ICS 33.050
M 30

团　体　标　准

T/TAF 073-2020

网络产品供应链安全要求

Security requirements for network product supply chain

2020-09-10 发布　　2020-09-10 实施

电信终端产业协会　发布

目　次

前言 II
引言 III
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 概述 2
5 网络产品供应链基础设施安全要求 3
6 网络产品供应链环节安全要求 4
参考文献 8

前　言

本标准对网络产品的生产者供应链安全提出要求。网络产品的生产者在构建本组织的供应链安全管理体系时可参考本标准。

标准按照 GB/T 1.1-2009 给出的规则起草。

本标准中的某些内容可能涉及专利。本标准的发布机构不承担识别这些专利的责任。

本标准由电信终端产业协会提出并归口。

本标准起草单位：中国信息通信研究院、华为技术有限公司、联想（北京）有限公司、中兴通讯股份有限公司、中国信息通信科技集团、杭州迪普科技股份有限公司。

本标准主要起草人：倪平、张治兵、薛勇波、李汝鑫、吴萍、段伟伦、仇俊杰、陈鹏、刘微、周继华、韩晓露、郝圣阳。

引　言

随着经济全球化发展，信息系统的运行依赖于分布在全球相互联系的供应链生态系统，供应链安全对国家经济增长和网络安全的重要性不断凸显。供应链安全管理是保障产业健康有序发展的重要举措。

网络产品供应链覆盖网络产品整个生命周期，从设计研发、生产、交付到运维直至废弃，每一个环节都可能涉及到第三方，如供货商、集成商、服务商等，因此每一个环节都应该提出相关的供应链安全要求。同时，每个环节都会涉及到对制度、人员、信息系统等要求，以上支撑了整个供应链安全管理的落实。

本标准是对组织自身的供应链管理提出的安全要求，组织可根据本标准中的安全要求，构建本组织的供应链安全管理体系，以提高本组织的供应链安全。

网络产品供应链安全要求

1 范围

本标准对网络产品在管理制度、组织机构和人员、信息系统等以及设计与研发、采购、生产、仓储、交付、运维等供应链环节提出了不同等级的安全要求。

本标准适用于重要信息系统和关键信息基础设施中网络产品的提供者对供应链进行安全管理，也适用于指导网络产品提供者加强供应链安全管理，同时可为网络产品的采购者和第三方机构对网络产品进行安全性评价时提供参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069 信息安全技术 术语

GB/T 18354-2006 物流术语

GB/T 36637-2018 信息安全技术 ICT 供应链安全风险管理指南

3 术语和定义

3.1

网络 network

是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

3.2

网络产品 network product

是指作为网络组成部分以及维持网络功能的设备、软件等。

3.3

供应链 supply chain

通过多个资源和过程联系在一起的一系列组织，根据由服务协议或其他采购协议建立连续的供应关系，每个组织充当一个需求方、提供方或双重角色。

3.4

供应链基础设施 supply chain infrastructure

由组织内的硬件、软件和制度流程等构成的集合，用于构建产品和服务的设计、开发、生产、集成、仓储、交付、运维等网络产品供应链声明周期的环境。

3.5

可追踪性 traceability

允许在整个供应链中跟踪身份、过程或元素的特性。

3.6

需求方 acquirer

获得或采购产品或服务的利益相关者，也可简称需方，在本标准中指网络产品的采购方或使用方。

3.7

供应商 supplier

与需求方签订协议以提供产品或服务的组织或个人。这包括供应链中的所有供应商。包括（1）信息系统、系统部件或软硬件产品的开发者或生产者；（2）货架产品供应商；（3）产品经销商；（4）提供运维等服务的服务商等。

3.8

采购 purchase

指组织在一定的条件下从供应市场获取产品或服务作为组织资源，以保证组织生产及经营活动正常开展的一项经营活动。

3.9

物流 logistics

物品从供应地向接收地的实体流动过程。根据实际需要，将运输、储存、装卸、搬运、包装、流通加工、配送、信息处理等基本功能实施有机结合。

3.10

关键部件 critical component

存储软件、数据的介质以及具备数据处理能力的部件。如芯片、存储介质、可编程控制器件等。

4 概述

4.1 供应链安全管理内容

供应链通常涵盖软、硬件产品的采购、开发、集成等环节，涉及到生产者、供应商、系统集成商、服务提供商等多类实体以及技术、法律、政策等软环境。与传统的供应链不同，网络产品供应链贯穿网络产品全生命周期，从产品的设计研发、生产、交付以及运维，包括供应商管理、采购、生产、仓储、

