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。

3.5

产品供应链　product supply chain

为满足供应关系通过资源和过程将供需各方相互连接的网链结构。

4　安全可控概述

4.1　风险分析

信息技术产品在安全可控方面所面临的风险主要包括：

a）　产品被非法控制、干扰和中断运行；

b）　产品及关键部件在生产、测试、交付、技术支持过程中引发的供应链安全问题；

c）　产品供应方利用提供产品的便利条件非法收集、存储、处理、使用、销毁用户相关数据；

d）　产品供应方利用应用方对产品的依赖实施不正当竞争或损害应用方利益；

e）　其他可能危害国家安全和公共利益的情况。

4.2　安全可控保障

4.2.1　保障目标

安全可控保障是应用方信任信息技术产品满足其安全可控需求的基础，其目标是保护应用方的数据支配权、产品控制权和产品选择权：

a）　数据支配权是指应用方能够自主控制自己的数据，信息技术产品供应方不在未经授权情况下以任何形式获取应用方的数据，损害应用方对自己数据的支配权；

b）　产品控制权是指应用方能够自主控制所使用的产品，信息技术产品供应方不在未经授权情况下通过网络控制和操纵应用方产品，损害应用方对自己所拥有和使用产品的控制权；

c）　产品选择权是指应用方能够自主选择所使用的产品，信息技术产品供应方不可利用应用方对其依赖性牟取不当利益或损害应用方权益，包括停止提供合理的安全技术支持、迫使应用方更新换代、恶意中断产品供应等。

4.2.2　保障要求

针对安全可控保障目标，结合信息技术产品在研发生产、供应、运维服务等生命周期各环节面临的潜在风险，对信息技术产品及其提供方提出了安全保障要求。其中，影响应用方数据支配权的主要风险来自数据收集、传输、存储、处理、使用、销毁等环节，为有效控制相关风险应确保产品数据相关实现与其声称功能一致、数据相关服务合规；影响应用方产品控制权的风险主要来自产品研发生产、供应、运维服务等环节，为有效控制相应风险应确保产品控制相关实现与其声称功能一致、控制相关服务合规；影响应用方产品选择权的风险主要来自供应链、运维服务等环节，为有效控制相应风险应确保产品的持续供应、正常使用。具体的安全可控保障要求如表 1 所示。

表 1　安全可控保障目标及要求

保障目标	保障要求
数据支配权	应用方数据不被非授权收集、处理和使用，应用方具有支配权： ——产品涉及数据收集、传输、存储、处理、使用、销毁等环节的实现应与其声称功能一致； ——产品严格遵守法律法规要求及其承诺，不存在非授权收集、处理应用方数据等情况； ——产品在构建系统过程中不会引入新的影响数据支配权的隐患

表 1（续）

保障目标	保障要求
产品控制权	应用方使用的产品不被非授权控制和操纵，应用方具有控制权： ——产品涉及操作控制、远程访问等方面的实现与其声称功能一致； ——产品相关服务严格按照法律法规要求及其承诺，没有非授权控制和操纵产品本身等情况； ——产品在构建系统过程中不引入新的影响产品控制权的隐患
产品选择权	应用方对产品的选择权不应被剥夺、被妨碍，不因相应选择付出不合理的额外代价： ——产品所有供应环节不存在因非技术因素、非正常商业因素中断供应的隐患； ——供应方不存在利用提供产品的便利条件获取不当利益、实施不正当竞争或损害应用方利益的情况； ——供应方不存在利用应用方依赖性非法获利的情况

