家与地区。这种复杂的供应链结构虽然带来了高效的资源整合与成本优势，但也引入了多层次、多源异构的安全风险。供应链攻击已从传统的“单点突破”转向“多点协同、全链条渗透”，攻击者可能通过植入恶意代码、利用第三方组件漏洞、篡改更新包等方式，在 ICT 供应链的多个环节发起攻击，威胁信息系统的安全可控性。

自 2009 年起，我国先后发布一系列 ICT 供应链安全管理相关国家标准，包括供应链风险管理指南、ICT 供应链安全风险管理指南和代码安全审计规范等，明确供应链风险管理过程、风险评分评价方法、ICT 供应链全生命周期风险识别流程及内容[1]。《中华人民共和国网络安全法》、《网络产品和服务安全审查办法》、《关键信息基础设施安全保护条例》等法律法规对 ICT 供应链安全提出了明确要求。GB/T 43698–2024《网络安全技术 软件供应链安全要求》、GB/T 36637–2018《信息安全技术 ICT 供应链安全风险管理指南》等国家标准，则从技术和管理的角度对供应链安全进行了细化规范。然而，在实际运行中，信息系统仍面临供应商管理不规范、组件来源不可控、全生命周期防护不足等问题，特别是在开源组件安全检测、供应商合规审查、废止阶段数据销毁等环节存在薄弱点。

为应对上述挑战，本文面向信息系统的供应链安全保护实践，提出了一套覆盖组织管理与技术管理的 ICT 供应链全生命周期保护策略，旨在为信息系统 ICT 供应链安全保护提供可借鉴的实施路径。

1 ICT 供应链安全风险与挑战

随着信息系统的不断发展，ICT 供应链的复杂性和依赖性也日益增加。这使得其面临多重安全风险和挑战，影响系统的稳定性和可靠性。具体而言，主要包括以下几个方面：

1.1 网络攻击的复杂性

网络攻击者的手段日益复杂，以往传统的“单点渗透”模式已演变为覆盖整个供应链的立体化攻击。从核心供应商到二级及三级供应商，攻击者可以通过植入恶意软件、利用 API 漏洞等手段，实现一次入侵全网扩散的效果。这些复杂的攻击模式不仅增加了防范和检测的难度，也使得信息系统的整体安全风险加大。

1.2 多层次供应关系的脆弱性

ICT 供应链通常由多个供应商组成，层次结构复杂，且供应商的资质与能力参差不齐。多层次的供应关系使得建立有效的风险管理体系变得更加困难。对于二级和三级供应商的潜在风险，过往的审查和认证体系可能无法及时识别和预警，导致潜在的安全隐患未能被充分管控。

1.3 隐蔽的安全漏洞与合规风险

软件开发中，特别是使用开源组件时，常常会引入未被发现的安全漏洞。根据统计，84% 的代码库含有漏洞，可能引发重大安全事件[2]。此外，不同的开源组件所遵循的许可证也可能导致合规性风险，若未能妥善管理可能会引发法律诉讼和经济损失。

1.4 供应链中断的风险

自然灾害、政治冲突和经济制裁等因素可能导致供应

链中断，进而影响到信息系统的可用性和服务连续性。供应链中断不仅影响企业的生产运营，还可能导致业务损失。

2 面向信息系统的 ICT 供应链保护总体框架设计

本章节将面向信息系统供应链安全建设，提出一套全面的 ICT 供应链保护总体框架，旨在提升信息系统 ICT 供应链的安全性与可靠性。

2.1 建设总体框架

ICT 供应链保护的总体框架涵盖从供应链的组织管理到技术管理，形成系统的安全防护体系。首先，组织管理涉及到安全管理职责的明确、人员的安全意识培训及供应商的管理。其次，技术管理则通过技术手段辅助 ICT 供应链各关键环节的技术验证以及自动化管理，通过管理和技术加强对开发、采购、获取、交付、运维及废止等各个环节的安全控制。