物流等供应链管理环节。根据所覆盖的产品生命周期的不同，网络产品供应链管理可以分为两类，一类是在整个生命周期中都会涉及到的要求，如与供应链安全管理相关的制度、组织机构及人员、信息系统等，这一类称之为网络产品供应链基础设施管理；另一类是和特定的生命周期环节相关的，如设计研发、采购、生产、交付等，这一类为网络产品供应链环节管理。网络产品供应链安全管理框架如图1所示。

4.2 供应链安全管理目标

(a) 供应链完整性：保障在网络产品全生命周期中，产品及其所包含的元器件、软件、关键部件、数据等以及所使用的工具不被植入、篡改、伪造或者替换。

(b) 供应链可用性：保障需求方对供应链的使用。一方面，确保供应链中各方按照与需求方签订的协议能够正常供应，不因人为或者自然因素中断，即可供应性；另一方面，即使在供应部分失效时，仍能在一定条件下，以可预计的方式恢复到可接受的供应状态的能力，即保持一定的弹性。

(c) 供应链保密性：保障供应链上传递的信息不被泄露给未授权者。

(d) 供应链可控性：保障需求方对供应链的控制能力，对供应链生命周期各环节信息的理解、各级供应商/服务商情况的透明度和可信度、数据流的管理，及供应链可追溯性。

图1 网络产品供应链安全管理框架

4.3 供应链安全要求

网络产品供应链安全要求需覆盖供应链基础设施和供应链各个环节，安全要求分两个等级，即基本级与增强级，安全等级由低到高，安全要求逐级增强。与基本级内容相比，增强级中要求有所增加的内容在正文中通过**加粗**表示。基本级只需满足非加粗安全要求，增强级则需满足全部的安全要求。

5 网络产品供应链基础设施安全要求

5.1 管理制度

组织应：

(a) 制定供应链安全管理的总体方针和安全策略，说明供应链安全管理的总体目标、范围、原则和安全框架等；

(b) 建立供应链安全管理制度和程序，覆盖网络产品全生命周期，内容包括但不限于设计与研发、采购、生产、仓储、交付及运维等；

(c) 定期或在发生重大安全事件、外部环境重大变化、组织策略变化时，对供应链安全管理制度（含自身和供应商制度、流程、规范、应急预案等的执行和演练情况）进行检查和审定，对存在不足或需要改进的安全管理制度进行修订；

注：供应链发生重大安全事件可能是关键部件断供、所购产品或者研发生产所使用的工具存在严重安全问题、供

应链重要数据泄露等。

(d) 通过制度保障供应链安全管理所需的资金、人员和权限等可用资源；

(e) 定期进行供应链风险评估，制定预案、采取措施进行消除或降低风险。

5.2 组织机构和人员管理

组织：

(a) 应明确负责供应链安全管理的部门/机构，并定义供应链安全管理职责和要求；

(b) 应明确供应链安全管理的责任人为组织的最高责任人；

(c) 应明确划分管理供应链安全的人员的职责定位；

(d) 应制定针对涉及供应链安全管理的人员的安全要求，包括但不限于管理者、普通员工和第三方人员等；

(e) 应制定安全培训计划，将供应链安全管理培训纳入组织的培训计划中，并定期执行；

(f) 应对所有参与供应链管理的组织内部员工进行安全意识和技能培训，尤其是采购、仓储、信息系统开发和管理、产品运维等人员应进行基于岗位要求的安全意识和技能培训；

(g) 应要求供应商对其接触组织产品或数据的员工进行安全意识培训。

5.3 信息系统安全管理

供应链管理信息系统应符合以下要求：

(a) 信息系统应实现对网络产品全生命周期相关物料和活动的追溯，如对组成产品的元器件、产品的软件版本等；

(b) 信息系统具备安全功能（如用户鉴别、用户审计等），并采取定期进行安全评估等措施进行安全管理；

(c) 信息系统应能够覆盖产品设计与研发、采购、生产、仓储、交付、运维等环节中供应链安全管理要求；

(d) 对信息系统中的数据分级分类存储，并采取不同的措施保证数据的安全。

6 网络产品供应链环节安全要求

6.1 设计与研发

6.1.1 产品开发过程控制

组织应对产品开发过程进行控制：

(a) 应建立安全开发流程，明确开发过程中的安全控制措施，如威胁分析、安全架构设计、安全编码、安全测试、补丁管理等；

(b) 应建立开发配置库，对开发过程中的文档、代码、版本、操作、工具等进行受控管理；

(c) 应对软件开发配置库进行安全管理，避免信息泄露等安全风险；

(d) 应要求外包开发交付的产品（含软件开发和硬件）明示所有的接口和功能；

(e) 应建立开发过程中产品对内发布和变更流程，对自研、外包开发以及选用的第三方软件、硬件进行统一管理和向内部下游发布和变更；

(f) 开发（含软件开发和硬件开发）外包时，应要求外包承担组织按照安全开发流程进行开发，并提供相关的证明材料；

(g) 在软件版本发布前，须对二进制与源代码的一致性进行验证，确保所有的二进制来源可靠，并进行防病毒检查，防止被篡改；

(h) 在软件和产品中采取技术手段保证完整性，如数字签名、数字证书等。

6.1.2 工具使用控制

组织应：

(a) 建立工具控制管理制度，建立研发/测试工具和设备白名单，采用网络安全检测、正版授权验证等措施进行白名单准入控制；

(b) 评估使用研发/测试工具和设备的安全风险，并制定相应的应对措施。

6.1.3 部件使用控制

组织应：

(a) 分析并制定影响最终产品网络安全的关键部件清单，并定期更新；

(b) 分析选用的关键部件可能面临的安全风险并制定应对措施，如断供风险、后门风险等；

(c) 明确元器件、关键部件等的安全选用原则；

(d) 明确关键部件更替流程；

(e) 明确禁止选用的关键部件。

6.2 采购

6.2.1 供应商管理

(a) 组织应对供应商进行认证或审核：

1) 分析不同类型的供应商（含外包方）在提供产品或服务时可能引入的安全风险；

注：可根据供货产品、提供的服务、企业规模等进行对供应商进行分类。

2) 制定供应商的认证或审核标准和流程，对供应商进行安全认证或审核，未通过的供应商不得进入合格供应商目录；

3) 制定安全协议（含网络安全协议、隐私保护协议、不扣货协议等），并与供应商或潜在的供应商进行签署；

4) 要求供应商提供其自身供应链管理安全风险评估结果和消减措施，涉及到商业秘密的除外。

(b) 组织应建立并维护合格供应商目录：

1) 避免单一来源供应商，如无法避免，应评估使用单一来源供应商的风险并制定应对措施；

2) 在供应商发生重大变化，可能影响组织的供应链安全时，应重新对供应商进行安全评估；

注：供应商发生重大变化可能是供应商所在地发生影响正常供应的事件、供应商资本背景发生变更、供应商资质发生变化、供应商产品架构发生变化等。

3) 根据组织特点以及供应环境变化，对合格供应商进行定期或不定期的安全风险复评审，复评审应在一定时期内覆盖目录中所有的供应商；

4) 对于复评审中发现的安全风险，应跟踪处理。

(c) 对于严重违反安全协议的供应商应进行再认证或者调整出合格供应商目录；

(d) 通过书面的方式向供应商明确传递组织关于供应链安全的要求。

6.2.2 外包管理

组织应：

(a) 评估外包可能引入的安全风险，并制定应对措施；

(b) 对外包进行管理，明确允许或禁止外包的条件、外包承担方的选择、外包数据的管理等；

(c) 与外包方签订的协议中，应明确对方的安全责任且不得低于组织内部相同或者类似部门的安全要求；

(d) 对多级外包制定明确的管理规范，明确允许或禁止的条件。

6.2.3 采购流程管理

组织：

(a) 应分析采购过程中面临的安全风险，并制定相应的应对措施；

(b) 应分析采购的产品交付过程中可能面临的安全风险，并制定相应的应对措施，避免产品被篡改或者敏感信息泄露；

(c) 应分析采购的产品运维过程中可能面临的安全风险，并制定相应的应对措施；

(d) 对于采购的产品或服务，包括但不限于元器件、关键部件以及软件、服务等，应制定安全检测或审核评估标准，并进行网络安全检测或审核评估。

6.3 生产

组织应：

(a) 依据关键部件清单，对采购的关键部件在进入生产前进行完整性和真实性的检查；

(b) 评估生产过程中使用的工具和设备的安全风险，并制定相应的应对措施；

(c) 建立生产工具和设备安全使用规范，如建立生产工具和装备白名单，采用网络安全检测、正版授权验证等措施进行白名单准入控制；

(d) 对生产过程中的关键环节进行控制，如建立安全的软件管理和发放机制，实施安全的软件灌装等，保证产品的完整性；

(e) 对生产环境的物理访问采取严格的安全措施；

(f) 对外包合作方进行管理，安全要求不低于组织的安全要求；

(g) 再利用的返回物料或产品(包括未使用但已拆箱的退货物料或产品)的安全性必须符合新品的要求，经过测试合格方可使用；

(h) 存储生产过程中的物料配送、交接、制造、测试过程中的记录和数据，确保生产过程可追溯；

(i) 建立一个独立的产品生产和测试网络；

(j) 对外包过程进行监控，包括但不限于外包过程中安全规范的落实情况，人员的安全意识等；

(k) 对关键部件建立唯一标识，记录关键部件的来料、生产、存储、交接、运输和交付等状态；

(l) 建立应急响应程序，对生产过程中基础设施（如 IT 系统、测试装备等）的故障、产品安全（如漏洞）等进行管理。

6.4 仓储

组织：

(a) 应分析仓储面临的安全风险，并制定相应的应对措施，以保障供应链的安全；

(b) 应对仓库实施严格的安全访问控制措施，建立物资、人员等的出入日志记录；

(c) 应对仓库管理员作业过程进行记录，并可追溯；

(d) 租赁外部仓库时，应与对方签订安全协议，确保物料安全，避免敏感信息泄露，或者物料被篡改、损坏、盗窃等；

(e) 应对仓库管理员进行安全意识培训和背景调查；

(f) 应对在库物资进行安全管理，如定期盘点、贵重物料分区管理、作业过程记录等；

(g) 租赁外部仓库时，应对仓储商进行背景审查；

(h) 未经允许或者未采取相关的完整性防护和检验措施，应禁止在仓库执行装配和上电操作，防止在

库物料被植入、篡改、遗失等。

6.5 交付

组织：

(a) 应分析交付过程中的安全风险，如物流环节的安全风险，并制定相应的应对措施，以保障供应链的安全，避免产品被植入、篡改、替换、伪造、破坏、滞留、丢失等；

(b) 应保护运输过程中的敏感信息，避免被泄露；

(c) 在接收货物时，应对待接收的货物的运载工具、包装及封签/封条的完整性进行检查，运载工具及包装完好，封签/封条与系统/单据一致的方可接收入库。货物存在异常时，须与供应商、承运商进行确认，执行确认程序，只有确认可信的产品方可接收和使用，并保留相关确认记录；

(d) 应对承运商进行相关的审查，选择可靠的物流服务商；

(e) 应选择可靠的物流路线，对物流过程进行监控和管理，对物流的节点、路径定期和不定期的进行审视，及时调整物流策略包括但不限于：物流承运商的替换、物料节点调整、路径变更等。

6.6 运维

组织应：

(a) 分析运维过程中可能面临的安全风险，并制定相应的应对措施，以保障供应链的安全；

(b) 对运维过程进行安全监控和审计；

(c) 选用可信的运维人员，所选用的运维人员应需求方认可或备案，并在需求方授权范围内开展运维工作；

(d) 对运维过程中产生的数据进行安全管控，避免数据被篡改、敏感数据泄露等安全风险；

(e) 要求供应链中产品或者服务的开发者/提供者建立产品或服务的漏洞管理流程，对产品和解决方案生命周期中发现的漏洞进行收集、处理和披露；

(f) 对返回再利用的物料采取有效措施保障其保密性，消除返回物料中可能存在的用户数字资产。

参 考 文 献

[1] GB/T 24420 供应链风险管理
[2] GB/T 32921 信息安全技术 信息技术产品供应方行为安全准则
[3] GB/T 36637-2018 信息安全技术 ICT 供应链安全风险管理指南
[4] ISO 28001 Security management systems for the supply chain - Best practices for implementing supply chain security, assessments and plans - Requirements and guidance
[5] ISO/IEC 27036-2 Information technology - Security techniques - Information security for supplier relationships - Part2: Requirements
[6] ISO/IEC 27036-3 Information technology - Security techniques - Information security for supplier relationships - Part3: Guidelines for information and communication technology supply chain security
[7] NIST 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations

电信终端产业协会团体标准

网络产品供应链安全要求

T/TAF 073-2020

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn