ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36630.2—2018

信息安全技术
信息技术产品安全可控评价指标
第2部分：中央处理器

Information security technology—Controllability evaluation index for security of information technology products—Part 2: Central processing unit

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

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 2 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、工业和信息化部软件与集成电路促进中心、中国电子技术标准化研究院、公安部第一研究所、中国软件评测中心、国家信息技术安全研究中心、中国信息安全测评中心、龙芯中科技术有限公司、上海高性能集成电路设计中心、国防科技大学、北京大学、清华大学、展讯通信有限公司、上海兆芯集成电路有限公司、天津飞腾信息技术有限公司、成都海光集成电路设计有限公司、贵州华芯通半导体技术有限公司等。

本部分主要起草人：王闯、范兵、李海涛、韩煜、张戈、叶润国、朱英、张承义、陆俊林、刘雷波、方进社、余红斌、高金萍、李冰、王鹏、陈斐利、刘新春、孙开本、刘权、刘龙庚、巨鹏锦、王超、李英的、王蓓蓓、马士民、翟艳芬、荣志刚、姚永斌。

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，为提高中央处理器产品安全可控水平，防范网络安全风险，维护国家和公共安全，进而满足中央处理器产品应用方安全可控需求，增强应用方使用信心，促进中央处理器产业的健康、快速发展，特制定 GB/T 36630 的本部分。

本部分评价对象为中央处理器产品，评价内容为中央处理器产品的安全可控程度，涵盖中央处理器产品的设计、流片、封装、测试、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中央处理器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。安全可控只是中央处理器产品的一个属性，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2部分:中央处理器

1 范围

GB/T 36630的本部分规定了中央处理器产品的相关概念,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中央处理器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

中央处理器 central processing unit

由运算器、控制器、寄存器和实现它们之间联系的各类总线,以及包含在同一产品内的其他功能模块组成的集成电路。

3.1.2

知识产权核 intellectual property core

包含软核、硬核和固核在内的,可通过协议由一方提供给另一方,形式为逻辑单元、芯片设计的可重复使用模块。

3.2 缩略语

下列缩略语适用于本文件。

IP核:知识产权核(Intellectual Property Core)

I/O:输入/输出(Input/Output)

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,结合中央处理器自身特点设定了评价指标项。在优先评价项方面,根据国家法律和政策要求,产品供应方应合法拥有或使用产品相关知识产权,包

括通过自主研发、合作研发或外部授权等方式获得的知识产权，为此选取产品知识产权状况为优先评价项。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、产品关键技术研发能力、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　中央处理器安全可控评价指标项及指标说明

编号	指标项	指标说明
1	产品知识产权状况[a]	根据产品供应方所提供的知识产权拥有情况、获得外部授权情况及知识产权纠纷情况等相关材料，对其产品知识产权进行评价
2	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，必要时可通过技术手段等方式进行评价
3	产品设计验证	对产品设计验证环境、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
4	产品关键技术研发能力	对产品供应方关键技术掌控能力、基于安全可控需求修改指令集架构及修改或替换关键IP核[b]的权限及能力进行评价
5	产品安全生态适应性	对产品所适配操作系统的安全可控程度和密码合规性[c]进行评价，必要时可通过技术测试的方式辅助评价
6	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
7	产品供应链保障能力	对产品设计环节、流片环节、封装环节、测试环节的供应链保障能力进行评价
8	产品服务保障能力	对产品供应方服务及时性和服务质量进行评价

[a] 特指中央处理器产品相关知识产权，包括但不限于商标、著作权、专利、集成电路布图。

[b] 关键IP核包括但不限于密码模块、高速I/O接口。

[c] 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中央处理器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部分所要求的所有材料。

