ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36630.1—2018

信息安全技术 信息技术产品安全可控评价指标 第1部分:总则

Information security technology—Controllability evaluation index for security of information technology products—Part 1:General principles

2018-09-17 发布　　2019-04-01 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 …… Ⅰ
引言 …… Ⅱ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　安全可控概述 …… 2
4.1　风险分析 …… 2
4.2　安全可控保障 …… 2
4.2.1　保障目标 …… 2
4.2.2　保障要求 …… 2
5　安全可控评价 …… 3
5.1　评价原则 …… 3
5.1.1　科学合理 …… 3
5.1.2　客观公正 …… 3
5.1.3　知识产权保护 …… 3
5.2　评价指标体系 …… 3
5.2.1　体系框架 …… 3
5.2.2　研发生产评价类 …… 4
5.2.3　供应链评价类 …… 5
5.2.4　运维服务评价类 …… 5
5.3　评价实施 …… 5
5.3.1　评价流程 …… 5
5.3.2　评价方法 …… 5
5.3.3　评价结果 …… 6
参考文献 …… 7

前　言

GB/T 36630《信息安全技术　信息技术产品安全可控评价指标》包括以下部分：

——第1部分：总则；

——第2部分：中央处理器；

——第3部分：操作系统；

——第4部分：办公套件；

——第5部分：通用计算机。

本部分为GB/T 36630的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分起草单位：中国电子信息产业发展研究院、公安部第一研究所、中国电子技术标准化研究院、中国信息安全研究院有限公司、中国电子科技集团公司、国家信息技术安全研究中心、工业和信息化部软件与集成电路促进中心、中国软件评测中心、公安部第三研究所、中国信息安全测评中心、中国信息通信研究院等。

本部分主要起草人：刘权、王闯、韩煜、李海涛、叶润国、刘贤刚、左晓栋、张建军、李冰、方进社、刘龙庚、顾健、张宝峰、宁华、翟艳芬、冯伟、许亚倩、杨永生、李英的、陈妍、赵爽、王超、马士民、荣志刚、韦安垒。

引　言

随着信息技术应用的日益深入，信息技术产品设计实现的复杂度不断提升，涉及的生命周期环节越来越多，人为设置的后门、不可控的产品供应链、不能持续的产品服务、未经授权的数据收集和使用等潜在的不可控因素不断增多，严重损害应用方的权益，甚至可能危害国家安全和公共利益。

依据《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（试行）》等要求，为提高信息技术产品安全可控水平，防范网络安全风险，维护国家和公共安全，进而满足信息技术产品应用方安全可控需求，增强应用方信心，推动信息技术产业健康、快速发展，特制定 GB/T 36630。

GB/T 36630 提出信息技术产品安全可控评价指标和评价方法，不包含对产品本身安全功能和安全性能的评价。安全可控只是信息技术产品的一个属性，如需评价信息技术产品的安全功能和安全性能等其他属性，可参照相关国家标准。

本部分明确了信息技术产品安全可控评价指标总体要求，为开展信息技术产品安全可控评价工作提供指导。

信息安全技术
信息技术产品安全可控评价指标
第1部分:总则

1 范围

GB/T 36630的本部分规定了信息技术产品安全可控的概念、保障目标,给出了信息技术产品安全可控的评价原则、评价指标体系和实施流程。

本部分适用于评价实施方对信息技术产品的安全可控程度进行评价,也可供信息技术产品供应方和应用方在产品供应和应用过程中保障产品安全可控进行参照。

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

3 术语和定义

GB/T 25069—2010界定的以及下列术语和定义适用于本文件。

3.1

信息技术产品 information technology product

具有采集、存储、处理、传输、控制、交换、显示数据或信息功能的硬件、软件、系统和服务。

注:信息技术产品包括计算机及其辅助设备、通信设备、网络设备、自动控制设备、操作系统、数据库、应用软件与服务等。

[GB/T 32921—2016,定义3.1]

3.2

安全可控 controllability for security

信息技术产品具备的保证其应用方数据支配权、产品控制权、产品选择权等不受损害的属性。

3.3

信息技术产品供应方 information technology product supplier

提供信息技术产品的组织。

注:信息技术产品供应方包括生产商、销售商、代理商、集成商、服务商等。

[GB/T 32921—2016,定义3.2]

3.4

信息技术产品应用方 information technology product user

采购和使用信息技术产品的用户。

注:信息技术产品应用方包括自然人、法人等。