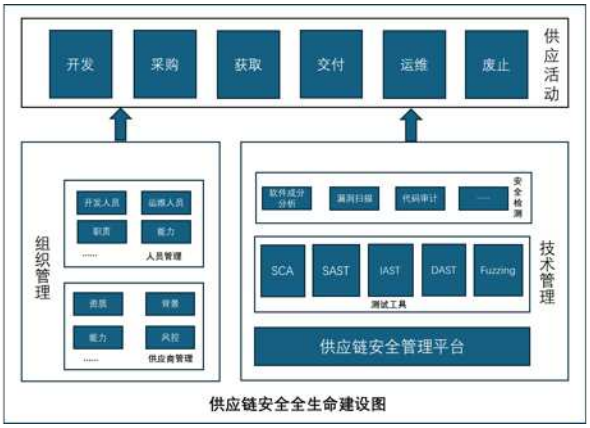

图 1 ICT 供应链安全建设架构图

2.2 组织管理建设

有效的组织管理是 ICT 供应链保护的基础。在人员管理方面，企业应定期组织供应链安全意识教育培训，增强全员的安全意识，使其能够及时识别和应对潜在的安全威胁。同时明确安全管理职责，确保各个环节的安全监管落实到位。通过建立合格的供应商目录，可以确保所选供应商在安全性、合规性方面的可靠性。对供应商的资质进行严格审核、定期评估及绩效评分，实现对供应商安全能力的动态管理，能显著降低潜在的安全风险。

2.3 技术管理建设

技术管理在于实施全面的检测和分析工作，以确保信息系统供应链的安全。在这一环节，企业应利用多种现代技术手段，建立并部署一系列针对采购产品和软件的检测工具，包括软件成分分析（SCA）、静态应用安全测试（SAST）、交互式应用安全测试（IAST）、动态应用安全测试（DAST）和模糊测试（Fuzzing）。这些工具能有效地识别潜在的安全漏洞并对代码质量进行评估。

在技术管理的框架下，可搭建一套供应链安全管理平台。该平台能够形成全面的供应链资产管理系统，展示供应链安全资产清单，从而识别和预警相关的风险。平台应具备供应链风险管理、资产跟踪、以及对供应链安全风险的管理功能，使得企业可以全面掌握供应链中各个环节的安全状态。

3 ICT 供应链全生命周期保护策略

本文将围绕 ICT 供应链的全生命周期，提出系统性的安全保护策略。这些策略涵盖从开发、采购、获取、交付到运维和废止的各个环节，确保信息系统始终处于可控、安全的状态。

3.1 整体保护策略

整体保护策略是保障 ICT 供应链全生命周期安全的基础，主要包括以下三部分内容：

3.1.1 开展 ICT 供应链安全风险评估

通过识别和分析潜在的安全风险、脆弱点和威胁源，评估现有控制措施的有效性，并提出改进建议。检测评估过程应包括对各个供应链环节的相关标准和政策的审查，确保识别与企业系统和环境相关的具体威胁。定期评估将有助于企业及时掌握供应链的安全现状并做出相应的调整。

3.1.2 供应链安全管理

供应链安全管理是维护 ICT 供应链整体安全性的重要环节，可以结合供应链安全管理平台实现以下几个方面的管理：

1. 构建供应链清单

企业应建立完整的供应链资产清单，记录所有关键的软硬件资产、第三方组件及相关服务。这一清单应详细列出每个资产的来源、功能、风险等级及合规性要求。通过清单管理，企业能够清晰识别哪些资产为关键资产，哪些资产存在更高的风险，从而制定相应的管理对策确保整体安全。

2. 供应链风险管理

结合供应链安全风险评估结果与安全检测的成果，实施有效的漏洞管理。这包括识别当前产品中存在的高风险组件与已知安全漏洞的数量；根据这些信息制定应对策略，以降低潜在风险。此外，企业也必须关注在供应链安全方面面临的合规风险和其他安全威胁，例如，如何满足相关法律法

规的要求、对外部审计的响应能力等。通过这些管理措施，企业能够有效减少漏洞对供应链安全的影响，并提升整体安全水平。

3.1.3 建立供应商安全管理体系

分类筛选合格的供应商，并对其资质进行定期审核，包括背景调查、资质认证和履约能力评估。对供应商的管理包括对其提供的产品与服务的安全性及合规性进行评估，确保其能够持续满足企业的安全要求。此外，也要考虑建立供应商更替预案，以防止受单一供应商的安全风险影响，从而保障供应链的稳定性。

3.2 供应活动保护策略

3.2.1 开发过程保护策略

构建安全开发的基线要求，明确开发环境的配置、密码策略、访问权限及审计日志管理等内容。对开发人员进行定期的安全意识培训，使其能够识别潜在的安全威胁非常重要。在实际开发中，应制定相关的安全编码规范，并严格执行代码审查与测试流程。利用静态应用安全测试 (SAST) 和动态应用安全测试 (DAST) 工具，对代码进行全面审核，以便尽早发现并修复潜在漏洞。