5.2　指标评价方法

5.2.1　优先评价项评价

本部分将产品知识产权状况作为优先评价项，若发现被评价产品知识产权存在经司法判决且未得

到妥善处理解决的侵权行为，则该产品评价分值为0分。

5.2.2 一般评价项评价

一般评价项的相关内容见表2。

表2 中央处理器指标评价表

指标项	考查内容		分值	评分说明
产品设计实现透明性[a]	指令集架构	指令定义(包括但不限于所有公有指令、私有指令)	2	指令定义相关材料满足真实性、可核查性、规范性和完备性的要求。(2分) 指令定义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) 指令定义相关材料不满足真实性或可核查性的要求。(0分)
		编程模型(包括但不限于数据类型、寄存器结构)	2	编程模型相关材料满足真实性、可核查性、规范性和完备性的要求。(2分) 编程模型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) 编程模型相关材料不满足真实性或可核查性的要求。(0分)
		存储管理(包括但不限于寻址模式、地址类型)	2	存储管理相关材料满足真实性、可核查性、规范性和完备性的要求。(2分) 存储管理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) 存储管理相关材料不满足真实性或可核查性的要求。(0分)
		中断及异常处理	2	中断及异常处理相关材料满足真实性、可核查性、规范性和完备性的要求。(2分) 中断及异常处理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) 中断及异常处理相关材料不满足真实性或可核查性的要求。(0分)
		系统模式(包括但不限于调试(debug)模式、高级权限模式)	2	系统模式相关材料满足真实性、可核查性、规范性和完备性的要求。(2分) 系统模式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) 系统模式相关材料不满足真实性或可核查性的要求。(0分)
	微架构设计	核心微结构(包括但不限于指令流水线、运算流水线、访存流水线)	2	核心微结构相关材料满足真实性、可核查性、规范性和完备性的要求。(2分) 核心微结构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) 核心微结构相关材料不满足真实性或可核查性的要求。(0分)
		I/O接口微结构	2	I/O接口微结构相关材料满足真实性、可核查性、规范性和完备性的要求。(2分) I/O接口微结构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) I/O接口微结构相关材料不满足真实性或可核查性的要求。(0分)
		片上互连微结构	2	片上互连微结构相关材料满足真实性、可核查性、规范性和完备性的要求。(2分) 片上互连微结构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) 片上互连微结构相关材料不满足真实性或可核查性的要求。(0分)
		片上存储微结构(包括但不限于缓存(Cache)一致性协议、片上内存控制器)	2	片上存储微结构相关材料满足真实性、可核查性、规范性和完备性的要求。(2分) 片上存储微结构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) 片上存储微结构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[a]	微架构设计	硬件设置管理（包括但不限于微码）	2	硬件设置管理相关材料满足真实性、可核查性、规范性和完备性的要求。（2 分） 硬件设置管理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） 硬件设置管理相关材料不满足真实性或可核查性的要求。（0 分）
	物理设计	版图规划	2	版图规划相关材料满足真实性、可核查性、规范性和完备性的要求。（2 分） 版图规划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） 版图规划相关材料不满足真实性或可核查性的要求。（0 分）
		布局布线	2	布局布线相关材料满足真实性、可核查性、规范性和完备性的要求。（2 分） 布局布线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） 布局布线相关材料不满足真实性或可核查性的要求。（0 分）
		标准单元库设计	2	标准单元库设计相关材料满足真实性、可核查性、规范性和完备性的要求。（2 分） 标准单元库设计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） 标准单元库设计相关材料不满足真实性或可核查性的要求。（0 分）
		全定制单元设计	2	全定制单元设计相关材料满足真实性、可核查性、规范性和完备性的要求。（2 分） 全定制单元设计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） 全定制单元设计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	前端设计验证环境	5	产品供应方提供前端设计验证环境，产品设计验证能力可核查。（5 分） 产品供应方提供核心部件前端设计验证环境，产品设计验证能力可核查。（3 分） 产品供应方无法提供前端设计验证环境，产品设计验证能力不可核查。（0 分）
		物理设计验证环境	5	产品供应方提供物理设计验证环境，产品设计验证能力可核查。（5 分） 产品供应方提供核心部件物理设计验证环境，产品设计验证能力可核查。（3 分） 产品供应方无法提供物理设计验证环境，产品设计验证能力不可核查。（0 分）
		测试环节验证环境	5	产品供应方提供测试环节验证环境，产品设计验证能力可核查。（5 分） 产品供应方提供核心部件测试环节验证环境，产品设计验证能力可核查。（3 分） 产品供应方无法提供测试环节验证环境，产品设计验证能力不可核查。（0 分）
	验证充分性		6	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。（6 分） 可验证产品核心部件设计全过程，能够说明相应关键技术的原理和实现机制。（3 分） 不能验证产品核心部件设计过程，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	设计验证结果与市场销售产品一致。（4 分） 设计验证结果与市场销售产品不一致[b]。（0 分）

表 2（续）

指标项	考查内容		分值	评分说明
产品关键技术研发能力	指令集架构	指令集架构修改权限	6	产品指令集架构为产品供应方自主设计。（6 分） 产品供应方有权或通过获得外部授权方式扩展指令。（4 分） 产品供应方不具备修改指令的权限。（0 分）
		指令集架构修改能力	4	产品供应方具有指令集架构修改权限，能够自主扩展指令，并已经应用到产品中。（4 分） 产品供应方具有指令集架构修改权限，能够证明具备自主扩展指令的能力。（2 分） 产品供应方不具备自主扩展指令的能力。（0 分）
	关键 IP 核研发能力		4	产品供应方可基于安全可控需求研发关键 IP 核，并应用到产品中。（4 分） 产品供应方可基于安全可控需求对关键 IP 核进行修改，并应用到产品中。（2 分） 产品供应方可基于安全可控需求对关键 IP 核进行替换，并应用到产品中。（1 分） 产品供应方不具备对关键 IP 核进行修改或替换的能力。（0 分）
产品安全生态适应性	操作系统适配能力		4	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		4	产品涉及的密码算法符合国家密码管理要求。（4 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		4	产品供应方能够保证产品持续供应，产品供应中断风险可控。（4 分） 产品供应方不能保证产品持续供应，产品供应中断风险较大。（0 分）
	核心团队情况		3	产品供应方具有稳定的中央处理器核心团队，有能力维持关键技术延续和发展。（3 分） 产品供应方的中央处理器核心团队稳定性较差，无法维持关键技术延续和发展。（0 分）
产品供应链保障能力	设计环节供应链保障能力		4	能够清晰展示产品设计环节供应链核心要素（涵盖 IP、设计工具等），要素信息清晰可追溯，相关要素供应中断风险可控。（4 分） 不能清晰展示产品设计环节供应链核心要素，或要素信息无法追溯，或相关要素供应中断风险较大。（0 分）
	流片环节供应链保障能力		2	能够清晰展示产品流片环节供应链核心要素（涵盖服务、原材料、设备、工艺等），要素信息清晰可追溯，相关要素供应中断风险可控。（2 分） 不能清晰展示产品流片环节供应链核心要素，或要素信息无法追溯，或相关要素供应中断风险较大。（0 分）
	封装环节供应链保障能力		2	能够清晰展示产品封装环节供应链核心要素（涵盖服务、材料、设备等），要素信息清晰可追溯，相关要素供应中断风险可控。（2 分） 不能清晰展示产品封装环节供应链核心要素，或要素信息无法追溯，或相关要素供应中断风险较大。（0 分）
	测试环节供应链保障能力		2	能够清晰展示产品测试环节供应链核心要素（涵盖服务、设备等），要素信息清晰可追溯，相关要素供应中断风险可控。（2 分） 不能清晰展示产品测试环节供应链核心要素，或要素信息无法追溯，或相关要素供应中断风险较大。（0 分）

表 2（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	4	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。（4 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，或不能提供及时有效的服务。（0 分）
	服务规范性	4	有明确的产品服务质量承诺，建立了全面的产品服务体系，能够保证产品服务过程的安全性。（4 分） 没有明确的产品服务质量承诺或有承诺不履行，或没有建立产品服务体系，或产品服务过程存在安全隐患。（0 分）
[a] 通过技术手段等方式进行评价的，评价结果可作为打分依据。 [b] 若设计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) 首先进行优先评价项评价，如果未通过，则得分为 0 分；

b) 如果优先评价项评价通过，则依据表 2 对一般评价项进行打分，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 $s=\{s_1,s_2,\cdots,s_n\}$，则最后得分 $score=\sum_{1\leqslant i\leqslant n}s_i$，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) 对于产品设计实现透明性指标项，若产品不涉及该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 16464—1996 半导体器件 集成电路 第1部分:总则

[2] GB/T 22186—2016 信息安全技术 具有中央处理器的IC卡芯片安全技术要求

[3] FIPS Publication 140-2 Security requirements for cryptographic modules