网络安全 FCIS 2023 创新大会

供应链安全管理模式探索与发展

公安部第三研究所　网络安全技术研发中心　陈晓霖

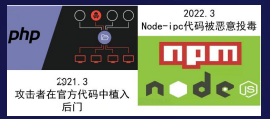
FREEBUF

供应链安全总体发展形势

随着开源技术应用、国际形势复杂、企业软硬件供应链的多样化，供应链各个环节的攻击事件数量急剧上升，已然成为企业乃至国家网络安全主要威胁。

世界各地出现了越来越多的针对不同国家公共和私人企业机构的**供应链攻击**。供应链攻击使得传统漏洞攻击获得了**“链式反应”**，呈现出网状蔓延的态势，放大了传统网络攻击效果。

直接引用该组件的开源软件仅有**6700多**个，但是**间接引用**的开源软件**超过17万**，近70%的企业线上业务系统受到影响。



供应链的发展为**供应链“投毒”**提供了便利，也使得**“预置后门”**变得明目张胆，这其中既有供应商、开发者的**自主行为**，也有供应链被劫持后代码被篡改的**被动行为**。

供应链环节的**断供、停服、封禁**等现象供应链断供行为在战时场景下尤为突出，并能够取得显著效果。

近年来供应链典型攻击事件

供应链安全风险典型特征

企业侧供应链安全现状

企业供应链安全涉及众多环节，所面临的网络攻击面大，供需方需要应对更多的安全威胁

190	*平均每个项目引入组件数
55	*平均每个项目缺陷组件数
161	* 平均每个项目存在漏洞数
63%	*项目中存在开源许可证风险

企业供应链建设常见的安全风险

软件依赖进口 源头难以控制

- 关键软件技术方面还无法实现完全自主研发可控
- 从国外引进的技术或软件产品，加大我国软件供应链安全出现威胁的可能性
- 无法摒除软硬件产品内预置后门

开源存在缺陷 易引入安全风险

- 开源技术的高效率已经成为企业的主流选择
- 开放源码组件的广泛应用带来新的安全挑战
- 开发者自身水平不足容易产生软件安全漏洞
- 无法避免恶意人员向开源软件注入木马程序

安全防护不足 缺乏安全意识

- 开发者为了提高效率，实行“业务先行”模式
- 业务逻辑漏洞和第三方开源组件漏洞频发
- 员工在缺乏安全意识的情况下缺少对敏感数据潜在攻击的识别能力

管理制度不完善 安全评估缺失

- 企业软件供应链管理制度不完善，缺乏针对软件生产等重要环节的管控措施
- 部分企业开源代码管理机制尚不完善，随意使用开源组件的现象屡见不鲜

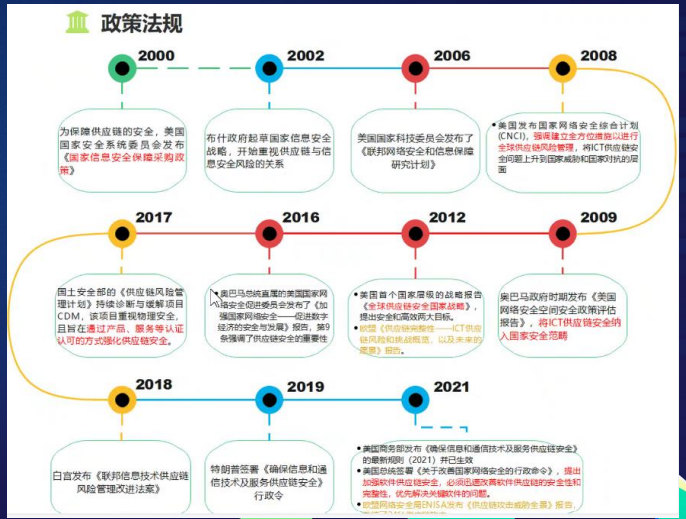
应对全球化高频攻击的国际举措

➢美国、俄罗斯、欧盟等国家和地区将信息通信技术（ICT）供应链保障上升到**国家战略地位**，尤其是美国在法律法规标准制度等方面，形成了较为**完善的供应链安全风险管控体系**。

➢欧盟为了**响应美国供应链安全管理战略**，于2005年通过欧盟海关法修正案，要求货物在抵达欧盟边境前进行货柜**安全信息风险分析管控**，以强化进出口通关安全。

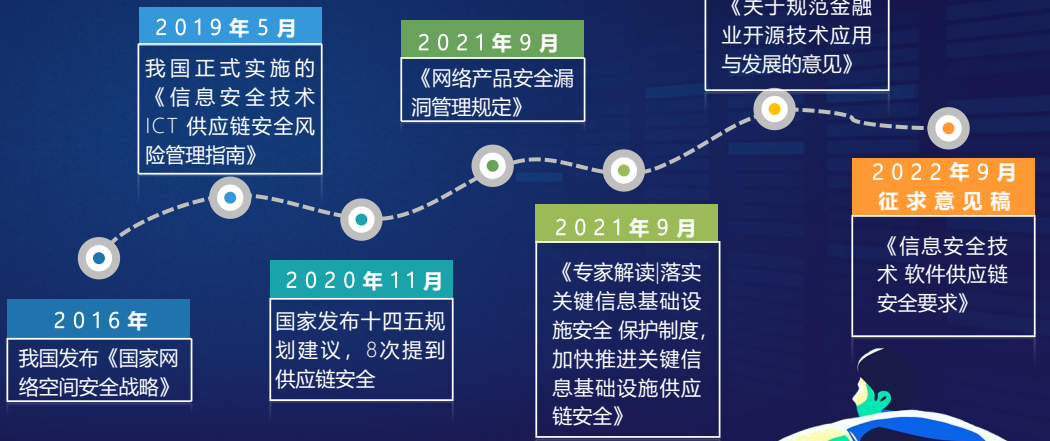
美国国家标准与技术研究院（NIST）

- 政策：CNCI#11 **全方位**方法实施全球供应链**风险管理**
- 计划：ICTSCRM 供应链风险**管理实践开发计划**
- 实施：NISTSP800-161 联邦信息系统和组织供应链风险**管理实践**
- 指南：NISTIR7622 联邦信息系统供应链风险**管理实践理论**



强合规监管深化供应链安全建设鞭子效力

随着供应链各个环节的攻击次数急剧上升，危害急剧加大,国家对供应链安全的**治理力度也在不断增强**。2016年我国在发布的**《国家网络空间安全战略》**中，明确提出“建立实施网络安全审查制度，加强供应链安全管理，提高产品和服务的安全性和可控性。”



供应链安全标准规范指引整体合力逐步形成

我国供应链安全标准战略体系

安全战略

- 2016 年我国发布了《国家网络空间安全战略》中，明确提出“建立实施网络安全审查制度，加强**供应链安全管理**，对**党政机关、重点行业**采购使用的重要信息技术产品和服务**开展安全审查**，提高产品和服务的**安全性**和**可控性**。

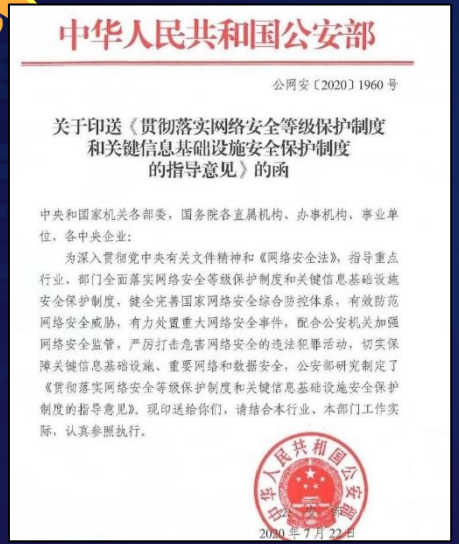
相关标准

- GB/T 24420-2009 供应链风险管理指南
- GB/T 29245-2012 政府部门信息安全管理基本要求
- GB/T 31168-2023 信息安全技术　云计算服务安全能力要求
- GB/T 32921-2016 信息技术产品供应方行为安全准则
- GB/T 22239-2019 信息系统安全等级保护基本要求
- 国标 信息安全技术 信息技术产品供应链安全要求 (即将发布)

实施落地

- 2019 年 5 月 1 日正式实施的 GB/T 36637-2018《信息安全技术 ICT 供应链安全风险管理指南》，在完整性、保密性、可用性、可控性的原则指导下制定的**指南**， 目标使用者包括了 ICT 产品服务的**采购方—— 党政部门、重点行业、关键信息基础设施**。

国家层面：公安部1960号文明确供应链要求



中华人民共和国公安部

公网安〔2020〕1960号

关于印送《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》的函

中央和国家机关各部委，国务院各直属机构、办事机构、事业单位，各中央企业：

为深入贯彻党中央有关文件精神和《网络安全法》，指导重点行业、部门全面落实网络安全等级保护制度和关键信息基础设施安全保护制度，健全完善国家网络安全综合防控体系，有效防范网络安全威胁，有力处置重大网络安全事件，配合公安机关加强网络安全监管，严厉打击危害网络安全的违法犯罪活动，切实保障关键信息基础设施、重要网络和数据安全，公安部研究制定了《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》。现印送给你们，请结合本行业、本部门工作实际，认真参照执行。

2020年7月22日

二、深入贯彻实施国家网络安全等级保护制度

（五）加强供应链安全管理。网络运营者应加强网络关键人员的安全管理，第三级以上网络运营者应对为其提供设计、建设、运维、技术服务的机构和人员加强管理，评估服务过程中可能存在的安全风险，并采取相应的管控措施。网络运营者应加强网络运维管理，因业务需要确需通过互联网远程运维的，应进行评估论证，并采取相应的管控措施。网络运营者应采购、使用符合国家法律法规和有关标准规范要求的网络产品及服务，第三级以上网络运营者应积极应用安全可信的网络产品及服务。

三、建立并实施关键信息基础设施安全保护制度

（五）强化核心岗位人员和产品服务的安全管理。要对专门安全管理机构的负责人和关键岗位人员进行安全背景审查，加强管理。要对关键信息基础设施设计、建设、运行、维护等服务实施安全管理，采购安全可信的网络产品和服务，确保供应链安全。当采购产品和服务可能影响国家安全的，应按照国家有关规定通过安全审查。公安机关加强对关键信息基础设施安全服务机构的安全管理，为运营者开展安全保护工作提供支持。

一线企业供应链安全建设需求

- 开发、运营、服务管控等原生性供应链安全开发需求比重依旧较大。
- 供应链安全、开源治理、供应商风险等新概念被频繁提及，衍生出供应链安全建设新方向

- 目前合规性需求依然占据绝大多数的需求比例。
- 因不合规而导致的安全事件给企业带来的成本损失，是影响企业发展的重要因素。

监管力度对合规性需求的影响

在合规性对企业发展的显著影响下，企业方对监管驱动的合规初步形成共识。

共识

力度

合规性需求的释放，依赖于监管的力度。监管力度越强，合规性需求的释放就越大，相应的市场就越大，这在网络安全市场已经得到很好的验证。

供应链安全建设存在的挑战

各方对监管需求不了解

供应链安全技术有待进一步成熟和完善

供应链安全人才缺口严重

供应链安全建设关注重点

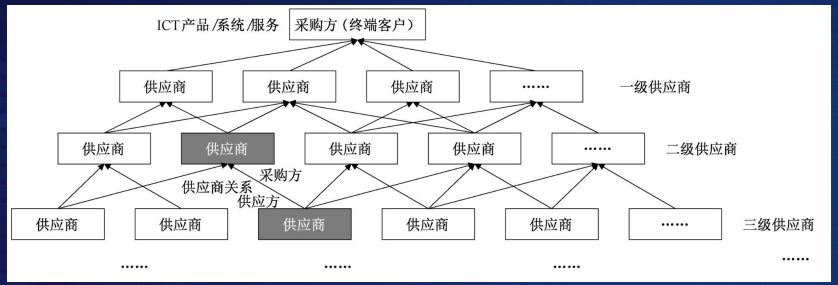
开源软件安全

外购安全产品安全

三方供应商及人员

代码及数据安全

供应链安全防御思路



攻击左移

安全左移

在软件功能、性能、场景等快速发展的同时，复杂的软件供应链会引入一系列的安全问题，导致信息系统的整体安全防护难度越来越大。

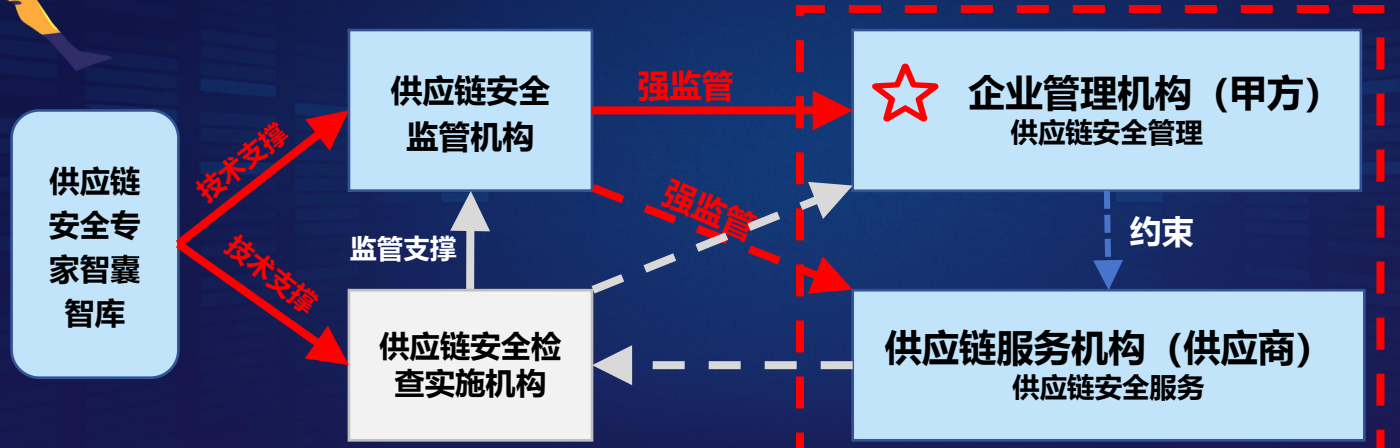
关于如何有效缓解此类安全问题，业内普遍认为应采用安全左移的思路——将安全嵌入至整个软件开发生命周期中。

企业不仅要考虑自身的安全流程，同时还需要仔细审查安装软件的来源及完整性、确认是否可信，了解供应商的安全流程。

供应链安全治理体系


软件供应过程风险治理
软件来源
1.供应商资质
2.开源社区活跃度
软件安全合规
1.软件物料清单
2.软件安全要求
3.软件合规要求
4.安全测试及评审报告
5.安全监护防护
软件资产管理
1.供应链清单管理
2.版本管理
3.漏洞管理
服务支持
1.产品及用户文档
2.服务水平协议
3.信息安全服务协议
安全应急响应
1.应急预案
2.应急响应团队
软件供应商
设计
开发
运营
下线
用户
软件开发生命周期安全风险治理
需求设计
1.安全需求分析
2.安全设计原则
3.确定安全标准
4.攻击面分析
5.安全隐私需求设计知识库等
开发测试
1.安全编码
2.管理开源及第三方组件安全风险
3.变更管理
4.代码安全审查
5.配置审计
6.安全隐私测试
7.漏洞扫描
8.模糊测试
9.渗透测试等
发布运营
1.发布管理
2.安全性检查
3.事件响应计划
4.安全监控
5.安全运营
6.风险评估
7.应急响应
8.升级与变更管理
9.服务与技术支持
10.运营反馈等
下线停用
1.制定服务下线方案与计划
2.明确隐私保护合规方案，确保数据留存符合最小化原则
人员管理
干系人管理
软件供应链任一环节的干系人，包括供应商、管理人员、开发人员、测试人员、运营人员、终端用户等，都应向其传达“安全可让每个个体受益”的理念，以提高其安全意识。
1.培训赋能
2.安全绩效考核
3.最小特权原则
4.零信任原则
5.明确规定安全策略

供应链安全监管治理的合力效应



供应链安全监管要求逐步完善

2022年9月30日
《信息安全技术 软件供应链安全要求》
国标公开征求意见

《信息安全技术 供应链安全工具技术要求与测试评价方法》

《信息安全技术 供应商安全能力要求与测评办法》

可持续的供应安全生态建设之路

供应链安全治理的发展路径：

达标式治理 → 配合式治理 → 自发式治理

制度的不断完善

技术的不断发展

运营的不断健全

供应链安全治理的终极目标：

供应链中的所有角色都应该为其涉及的供应链环节安全负责

网络安全 FCIS 2023创新大会

THANKS

FREEBUF