



中华人民共和国国家标准

GB/T 36630.5—2018

信息安全技术 信息技术产品安全可控评价指标 第5部分：通用计算机

Information security technology—Controllability evaluation index for security of
information technology products—Part 5: General purpose computer

2018-09-17 发布

2019-04-01 实施

国家市场监督管理总局 发布
中国国家标准化管理委员会

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义、缩略语	1
3.1 术语和定义	1
3.2 缩略语	1
4 评价指标项	1
5 评价方法	2
5.1 评价材料要求	2
5.2 指标评价方法	3
5.2.1 服务器产品	3
5.2.2 个人计算机产品	6
5.3 计分方法	8
参考文献	9

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 5 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：工业和信息化部软件与集成电路促进中心、中国电子信息产业发展研究院、公安部第一研究所、中国软件评测中心、中国电子技术标准化研究院、浪潮电子信息产业股份有限公司、中国长城科技集团股份有限公司、华为技术有限公司、联想(北京)有限公司、曙光信息产业股份有限公司、新华三技术有限公司、海光信息技术有限公司、北京华胜天成信息技术发展有限公司。

本部分主要起草人：刘龙庚、王闯、韩煜、王超、叶润国、李海涛、翟艳芬、杜晓黎、张东、朱瑞瑾、石明、林俊、樊洞阳、王玮、葛小宇、王松宇、杨晓君、施光源、万晓兰、李汝鑫、张榆、王宇航、陈彦灵、马士民、荣志刚、王海洋。

引 言

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,为提高通用计算机产品安全可控水平,防范网络安全风险,维护国家和公共安全,满足通用计算机产品应用方安全可控需求,增强应用方使用信心,促进通用计算机产业的健康、快速发展,特制定 GB/T 36630 的本部分。

本部分评价对象为通用计算机产品,评价内容为通用计算机产品的安全可控程度,涵盖通用计算机产品的设计、生产、服务保障等环节。

本部分所述安全可控评价指标主要用于评价通用计算机产品的安全可控程度,不包含对产品本身安全功能和安全性能的评价。安全可控只是通用计算机产品的一个属性,如需评价安全功能和安全性能等其他属性,可参照相关国家标准。



信息安全技术

信息技术产品安全可控评价指标

第5部分：通用计算机

1 范围

GB/T 36630 的本部分规定了通用计算机产品的相关概念,并给出了安全可控评价的指标项及相应的评价方法。

本部分适用于评价实施方对通用计算机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

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

3 术语和定义、缩略语

3.1 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。

3.1.1

服务器 server

一个管理资源并为用户提供服务的计算设备。

注:本部分中的服务器主要包括 X86 服务器、Power 服务器、ARM 服务器等。

3.1.2

个人计算机 personal computer

由硬件系统和软件系统组成,能独立运行并完成特定功能的设备。

注:本部分中的个人计算机主要包括台式计算机、笔记本、一体机等,但不包括手机和平板等移动计算设备。

3.1.3

通用计算机 general purpose computer

具备计算机基本组件和核心功能的规模化产品,主要包括服务器和个人计算机两大类。

3.2 缩略语

下列缩略语适用于本文件。

BMC:基板管理控制器(Baseboard Management Controller)

BIOS:基本输入输出系统(Basic Input Output System)

4 评价指标项

依据 GB/T 36630.1—2018 中 5.2.1 的评价指标体系框架,结合通用计算机产品自身特点设定了评

价指标项。在本部分中,没有为通用计算机安全可控评价设置优先评价项。在一般评价项方面,选取了产品设计实现透明性、产品设计验证、产品重现能力、产品安全生态适应性、产品持续供应能力、产品供应链保障能力、产品服务保障能力等七个指标项,如表 1 所示。

表 1 通用计算机安全可控评价指标项及指标说明

编号	指标项	指标说明
1	产品设计实现透明性	根据产品供应方所提供的关键技术相关材料的真实性、可核查性、规范性和完备性,对其设计实现透明性进行评价,必要时可通过技术举证的方式辅助评价
2	产品设计验证	对产品硬件部分的设计验证环境、设计验证充分性、设计验证结果与产品一致性等进行评价,必要时可通过技术手段等方式进行评价
3	产品重现能力	对产品软件部分的重现环境、重现充分性、重现结果与产品一致性等进行评价,必要时可通过技术手段等方式进行评价
4	产品安全生态适应性	对产品所适配的操作系统等软件产品的安全可控程度和密码合规性 ^a 进行评价,必要时可通过技术测试的方式辅助评价
5	产品持续供应能力	对产品供应方的产品供应情况和核心团队情况进行评价
6	产品供应链保障能力	对产品核心部件安全可控程度,以及供应链各环节关键要素的可追溯性和供应稳定性进行评价
7	产品服务保障能力	对产品供应方的服务及时性和规范性进行评价
^a 本部分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 评价方法

5.1 评价材料要求

评价材料包括提供给评价实施方的提交材料和供评价实施方现场核查的验证材料。提交材料包括但不限于产品样品、供应方基本情况、产品基本信息、指标符合性证明文件等,验证材料则包括能证明产品安全可控的相关材料。验证材料可保存在由产品供应方提供的核查环境中。评价材料要求如下:

a) 真实性

产品供应方所提供材料应真实反映通用计算机产品指定关键技术的工作原理、设计技术和实现过程,并确保产品设计验证和重现结果与市场销售的产品一致。

b) 可核查性

产品供应方应确保所提供材料可核查,并为评价实施方核查提供必要的技术支持,包括支持必要技术手段进行验证。

c) 规范性

产品供应方所提供材料应符合业界通行标准和规范,能够支持评价实施方对相应技术原理和实现机制的准确理解。

d) 完备性

产品供应方所提供材料应覆盖本标准所指定的所有材料。

5.2 指标评价方法

5.2.1 服务器产品

服务器包括产品设计实现透明性、产品设计验证、产品重现能力、产品安全生态适应性、产品持续供应能力、产品供应链保障能力、产品服务保障能力七个指标项,具体如表 2 所示。

表 2 服务器指标评价表

指标项	考查内容		分值	评分说明
产品设计实现透明性	处理器互连技术	多路处理器互连技术	3	多路处理器互连技术相关材料满足真实性、可核查性、规范性和完备性的要求。(3分) 多路处理器互连技术相关材料满足真实性和可核查性,但不满足规范性或完备性的要求。(1分) 多路处理器互连技术相关材料不满足真实性或可核查性的要求。(0分)
		板上互连技术	3	板上互连技术相关材料满足真实性、可核查性、规范性和完备性的要求。(3分) 板上互连技术相关材料满足真实性和可核查性,但不满足规范性或完备性的要求。(1分) 板上互连技术相关材料不满足真实性或可核查性的要求。(0分)
	整机平台设计技术	主板设计技术	3	主板设计技术相关材料满足真实性、可核查性、规范性和完备性的要求。(3分) 主板设计技术相关材料满足真实性和可核查性,但不满足规范性或完备性的要求。(1分) 主板设计技术相关材料不满足真实性或可核查性的要求。(0分)
		基础架构设计技术(磁盘阵列、中央处理器布局等)	3	基础架构设计技术相关材料满足真实性、可核查性、规范性和完备性的要求。(3分) 基础架构设计技术相关材料满足真实性和可核查性,但不满足规范性或完备性的要求。(1分) 基础架构设计技术相关材料不满足真实性或可核查性的要求。(0分)
	整机管理与开发技术	BMC 开发技术	3	BMC 开发技术相关材料满足真实性、可核查性、规范性和完备性的要求。(3分) BMC 开发技术相关材料满足真实性和可核查性,但不满足规范性或完备性的要求。(1分) BMC 开发技术相关材料不满足真实性或可核查性的要求。(0分)
		BIOS 开发技术	3	BIOS 开发技术相关材料满足真实性、可核查性、规范性和完备性的要求。(3分) BIOS 开发技术相关材料满足真实性和可核查性,但不满足规范性或完备性的要求。(1分) BIOS 开发技术相关材料不满足真实性或可核查性的要求。(0分)

表 2 (续)

指标项	考查内容		分值	评分说明
产品设计实现透明性	整机管理与开发技术	随机管理软件	3	随机管理软件相关材料满足真实性、可核查性、规范性和完备性的要求。(3分) 随机管理软件相关材料满足真实性和可核查性,但不满足规范性或完备性的要求。(1分) 随机管理软件相关材料不满足真实性或可核查性的要求。(0分)
	可靠性、可用性和可维护性设计技术		3	可靠性、可用性和可维护性设计技术相关材料满足真实性、可核查性、规范性和完备性的要求。(3分) 可靠性、可用性和可维护性设计技术相关材料满足真实性和可核查性,但不满足规范性或完备性的要求。(1分) 可靠性、可用性和可维护性设计技术相关材料不满足真实性或可核查性的要求。(0分)
	整机测试和诊断技术(包括但不限于测试工具、后期远程维护工具)		3	整机测试和诊断技术相关材料满足真实性、可核查性、规范性和完备性的要求。(3分) 整机测试和诊断技术相关材料满足真实性和可核查性,但不满足规范性或完备性的要求。(1分) 整机测试和诊断技术相关材料不满足真实性或可核查性的要求。(0分)
产品设计验证	验证环境		4	产品供应方提供产品设计验证环境,产品设计验证能力可核查。(4分) 产品供应方无法提供产品设计验证环境,产品设计验证能力不可核查。(0分)
	验证充分性		4	可完整验证产品设计全过程,能够说明各关键技术的原理和实现机制。(4分) 不能验证产品设计过程,或不能说明相应关键技术的原理和实现机制。(0分)
	验证结果与产品一致性		4	验证环境中板卡等硬件产品与市场销售产品的硬件一致。(4分) 验证环境中板卡等硬件产品与市场销售产品的硬件不一致 ^a 。(0分)
产品重现能力	重现环境		4	产品供应方提供产品重现环境,产品重现能力可核查。(4分) 产品供应方无法提供产品重现环境,产品重现能力不可核查。(0分)
	重现充分性		4	可完整验证产品重现全过程,能够说明各关键技术的原理和实现机制。(4分) 不能验证产品重现过程,或不能说明相应关键技术的原理和实现机制。(0分)
	重现结果与产品一致性		4	设计验证环境中 BIOS 等的源代码编译结果与市场销售产品的软件一致。(4分) 设计验证环境中 BIOS 等的源代码编译结果与市场销售产品的软件不一致 ^b 。(0分)

表 2 (续)

指标项	考查内容		分值	评分说明
产品安全生态适应性	操作系统适配能力		5	产品所能够适配操作系统的安全可控程度(参考操作系统评价指标)与本项的分值按比例相乘
	密码合规性		6	产品涉及的密码算法符合国家密码管理要求。(6分) 产品涉及的密码算法不符合国家密码管理要求。(0分)
产品持续供应能力	产品供应情况		5	产品供应方能够保证产品持续供应,不会造成产品供应中断。(5分) 产品供应方不能保证产品持续供应,易造成产品供应中断。(0分)
	核心团队情况		5	产品供应方能够保证服务器核心团队持续研发,有能力维持关键技术延续和发展。(5分) 产品供应方不能保证服务器核心团队持续研发,无法维持关键技术延续和发展。(0分)
产品供应链保障能力	核心部件安全可控程度	中央处理器	8	产品采用的中央处理器的安全可控程度(参考中央处理器评价指标)与本项的分值按比例相乘
		其他核心部件	5	产品采用的内存、硬盘、控制芯片等其他核心部件均与供应方签订了完备的供应协议,供应链各环节清晰可追溯,不会造成产品供应中断。(5分) 产品采用的内存、硬盘、控制芯片等其他核心部件的供应协议不完备,或供应链某些环节无法追溯,或易造成产品供应中断。(0分)
	供应链可追溯性		5	能够清晰展示产品研发、设计、生产各环节的关键要素(涵盖设计工具、知识产权等),要素信息清晰可追溯,不会造成相关要素供应中断。(5分) 不能够清晰展示产品研发、设计、生产各环节的关键要素,或要素信息无法追溯,或者易造成产品供应中断。(0分)
产品服务保障能力	服务及时性		5	拥有专业的本地服务团队,能够提供原厂级服务,具备面向全国范围内的产品应用方做出服务响应的能力,能提供及时有效的服务。(5分) 拥有专业的本地服务团队,具备面向全国范围内的产品应用方做出服务响应的能力,能提供及时有效的服务。(2分) 没有专业的本地服务团队,不能提供及时有效的服务。(0分)
	服务规范性		5	有明确的产品服务规范和质量承诺,建立了全面的产品服务体系并通过权威第三方认证,能够保障产品在交付、维护(包括但不限于现场维护、远程维护)过程中的安全性。(5分) 有明确的产品服务规范和质量承诺,建立了产品服务体系但未通过权威第三方认证,能够保障产品在交付、维护(包括但不限于现场维护、远程维护)过程中的安全性。(2分) 没有明确的产品服务规范或质量承诺,或无法严格执行,不能够保障产品在交付、维护(包括但不限于现场维护、远程维护)过程中的安全性。(0分)
<p>^a 若验证结果与产品不一致,则产品设计实现透明性相关材料不满足真实性要求。</p> <p>^b 若重现结果与产品不一致,则产品设计实现透明性相关材料不满足真实性要求。</p>				

5.2.2 个人计算机产品

个人计算机包括产品设计实现透明性、产品设计验证、产品安全生态适应性、产品持续供应能力、产品供应链保障能力、产品服务保障能力六个指标项，具体如表 3 所示。

表 3 个人计算机指标评价表

指标项	考查内容		分值	评分说明
产品设计实现透明性	整机平台设计技术	主板设计技术	4	主板设计技术相关材料满足真实性、可核查性、规范性和完备性的要求。(4分) 主板设计技术相关材料满足真实性和可核查性,但不满足规范性或完备性的要求。(2分) 主板设计技术相关材料不满足真实性或可核查性的要求。(0分)
		基础架构设计技术	4	基础架构设计技术相关材料满足真实性、可核查性、规范性和完备性的要求。(4分) 基础架构设计技术相关材料满足真实性和可核查性,但不满足规范性或完备性的要求。(2分) 基础架构设计技术相关材料不满足真实性或可核查性的要求。(0分)
	整机管理与开发技术	随机管理软件	4	随机管理软件相关材料满足真实性、可核查性、规范性和完备性的要求。(4分) 随机管理软件相关材料满足真实性和可核查性,但不满足规范性或完备性的要求。(2分) 随机管理软件相关材料不满足真实性或可核查性的要求。(0分)
	可靠性、可用性和可维护性设计技术		4	可靠性、可用性和可维护性设计技术相关材料满足真实性、可核查性、规范性和完备性的要求。(4分) 可靠性、可用性和可维护性设计技术相关材料满足真实性和可核查性,但不满足规范性或完备性的要求。(2分) 可靠性、可用性和可维护性设计技术相关材料不满足真实性或可核查性的要求。(0分)
	整机测试和诊断技术(包括但不限于测试工具、后期远程维护工具)		4	整机测试和诊断技术相关材料满足真实性、可核查性、规范性和完备性的要求。(4分) 整机测试和诊断技术相关材料满足真实性和可核查性,但不满足规范性或完备性的要求。(2分) 整机测试和诊断技术相关材料不满足真实性或可核查性的要求。(0分)
产品设计验证	验证环境		4	产品供应方提供产品设计验证环境,产品设计验证能力可核查。(4分) 产品供应方无法提供产品设计验证环境,产品设计验证能力不可核查。(0分)

表 3 (续)

指标项	考查内容		分值	评分说明
产品设计验证	验证充分性		4	可完整验证产品设计全过程,能够说明各关键技术的原理和实现机制。(4分) 不能验证产品设计过程,或不能说明相应关键技术的原理和实现机制。(0分)
	验证结果与产品一致性		4	设计验证环境中板卡等与市场销售产品一致。(4分) 设计验证环境中板卡等与市场销售产品不一致。(0分)
产品安全生态适应性	办公套件适配能力		5	产品所能够适配办公套件的安全可控程度(参考办公套件评价指标)与本项的分值按比例相乘
	密码合规性		6	产品涉及的密码算法符合国家密码管理要求。(6分) 产品涉及的密码算法不符合国家密码管理要求。(0分)
产品持续供应能力	产品供应情况		5	产品资本方或供应方能够保证产品持续供应,不会造成产品供应中断。(5分) 产品资本方或供应方不能保证产品持续供应,易造成产品供应中断。(0分)
	核心团队情况		5	产品供应方能够保证个人计算机核心团队持续研发,有能力维持关键技术延续和发展。(5分) 产品供应方不能保证个人计算机核心团队持续研发,无法维持关键技术延续和发展。(0分)
产品供应链保障能力	核心部件安全可控程度	中央处理器	9	产品采用的中央处理器的安全可控程度(参考中央处理器评价指标)与本项的分值按比例相乘
		操作系统	9	产品采用的操作系统的安全可控程度(参考操作系统评价指标)与本项的分值按比例相乘
		BIOS	5	产品采用的 BIOS 与供应方签订了完备的供应协议,供应链各环节清晰可追溯,BIOS 供应中断风险可控。(5分) 产品采用的 BIOS 的供应协议不完备,或供应链部分环节无法追溯,或 BIOS 供应中断风险较大。(0分)
		其他核心部件	9	产品采用的内存、硬盘、控制芯片等其他核心部件均与供应方签订了完备的供应协议,供应链各环节清晰可追溯,不会造成产品供应中断。(9分) 产品采用的内存、硬盘、控制芯片等其他核心部件的供应协议不完备,或供应链某些环节无法追溯,或易造成产品供应中断。(0分)
	供应链可追溯性		5	能够清晰展示供应链各环节的关键要素(涵盖设计工具、知识产权等),要素信息清晰可追溯,相关要素供应中断风险可控。(5分) 不能够清晰展示供应链各环节的关键要素,或要素信息无法追溯,或关键要素供应中断风险较大。(0分)

表 3 (续)

指标项	考查内容	分值	评分说明
产品服务保障能力	服务及时性	5	拥有专业的本地服务团队,能够提供原厂级服务,具备面向全国范围内的产品应用方做出服务响应的能力,能提供及时有效的服务。(5分) 拥有专业的本地服务团队,具备面向全国范围内产品应用方做出服务响应的能力,能提供及时有效的服务。(2分) 没有专业的本地服务团队,或不能提供及时有效的服务。(0分)
	服务规范性	5	有明确的产品服务规范和质量承诺,建立了全面的产品服务体系并通过权威第三方认证,能够保障产品在交付、维护(包括但不限于现场维护、远程维护)过程中的安全性。(5分) 有明确的产品服务规范和质量承诺,建立了产品服务体系,能够保障产品在交付、维护(包括但不限于现场维护、远程维护)过程中的安全性。(2分) 没有明确的产品服务规范或质量承诺,或无法严格执行,不能够保障产品在交付、维护(包括但不限于现场维护、远程维护)过程中的安全性。(0分)
^a 若验证结果与产品不一致,则产品设计实现透明性相关材料不满足真实性要求。			

5.3 计分方法

具体计分方法如下:

- a) 针对服务器产品,依据表 2 对各指标项进行打分,因被评价方原因无法核查的考查内容得 0 分,若指标项各考查内容得分分别为 $s = \{s_1, s_2, \dots, s_n\}$,则服务器产品最后得分 $score = \sum_{1 \leq i \leq n} s_i$,其中 s_i 为各考查内容得分, n 为各指标项考查内容的总数量;
- b) 针对个人计算机产品,依据表 3 对各指标项进行打分,因被评价方原因无法核查的考查内容得 0 分,若指标项各考查内容得分分别为 $s = \{s_1, s_2, \dots, s_n\}$,则个人计算机产品最后得分为 $score = \sum_{1 \leq i \leq n} s_i$,其中 s_i 为各考查内容得分, n 为各指标项考查内容的总数量;
- c) 对于服务器和个人计算机产品设计实现透明性指标项,若产品不涉及其对应指标项中的部分考查内容,可按照该指标项其他考查内容的得分比例计算该考查内容得分。

参 考 文 献

- [1] GB/T 9813.3—2017 计算机通用规范 第3部分:服务器
- [2] GB/T 21028—2007 信息安全技术 服务器安全技术要求
- [3] GB/T 25063—2010 信息安全技术 服务器安全测评要求
- [4] GB/T 32925—2016 信息安全技术 政府联网计算机终端安全管理基本要求