同时，建立软件物料清单（SBOM），通过记录所使用的每一个组件的版本、来源及相关安全信息，为后续的安全管理奠定基础。使用代码审查工具以及开源组件登记工具，确保所有需用的开源组件都是经过审核的，并符合相应的安全及合规要求。

3.2.2 采购过程保护策略

在采购流程中，要建立一套详细的安全需求基线，明确采购产品的安全性、性能等基本要求。同时，注重供应商的合规性，这包括对其背景、资质证书、历史表现等方面的评估，以确保其能够满足企业的安全要求。

在采购执行阶段，邀请网络安全领域的专家参与招标过程，有助于提高识别潜在风险的能力。对供应商提供的产品进行安全审查，确保不存在恶意代码或高危漏洞。在评估时，企业可借助综合监测工具与技术手段，对供应商所提供的产品进行系统性的风险评估。

3.2.3 获取过程保护策略

产品获取环节，所有从供应商处获取的软件或组件，应通过官方渠道进行，不得通过非正规途径获得。采用 HTTPS、SFTP 等安全协议进行加密流量传输，以防止数据在下载过程中遭到篡改或窃取。获得安装包后，应先进行完整性校验与数字签名验证，确保其未被恶意修改。

获取过程可结合软件成分分析 (SCA) 工具及其他安全检测技术，实施全面的安全扫描和漏洞检测，以确保引入的组件和软件均是安全的，避免高风险问题被引入系统。

3.2.4 交付过程保护策略

供需双方的角色不是一成不变，当企业开发产品作为供应产品交付时，不仅需要准备所有必要的技术文档，还应确保交付的合规性，遵循保密协议，以保护用户的敏感数据和知识产权。交付的产品应附带经过审核的版本和技术规格，确保其在安全性上能够符合预期的要求。

在交付过程中与用户保持密切沟通，确认交付的内容与技术方案是否符合用户要求。确保用户能够接受技术培训，使其充分理解产品的安全配置和操作规范，降低因操作不当导致的安全风险。

3.2.5 运维过程保护策略

在运维阶段，应建立一套完善的监控机制，通过日志审计工具和实时监控系统，对运维操作进行全面的记录和分析。确保能够第一时间发现安全事件，并及时启动应急预案进行处理。

借助安全信息和事件管理 (SIEM) 系统，可以实现对各类安全事件的集中管理和分析，提升对潜在安全威胁的预警能力。运维团队还需定期对系统进行安全性回顾和漏洞扫描，进行必要的补丁更新，以保障系统始终处于安全可控的状态。

3.2.6 废止过程保护策略

在产品生命周期末期，明确的废止策略，确保不再使用的软件或组件及时停用，并彻底从系统中卸载。对已废止的数据和设备进行合规的数据销毁，采用专业的工具和流程，确保敏感数据无法被恢复。

为保障透明性和可追溯性，应记录各项废止操作的详细信息，并制定监督措施，确保废止过程中的每一步都受到审查，从而最大限度地降低安全风险。

4. 结论与展望

本文围绕 ICT 供应链的安全保护问题，从全生命周期的角度提出了系统性的保护策略。通过深入分析 ICT 供应链开发、采购、获取、交付、运维和废止各环节的安全风险，制定了相应的防护措施，以加强信息系统的安全性与可靠性。

有效的组织管理和技术管理相结合，确保各项安全策略能够落地实施，实现对 ICT 供应链的全方位监控与管理。

展望未来，随着技术的不断进步和网络安全威胁形态的演变，ICT 供应链的安全保护将面临更加复杂的挑战。企业需要持续关注新兴安全风险，灵活调整保护策略，结合先进的安全技术与管理手段，维护信息系统 ICT 供应链的安全性。同时，加强跨行业、跨领域的合作，形成合力，共同应对 ICT 供应链的安全挑战，为构建安全、可信的信息环境奠定基础。

参考文献：

[1] 何熙巽 , 张玉清 , 刘奇旭 . 软件供应链安全综述 [J/OL]. 信息安全学报 , 2020, 5(1): 57–73.

[2] 纪守领 , 王琴应 , 陈安莹 , 等 . 开源软件供应链安全研究综述 [J/OL]. 软件学报 , 2023, 34(3): 1330–1364.

[3] 王晓周 , 叶剑飞 , 张俊 , 等 . 电信运营商 ICT 供应链安全风险评估方法研究 [J]. 数字通信世界 , 2025(5): 194–196.

[4] 王博 , 吴舟婷 , 吴倩 , 等 . 关键信息基础设施 ICT 供应链安全风险评估指标体系研究 [J]. 信息安全与通信保密 , 2020(12): 103–111.

[5] 陈丽娜 , 廖璇 , 董国豪 , 等 . 基于供应链第三方开源组件的风险与挑战研究 [J]. 软件 , 2025, 46(1): 53–55.

[6] 张熙 , 颉夏青 . 全球 ICT 供应链视角下的安全风险 [J]. 中国网信 , 2024(11): 60–63.

[7] 朱丽璇 . 铁路信息系统供应链安全风险管理刍议 [J]. 铁路计算机应用 , 2023, 32(11): 56–62.

[8] 王佳硕 , 程建宁 , 周天成 . 新形势下通信运营企业 ICT 供应链安全分析及对策 [J]. 中国招标 , 2022(11): 70–74.

[9] 上官晓丽 , 孙彦 , 李彦峰 . 信息通信技术供应链安全政策法规与标准研究 [J]. 中国信息安全 , 2021(10): 43–46.

[10] 杨璐 , 刘家祺 , 卢春阳 . 信息通信行业绿色供应链管理研究 [J]. 信息通信技术与政策 , 2025, 51(5): 80–84.

[11] 刘秋月 , 刘佳良 . 云服务供应链安全研究及建议 [J]. 通信管理与技术 , 2024(1): 7–9.

[12] 周鑫红 . 中美博弈对中国 ICT 产业链韧性的影响研究 [D/OL]. 吉林大学 , 2025. https://link.cnki.net/doi/10.27162/d.cnki.gjlin.2025.000003.

[13]MIN S hyun, SON K ho. Comparative Analysis on ICT Supply Chain Security Standards and Framework[J/OL]. Journal of the Korea Institute of Information Security & Cryptology, 2020, 30(6): 1189–1206.

[14] 徐海 , 钟书棋 , 胡宁 , 等 . ICT 供应链安全风险研究及建议 [J]. 电子产品可靠性与环境试验 , 2024, 42(4): 124–128.

[15] 丰诗朵 , 高婧杰 , 李慎之 , 等 . ICT 供应链安全制度演进趋势研究 [J]. 信息通信技术与政策 , 2023, 49(2): 49–53.

[16] 何佳佳 , 李庭辉 . ICT 贸易依赖网络结构的演化特征及影响因素研究 [J/OL]. 统计研究 , 2025, 42(5): 62–76.

[17] 蒋小娟 , 黄亮 , 唐双林 . ICT 行业供应链安全风险管理与应对机制 [J]. 招标采购管理 , 2025(3): 58–60.

[18]VAN DER VORST J, BEULENS A, VAN BEEK P. Innovations in logistics and ICT in food supply chain networks[M/OL]//JONGEN W M F, MEULENBERG M T G. Innovation in agri-food systems. Brill | Wageningen Academic, 2005: 245–292[2025–08–03]. https://brill.com/view/book/9789086866663/BP000011.xml.

[19]LU T, GUO X, XU B, 等 . Next Big Thing in Big Data: The Security of the ICT Supply Chain[C/OL]//2013 International Conference on Social Computing. Alexandria, VA, USA: IEEE, 2013: 1066–1073[2025–08–03]. http://ieeexplore.ieee.org/document/6693469/.

[20]JAGDEEP SINGH, SHIVOHAM SINGH, KUMARI M. Role of ICT in Supply Chain Management[J/OL]. 2020[2025–08–03].http://rgdoi.net/10.13140/RG.2.2.29744.58881.

[21]DIMITROV W, NOVAKOVA G. Security in the Supply Chain of ICT Companies[J]. 2016.

[22]HAMMI B, ZEADALLY S, NEBHEN J. Security Threats, Countermeasures, and Challenges of Digital Supply Chains[J/OL]. ACM Computing Surveys, 2023, 55(14s): 1–40.

[23]ABDULLAHI H O, MOHAMUD I H. The Impact of ICT on Supply Chain Management Efficiency and Effectiveness: A Literature Review[J/OL]. Journal Europ é en des Syst è mes Automatis é s, 2023, 56(2): 309–315.