大数据与决策研究

（政策与技术跟踪专题）

2023 年第 25 期（总第 181 期）

广西壮族自治区信息中心
广西壮族自治区大数据研究院　　2023 年 8 月 14 日

编者按：近年来，针对关键信息基础设施供应链安全的攻击事件频发，如何识别关键信息基础设施供应链安全风险，降低关键信息基础设施供应链安全事件发生概率成为网络安全防护的重要工作。本期将介绍关键信息基础设施供应链安全相关情况。

本期要目

关键信息基础设施供应链安全基本内涵

一、基本内涵

关键信息基础设施是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。关键信息基础设施是国家重要的战略资源，关系国家安全、国计民生和公共利益，具有**基础性、支撑性、全局性**作用，保护关键信息基础设施安全是国家网络安全工作的重中之重。

近期，国内外关键信息基础设施供应链安全事件频发，损害供应链安全，就会损害到关键信息基础设施安全，保障好供应链安全，使关键信息基础设施稳定运行就变得尤为重要。关键信息基础设施供应链安全是一个非常庞大和复杂的概念，主要涉及供应链上下游的相关产品和服务的**生产、仓储、销售、交付、设计、开发、集成、安装、运维**等环节，每一个环节在其全生命周期都会面临安全风险。一旦供应链的某一个环节被破坏，就有可能直接威胁到关键信息基础设施的稳定运行，尤其是在近几年针对操作系统、数据库、行业应用软件、大型工业软件等软件供应链的攻击呈明显上升趋势的背景下，供应链安全保障就成为关键信息基础设施安全防护的重点。

二、评估指标体系

关键信息基础设施供应链目前面临着严峻的安全风险和监管需求，但是尚无统一规范的安全评估指标体系，有学者参考国内外现有标准研究，从指标框架、指标体系、指标释义和实施过程等方面构建一套对关键信息基础设施的 ICT（Information & Communication Technology，信息通信技术）供应链安全的评估指标体系，如下图所示：

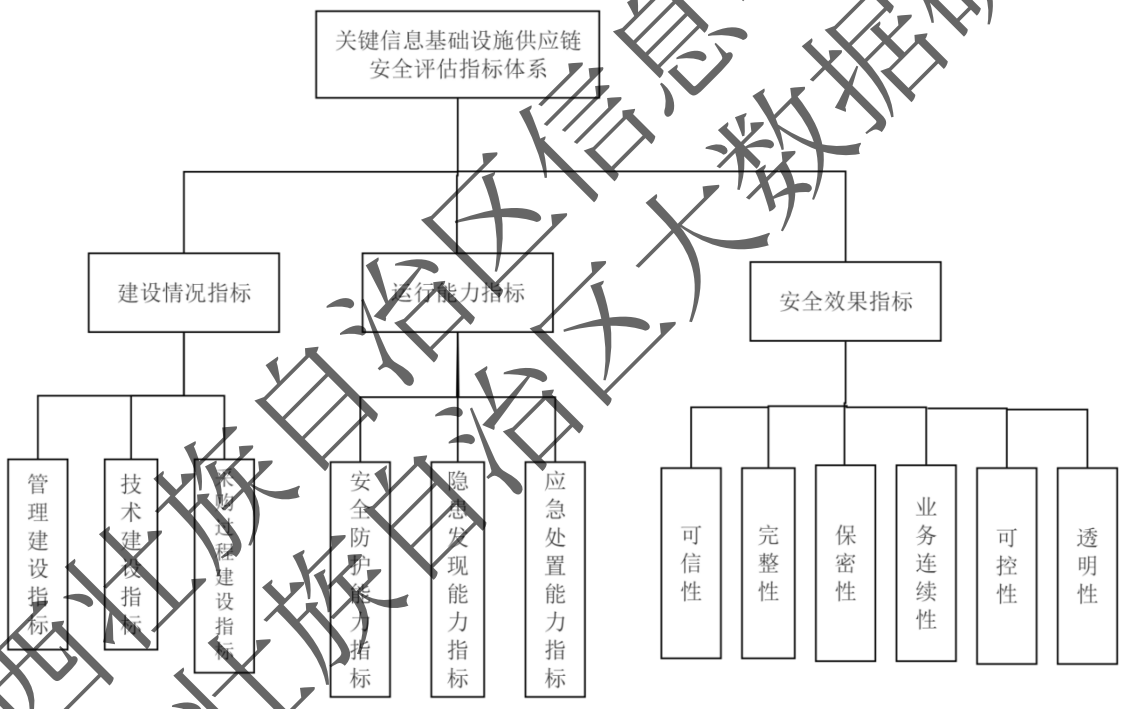

图 1 关键信息基础设施的供应链安全风险评估指标体系

关键信息基础设施的供应链安全风险评估指标体系共有三个层级，其中第一层级指标对应关键信息基础设施建设、运行和安全防护的三个大方面，用建设情况指标评估供应链安全措施；用运行能力指标评估供应链安全能力；用安全效

果指标评估供应链安全程度。二级指标对应在三个大方面中应该考虑的具体元素，三级指标对应具体指导落地实施的评估因素。对于每一个指标，还可以用具体的三级指标来进行衡量，从而得出更加精准的评估结论。

下面给出一个可供参考的关键信息基础设施供应链安全风险评估体系，如表 1 所示，关键信息基础设施 ICT 供应链安全风险评估指标体系包含由 3 个一级指标和 12 个二级指标构成的指标框架以及 45 个三级指标，三级指标为可用于测量的底层指标。

表 1　供应链安全风险评估指标

一级指标	二级指标	三级指标
建设情况指标	管理建设指标	组织机构建设指标
		法律标准建设指标
		基础设施建设指标
		人才队伍建设指标
		教育培训建设指标
		资源投入指标
		开发制造过程指标
		维护过程指标
		退服过程指标
	技术建设指标	物理与环境
		系统与通信
		访问控制
		标识与鉴别
		供应链完整性保护
		可追溯性
	采购过程建设指标	供应商选择指标
		协议过程指标
		交付过程指标

一级指标	二级指标	三级指标
运行能力指标	安全防护能力指标	等级保护测评指标
		网络信任体系指标
		信息安全监控指标
	隐患发现能力指标	风险评估指标
	应急处置能力指标	灾难备份和恢复指标
		事件处置指标
安全效果指标	可信性指标	ICT 供应商组织可信性指标
		ICT 产品和服务可信性指标
	完整性指标	防恶意篡改指标
		防赝品组件指标
		防违规远程控制指标
	保密性指标	防 ICT 供应链敏感数据泄露指标
		防 ICT 供应链敏感数据滥用指标
		防用户信息非法收集处理指标
	业务连续性指标	防突发中断事件效果指标
		防供应商垄断行为效果指标
		防不被支持的系统组件指标
		产品和服务来源的多样性指标
	可控性指标	用户信息可管理性指标
		产品远程控制可管理性指标
		供应链可追溯性指标
		供应商遵守中国法律法规章指标
	透明性指标	产品/服务资料规范完备性指标
		供应链过程信息透明性指标
		用户信息收集和处理透明性指标
		产品远程控制透明性指标
		供应商信息透明性指标

（来源：《关键信息基础设施 ICT 供应链安全风险评估指标体系研究》）

关键信息基础设施供应链安全风险分析

一、供应链产品和服务可靠性风险

近年来，因供应链产品漏洞爆出的安全事件屡见不鲜，如 2014 年 Target 数据泄漏事件、2017 年远程终端管理工具 Xshell 后门事件、2020 年 4 月 DarkHotel 利用 VPN 漏洞攻击事件等等，黑客可通过脆弱的供应链产品作为突破口进而实现篡改数据、获取控制权限、植入或伪造包含恶意逻辑的软硬件，达到情报收集、破坏基础设施和数据资产等目的。供应链服务商为便于后续产品维护，常利用产品远程控制功能，加载、绕过或禁用部分安全策略，甚至隐藏行迹未告知用户远程控制的目的，极大增加用户方的安全隐患风险。

二、供应链信息共享数据泄露风险

首先，随着云计算、物联网、人工智能、大数据等信息技术在社会生活中的广泛应用，促进了供应链的发展。同时，使得信息网络的建设规模不断扩大，在运行过程中对于共享资源的需求也不断提升，可能会导致更为严重的信息泄露问题。其次，供应链的企业成员之间也可能出现信息泄露问题，部分企业为了提高经营收益，往往会泄露企业的创新技术，以此促进企业竞争，获得更为低廉的市场价格，降低企业经营成本。下游经销商在泄密技术后，上游企业为增加收益，提升市场竞争力会进一步进行技术研发，降低原有产品的价