5 安全可控评价

5.1 评价原则

5.1.1 科学合理

评价指标覆盖产品安全可控的关键要素，分值设置科学，评价方法合理。

5.1.2 客观公正

评价指标客观无歧视，评价过程公平公正，同类信息技术产品评分规则统一。

5.1.3 知识产权保护

充分尊重供应方知识产权，保护供应方合法权益，评价过程中供应方知识产权不受侵害。

5.2 评价指标体系

5.2.1 体系框架

为有效控制信息技术产品在安全可控方面面临的风险，实现安全可控保障目标，依据安全可控保障要求制定了安全可控评价指标体系，具体包括优先评价项和一般评价项两大类：

a) 优先评价项指严重影响产品安全可控的指标项，该类指标项在评价开始时优先评价。在评价过程中，若优先评价项不满足要求，则评价结果为 0 分，无需进行后续的一般评价项评价。是否设置优先评价项、以及选择哪项指标作为优先评价项由该类信息技术产品自身技术特点决定。例如可将中央处理器产品的知识产权设置为优先评价项，若发现被评价产品存在经司法判决且未得到妥善处理解决的侵权行为，则按照优先评价项的判定原则，直接判定该中央处理器产品安全可控评价结果为 0 分；

b) 一般评价项是针对信息技术产品全生命周期中可能面临的风险，设置的评价安全可控程度的一系列指标项。根据信息技术产品的生命周期将指标项划分为研发生产评价类、供应链评价类、运维服务评价类三类。表 2 给出了各评价类对应的指标项及考查内容，并明确了各指标项与安全可控保障目标的对应关系。本标准中，中央处理器、操作系统、办公套件、通用计算机等具体信息技术产品依据自身技术特点和需求设置相应的一般评价项。各信息技术产品的指标项应结合应用方关注点和专家论证结果，设置分档次的参考分值。

表 2　一般评价项

评价类	指标项	考查内容	数据支配权	产品控制权	产品选择权
研发生产评价类	产品设计实现透明性	产品涉及安全可控的核心技术	√	√	
	产品设计验证	验证环境	√	√	
		验证充分性			
		验证结果与产品一致性			
	产品重现能力	重现环境	√	√	
		重现充分性			
		重现结果与产品一致性			
	产品关键技术研发能力	产品定制权限	√	√	
		产品定制能力			
	产品安全生态适应性	安全可控产品适配性			√
		接口开放性			
		密码合规性			
供应链评价类	产品持续供应能力	产品供应情况			√
		核心团队情况			
		产品交付管理			
	产品供应链保障能力	核心部件安全可控程度	√	√	√
		供应链各环节的可追溯性和供应稳定性			
运维服务评价类	产品服务保障能力	服务及时性		√	√
		服务规范性			
		服务可持续性			
	数据处理规范性	数据收集	√		
		数据传输			
		数据存储			
		数据处理			
		数据使用			
		数据销毁			

5.2.2　研发生产评价类

研发生产评价类主要包括产品设计实现透明性、产品设计验证、产品重现能力、产品关键技术研发能力和产品安全生态适应性 5 个指标项：

a）　产品设计实现透明性指标主要验证产品中安全可控相关功能模块的实现是否与其声称的一致，可以通过供应方所提供材料进行评价，必要时可通过技术手段等方式进行评价；

b）　产品设计验证指标主要验证产品硬件设计部分是否与实际产品一致，重点考查验证环境、验证

充分性，以及验证结果与产品一致性等内容，必要时可通过技术手段等方式进行评价；

c) 产品重现能力指标主要验证产品软件设计实现部分是否与实际产品一致，重点考查重现环境、重现充分性，以及重现结果与产品一致性等内容，必要时可通过技术手段等方式进行评价；

d) 产品关键技术研发能力指标主要评价供应方对影响到安全可控的核心技术的掌握能力，重点考查产品定制权限和产品定制能力等内容；

e) 产品安全生态适应性指标主要评价产品与应用环境的适配性，重点考查安全可控产品适配性、接口开放性、密码合规性等内容，本标准凡涉及密码算法的相关内容按国家有关法规实施，凡涉及到采用密码技术解决保密性、完整性、真实性、不可否认性需求的遵循密码相关国家标准和行业标准。

