ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36637—2018

信息安全技术
ICT 供应链安全风险管理指南

Information security technology—Guidelines for the information and communication technology supply chain risk management

2018-10-10 发布　　2019-05-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国电子技术标准化研究院、中国科学院软件研究所、联想(北京)有限公司、华为技术有限公司、浙江蚂蚁小微金融服务集团股份有限公司、阿里巴巴(北京)软件服务有限公司、北京京东叁佰陆拾度电子商务有限公司、中国信息通信研究院、微软(中国)有限公司、浪潮电子信息产业股份有限公司、国家信息技术安全研究中心、英特尔(中国)有限公司、北京赛西科技发展有限责任公司、阿里云计算有限公司、中国信息安全认证中心、中国科学院信息工程研究所信息安全国家重点实验室、北京工业大学、北京邮电大学、北京中电普华信息技术有限公司。

本标准主要起草人:刘贤刚、胡影、卿斯汉、叶润国、孙彦、李汝鑫、薛勇波、范科峰、王昕、白晓媛、黄少青、刘陶、赵江、杨煜东、赵丹丹、张凡、陈星、宁华、樊洞阳、陈晔、吴迪、朱红儒、杨震、马占宇、曹占峰。

引　言

随着信息通信技术的普及应用，加强 ICT 供应链的安全可控保障变得至关重要。目前，世界各国和 ICT 行业已普遍认识到，相比传统行业 ICT 行业供应链更加复杂，存在安全风险的概率更大。加强 ICT 供应链安全管理，可增强客户对 ICT 供应链以及 ICT 行业的安全信任。

与传统供应链相比，ICT 供应链具有许多不同的特点，例如：ICT 供应链涵盖 ICT 产品和服务的全生命周期，不仅包括传统供应链的生产、集成、仓储、交付等供应阶段，也包括产品服务的设计开发阶段和售后运维阶段；ICT 产品由全球分布的供应商开发、集成或交付，供应链的全球分布性使得客户对供应链的掌握情况和安全风险控制能力在下降；传统供应链主要关注如何将产品有效地交付给客户，或者供应链健壮性的强度，而 ICT 供应链安全更关注是否会有额外的功能注入产品和服务中，交付的产品和服务是否与预期一致等。这些特点使得 ICT 供应链比传统供应链存在更多的安全风险，加强 ICT 供应链的安全风险管理刻不容缓。

本标准不规范信息技术产品供应方的安全行为准则。推荐在关键信息基础设施或重要信息系统中使用本标准。然而，由于个别需要和相关性，组织可选择将标准应用到其他系统或特定组织，不过应用本标准的控制措施可能会增加组织和外部供应商的潜在成本，需要组织在成本和风险间进行权衡。

信息安全技术
ICT 供应链安全风险管理指南

1 范围

本标准规定了信息通信技术(以下简称 ICT)供应链的安全风险管理过程和控制措施。

本标准适用于重要信息系统和关键信息基础设施的 ICT 供方和运营者对 ICT 供应链进行安全风险管理,也适用于指导 ICT 产品和服务的供方和需方加强供应链安全管理,同时还可供第三方测评机构对 ICT 供应链进行安全风险评估时参考。

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—2010 信息安全技术 术语

GB/T 31722—2015 信息技术 安全技术 信息安全风险管理

3 术语和定义

GB/T 25069—2010 和 GB/T 31722—2015 界定的以及下列术语和定义适用于本文件。

3.1

ICT 需方 ICT acquirer

从其他组织获取 ICT 产品和服务的组织或个人。

注 1:获取可能涉及或不涉及资金交换。

注 2:重要信息系统和关键信息基础设施的运营者,通常是从 ICT 供方获取网络产品和服务的 ICT 需方。

3.2

ICT 供方 ICT supplier

提供 ICT 产品和服务的组织。

注 1:供方也可称供应商、供应方。

注 2:供方可以是内部的或外部的组织。

注 3:ICT 供方包括产品供应商、服务提供商、系统集成商、生产商、销售商、代理商等。

3.3

供应关系 supplier relation

在需方和供方之间的协议,可用于开展业务,提供产品和服务,实现商业收益。

注 1:需方和供方可以是同一个机构。

注 2:在供应链中,上游机构的需方同时也是下游机构的供方。终端客户可以理解为一种特殊的需方。

3.4

ICT 供应链 ICT supply chain

ICT 产品和服务的供应链,是指为满足供应关系通过资源和过程将需方、供方相互连接的网链结构,可用于将 ICT 的产品和服务提供给需方。