格以提升市场占有率，减少零售企业经营成本。再者，因第三方企业造成信息的泄露，部分咨询公司管理不严格，造成技术和产品信息的泄露，给企业的经营造成负面影响。

三、供应链供给中断服务停止风险

当关键信息基础设施正以高速发展的状态逐步进入到高端领域时，某些技术领先的供应链突然显得很脆弱。主要表现在：核心产品缺货、交付周期一拖再拖、供给总量无法满足需求，甚至产品投诉得不到回应等等。由于对关键信息基础设施领域中核心技术的稀缺，产品及服务需要依赖于进口，增加供应链不可控风险，可能造成整体的业务服务中断。其次因自然因素、国际政治形势等不可抗力因素中断供应链渠道，导致整体业务连续性中断。主要表现在产品停产、供应链服务商注销，国际贸易管制、知识产权、限制销售等。再有，或因恶意竞争、弄虚作假等手段导致供应链品质下降，限制用户合理选择或替换供应商，导致业务支撑力度不足，品质下降。

（来源：《关键信息基础设施供应链安全思考》）

关键信息基础设施供应链安全发展趋势

关键信息基础设施供应链安全防护是关键信息基础设施安全防护的重要环节，是贯彻落实好《关键信息基础设施安全保护条例》的必然要求。当前，指导关键信息基础设施运营者做好关键信息基础设施供应链安全防护，确保关键信息基础设施供应链安全，成为关键信息基础设施运营者的重要工作，未来关键信息基础设施供应链安全防护主要呈现以下发展趋势。

一、形成常态化安全监管机制

2020 年，国家互联网信息办公室等 12 个部门联合发布的《网络安全审查办法》，明确要求电信、广播电视、能源、金融等行业领域的重要网络和信息系统运营者在采购网络产品和服务时，应当申报网络安全审查，确保关键信息基础设施供应链安全。

国家网信部门协同行业保护工作部门建立关键信息基础设施供应链安全常态化监管机制，重点关注供应链安全风险最为突出和急迫的行业及领域，开展供应链安全风险评估，针对关键信息基础设施使用的重要基础通用软件、行业软件、数据库、软件下载平台、云平台等，要开展开源代码安全检测，有效防范软件供应链安全威胁。国家监管部门要加大对网络攻击、传播病毒、设置软件后门等违法犯罪的打击力度。

二、安全政策趋于标准化、规范化

目前关键信息基础设施供应链安全在细分领域尚无统一的标准和政策，但是国内外许多有关专家学者、政府企业等已在供应链安全领域开展研究，提出许多有效的管理政策和标准，如美国颁布的《ICT 供应链风险管理标准》（NIST SP800-161）、《商用信息技术软件及固件审查项目》（VET）、《确保信息通信技术与服务供应链安全》等管理要求、《信息安全技术 ICT 供应链安全风险管理指南》（GB/T 36637-2018）等。

各有关部门认真细化《关键信息基础设施安全保护条例》各项要求，出台指导意见，制定完善关键信息基础设施供应链安全的相关标准，指导相关部门、行业保护工作部门和关键信息基础设施运营者研究制定实施关键信息基础设施安全管理措施。

三、结合信创产业同步发展

在国家相关政策的扶持和带动下，国产的关键信息基础设施软硬件已经得到了较快发展，但是产业规模化效应不断扩大形成，带来的软件供应链安全问题日显突出，为了解决关键信息基础设施的“卡脖子”问题，国家相关部门也在加大对信创产品、行业应用软件和大型工业软件安全防护建设的政策支持，鼓励国内信创厂商和金融、电信、能源等重点行业加大研发投入，加快突破核心关键技术突破，尽快形成一大批核心通用基础和行业软件储备，不断完善重点行业软件供应链安全生态体系，积极有效应对关键信息基础设施软件供应链安全风险。

四、积极吸纳专业人才，开展相关培训

近年来，国家加强网络安全学科建设，在高校增设网络空间安全一级学科，并建立了国家网络安全人才与创新基地，已经开始培养了一大批网络安全专业人才。关键信息基础设施运营者设立网络安全监测、检测和风险评估等关键岗位，推动关键信息基础设施网络安全防护能力建设，开展网络安全监测、检测和风险评估成为发展趋势，并且通过参加国家不同层级网络攻防演练、专业教育培训等方式，不断强化关键岗位专业人员业务水平。

国际网络空间安全形势日益复杂，针对关键信息基础设施的网络攻击威胁与日俱增，有关部门和关键信息基础设施运营者要坚决贯彻落实好《关键信息基础设施安全保护条例》，不断强化责任主体意识，采取有效措施防范供应链安全风险，确保关键信息基础设施安全运行。

（来源：《贯彻〈关键信息基础设施安全保护条例〉，加强供应链安全工作》）

编辑部地址：南宁市体强路 18 号广西信息中心 1412 号房
联系电话：0771-6113592
电子邮箱：dsjyjs@gxi.gov.cn
网址：http：//gxxxzx.gxzf.gov.cn/

扫描二维码获取
更多决策参考信息