5.2.3 供应链评价类

供应链评价类主要包括产品持续供应能力和产品供应链保障能力 2 个指标项：

a) 产品持续供应能力指标主要评价供应方具备持续供应产品的能力，重点考查产品供应情况、核心团队情况、产品交付管理等内容；

b) 产品供应链保障能力指标主要评价供应方的供应链可靠性，重点考查核心部件安全可控程度、供应链各环节的可追溯性和供应链稳定性等内容。

5.2.4 运维服务评价类

运维服务评价类主要包括产品服务保障能力和数据处理规范性 2 个指标项：

a) 产品服务保障能力指标主要评价供应方为应用方提供持续运维服务的能力，重点考查服务及时性、服务规范性、服务可持续性等内容；

b) 数据处理规范性指标主要评价供应方对应用方数据的操作各环节的规范性，重点考查数据收集、数据传输、数据存储、数据处理、数据使用和数据销毁等方面的操作规范性内容。

5.3 评价实施

5.3.1 评价流程

评价流程主要包括评价准备、方案制定、现场实施、分析评估 4 个阶段：

a) 在评价准备阶段，评价实施方接收供应方提交的评价申请后，与供应方沟通所需的评价材料，包括拟提供的评价样品、材料和证据等，依据具体产品的评价指标审核供应方提供的评价材料是否满足条件，通过审核后，组建评价实施团队，根据需要可设置专家组；

b) 在方案制定阶段，评价实施方针对具体产品确定评价方法、程序和进度，形成评价方案；

c) 在现场实施阶段，评价实施方依据评价方案，结合供应方提供的评价材料逐项查验，必要时可要求供应方补充相关材料，双方对现场实施结果进行确认；

d) 在分析评估阶段，评价实施方依据现场实施情况对产品进行具体评价和打分。

5.3.2 评价方法

评价实施方在开展信息技术产品安全可控评价工作中应综合采用访谈、检查和测试等基本评价方法，以核实供应方所提供评价材料是否满足指标考查内容要求：

a) 访谈：评价实施方通过与供应方相关人员进行有针对性的交流以帮助理解、厘清或取得证据，访谈的对象为个人或团体，如技术团队负责人、核心技术工程师、采购部门负责人等；

b) 检查：评价实施方对供应方提供的相关材料进行观察、查验、分析以帮助理解、厘清或取得证据，检查的对象为制度、文档和记录，如必要的技术设计文档、核心材料采购记录等；

c) 测试：评价实施方使用预定的方法/工具使测试对象产生特定的结果，并将运行结果与预期的结果进行比对，测试的对象为信息技术产品的技术或功能特性，如安全可控产品适配性、重现结果与产品一致性等。

5.3.3 评价结果

信息技术产品安全可控评价采取百分制，最低得分为 0 分，未能通过优先评价项的按照最低分计分，最高得分为 100 分，即所有一般评价项所设定参考分值之和为 100 分。在评价过程中，评价实施方可根据产品的实际情况，在参考分值的区间范围内给出各评价指标项的具体分值。各评价指标项分值之和为该产品安全可控评价的结果，该结果可作为认定该产品安全可控程度的依据。

参 考 文 献

[1] GB/T 18336.1—2015 信息技术 安全技术 信息技术安全评估准则 第1部分:简介和一般模型

[2] GB/T 18336.3—2015 信息技术 安全技术 信息技术安全评估准则 第3部分:安全保障组件

[3] GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南

[4] GB/T 32921—2016 信息安全技术 信息技术产品供应方行为安全准则

[5] ISO 28002:2011 Security management systems for the supply chain—Development of resilience in the supply chain

[6] ISO/IEC 27034-1:2011 Information technology—Security techniques—Application security—Part 1:Overview and concepts

[7] ISO/IEC 27036-1:2014-03-15 (1st edition)Information security for supplier relationships—Part 1:Overview and concepts

[8] NIST Special Publication 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations

[9] General Data Protection Regulation, REGULATION (EU)2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL