ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36630.3—2018

信息安全技术
信息技术产品安全可控评价指标
第3部分:操作系统

Information security technology—Controllability evaluation index for security of information technology products—Part 3:Operating system

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

知识星球https://t.zsxq.com/JmiaeUR

目　　次

知识星球https://t.zsxq.com/JmiaeUR

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3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、中国电子技术标准化研究院、公安部第一研究所、工业和信息化部软件与集成电路促进中心、中国信息安全研究院有限公司、中国软件评测中心、中国信息安全测评中心、中标软件有限公司、普华基础软件有限公司、北京凝思科技有限公司等。

本部分主要起草人：李震宁、王闯、叶润国、李海涛、韩煜、左晓栋、武校田、郭同彬、翟艳芬、贾炜、刘权、刘龙庚、冯伟、王超、张猛、马士民、荣志刚、董军平、邓辉、韦安垒。

知识星球https://t.zsxq.com/JmiaeUR

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，为提高操作系统产品安全可控水平，防范网络安全风险，维护国家和公共安全，进而满足操作系统产品应用方安全可控需求，增强应用方使用信心，促进操作系统产业的健康、快速发展，特制定 GB/T 36630 的本部分。

本部分评价对象是操作系统产品，评价内容为操作系统产品的安全可控程度，涵盖操作系统产品的研发、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操作系统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。安全可控只是操作系统产品的一个属性，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。

知识星球https://t.zsxq.com/JmiaeUR

信息安全技术
信息技术产品安全可控评价指标
第3部分:操作系统

1 范围

GB/T 36630的本部分规定了操作系统产品的相关概念,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操作系统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

GB/T 25069—2010界定的以及下列术语和定义适用于本文件。

3.1

操作系统 operating system

用于管理硬件资源、控制程序运行、提供人机界面,并为应用软件提供支持的一种系统软件产品。

注:包括但不限于服务器、个人计算机、手机平板、网络设备、存储设备所使用的操作系统产品。

3.2

操作系统内核 operating system kernel

操作系统中负责系统进程、内存、设备驱动、文件和网络系统等核心功能的计算机程序。

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,结合操作系统自身特点设定了评价指标项。在本部分中,没有为操作系统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、产品重现能力、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、产品服务保障能力和数据处理规范性等八个指标项,如表1所示。

知识星球https://t.zsxq.com/JmiaeUR

表 1　操作系统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关键模块相关材料的真实性、可核查性、规范性和完备性对其设计实现透明性进行评价，必要时通过技术手段辅助评价
2	产品重现能力	对产品重现环境、产品重现充分性、重现结果与产品一致性等进行评价，必要时通过技术手段辅助评价
3	产品关键技术研发能力	对产品供应方定制关键模块的权限和能力进行评价，涵盖身份鉴别、访问控制、安全审计等关键功能模块和内存管理、设备管理、进程管理等操作系统内核关键模块
4	产品安全生态适应性	对产品所适配中央处理器的安全可控程度、内部关键模块接口和应用编程接口的开放性，以及密码合规性[a] 进行评价
5	产品持续供应能力	对产品供应方的产品供应情况、核心团队情况和产品交付管理进行评价
6	产品供应链保障能力	对产品供应链的可追溯性和供应稳定性进行评价
7	产品服务保障能力	对产品技术支持服务、漏洞响应服务、延保服务能力等保障能力进行评价
8	数据处理规范性	涉及产品应用方个人信息和重要数据的，对产品收集、传输、存储和处理行为的规范性进行评价
[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操作系统产品指定关键技术的工作原理、设计技术和实现过程，并确保产品重现结果与市场销售产品一致；

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

各指标项相关内容见表 2。

知识星球https://t.zsxq.com/JmiaeUR

表 2　操作系统指标评价表

指标项	考查内容		分值	评分说明
产品设计实现透明性	资源管理技术	内存管理技术	2	内存管理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。(2 分) 内存管理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) 内存管理技术相关材料不满足真实性或可核查性的要求。(0 分)
		设备管理技术	2	设备管理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。(2 分) 设备管理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) 设备管理技术相关材料不满足真实性或可核查性的要求。(0 分)
		网络通讯技术	2	网络通讯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。(2 分) 网络通讯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) 网络通讯技术相关材料不满足真实性或可核查性的要求。(0 分)
		文件系统	2	文件系统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) 文件系统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) 文件系统相关材料不满足真实性或可核查性的要求。(0 分)
	系统管理技术	进程控制技术	2	进程控制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。(2 分) 进程控制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) 进程控制技术相关材料不满足真实性或可核查性的要求。(0 分)
		身份标识和鉴别技术	2	身份标识和鉴别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。(2 分) 身份标识和鉴别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) 身份标识和鉴别技术相关材料不满足真实性或可核查性的要求。(0 分)
		访问控制技术	2	访问控制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。(2 分) 访问控制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) 访问控制技术相关材料不满足真实性或可核查性的要求。(0 分)
		安全管理技术	2	安全管理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。(2 分) 安全管理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) 安全管理技术相关材料不满足真实性或可核查性的要求。(0 分)

知识星球https://t.zsxq.com/JmiaeUR

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	数据和应用管理技术	软件管理技术	2	软件管理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。（2 分） 软件管理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） 软件管理技术相关材料不满足真实性或可核查性的要求。（0 分）
		数据保护技术	2	数据保护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。（2 分） 数据保护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） 数据保护技术相关材料不满足真实性或可核查性的要求。（0 分）
产品重现能力	产品重现环境	产品研发重现环境	5	产品供应方提供研发重现环境，产品重现能力可核查。（5 分） 产品供应方提供核心功能组件研发重现环境，产品重现能力可核查。（3 分） 产品供应方无法提供研发重现环境，产品重现能力不可核查。（0 分）
		产品测试重现环境	4	产品供应方提供测试重现环境，产品重现能力可核查。（4 分） 产品供应方提供核心功能组件测试重现环境，产品重现能力可核查。（2 分） 产品供应方无法提供测试重现环境，产品重现能力不可核查。（0 分）
		产品升级维护重现环境	3	产品供应方提供升级维护重现环境（含补丁和升级包研发、测试和分发等环节），产品重现能力可核查。（3 分） 产品供应方无法提供升级维护重现环境，产品重现能力不可核查。（0 分）
	产品重现充分性		6	可完整重现产品研发、测试和升级维护全过程，能够说明各关键技术的原理和实现机制。（6 分） 可完整重现核心功能组件（含补丁和升级包）研发、测试和升级维护全过程，能够说明相应关键技术的原理和实现机制。（3 分） 不能重现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）
	重现结果与产品一致性		4	产品重现环境中基于源代码的重现结果与市场销售产品一致。（4 分） 产品重现环境中基于源代码的重现结果与市场销售产品不一致[a]。（0 分）
产品关键技术研发能力	产品定制权限		2	产品由产品供应方自主研发，供应方拥有对产品的完整定制权限。（2 分） 产品供应方通过遵守开源协议或获得外部授权等方式获得完整定制权限。（1 分） 产品提供者不具有合法定制权限。（0 分）

知识星球https://t.zsxq.com/JmiaeUR

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	产品定制能力	功能定制能力	4	可基于应用方安全可控需求定制身份鉴别、访问控制、安全审计等关键功能模块，提供定制化产品。（4 分） 可证明具备基于应用安全可控需求定制关键功能模块的能力。（2 分） 不能对关键功能模块进行定制，也不提供定制服务。（0 分）
		内核定制能力	6	具备定制内存管理、设备管理、进程控制等操作系统内核关键模块的能力，提供定制化产品。（6 分） 可证明具备定制关键内核模块的能力。（3 分） 不能对关键内核模块进行定制，也不提供定制服务。（0 分）
产品安全生态适应性	中央处理器适配能力		4	产品适配 4 种以上指令集架构的中央处理器产品。（4 分） 产品适配 3 种指令集架构的中央处理器产品。（3 分） 产品适配 2 种指令集架构的中央处理器产品。（2 分） 产品适配 1 种指令集架构的中央处理器产品。（1 分）
	接口开放性	内部关键模块接口	3	产品中身份鉴别、访问控制、证书和密钥管理、安全审计以及密码算法等关键模块采用开放接口。（3 分） 产品关键模块的接口未采用开放接口。（0 分）
		应用编程接口	2	产品应用编程接口采用开放接口，包括但不限于 POSIX 标准。（2 分） 产品应用编程接口未采用开放接口。（0 分）
	密码合规性	密码算法	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）
		数字证书	3	产品涉及的数字证书符合国家及相关主管部门要求。（3 分） 产品涉及的数字证书不符合国家及相关主管部门要求。（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操作系统核心团队，能够保证产品的持续研发和生产，有能力维持关键技术延续和发展。（3 分） 产品供应方操作系统核心团队稳定性较差，无法维持关键技术延续和发展。（0 分）
	产品交付管理		3	产品供应方制定了完善的交付管理制度，实施了配套的交付管理方法和流程，保证产品不被破坏或篡改。（3 分） 产品供应方未制定完善的交付管理制度，或未实施配套的流程和方法，不能保证产品不被破坏或篡改。（0 分）

知识星球https://t.zsxq.com/JmiaeUR

表 2（续）

指标项	考查内容	分值	评分说明
产品供应链保障能力	供应链可追溯性	3	能够清晰展示产品供应链各环节核心要素（涵盖核心技术知识产权、开发工具等），要素信息清晰可追溯。（3 分） 不能清晰展示产品供应链各环节核心要素，或核心要素信息无法追溯。（0 分）
	供应稳定性	3	制定和实施了完善的供应链保障制度，能够保障产品研发生产各环节关键要素稳定性，相关要素供应中断风险可控。（3 分） 未制定或实施有效的供应链保障制度，供应中断风险较大。（0 分）
产品服务保障能力	服务及时性	2	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。（2 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。（1 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	2	有明确的产品服务承诺（包括提供完整的本地技术支持、本地漏洞响应服务等），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。（2 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）
	服务可持续性	2	产品生命周期结束后，产品供应方可根据产品应用方要求，免费或以合理价格，继续提供服务，与产品应用方签署规范的服务水平协议。（2 分） 产品生命周期结束后，产品供应方不能提供延保服务（0 分）
数据处理规范性	数据收集	2	产品只在必要时收集应用方的个人信息和重要数据，收集前获得应用方明示授权，并明示数据的使用目的和范围。（2 分） 产品在收集应用方的个人信息和重要数据前未经应用方明示授权，或未明示应用方数据使用的目的或范围。（0 分）
	数据传输	2	产品供应方对产品所收集数据的传输环节采取了充分的安全保障措施，并可验证。（2 分） 产品供应方未对产品所收集数据的传输环节采取充分的安全保障措施，或不可验证。（0 分）
	数据存储	2	产品运行过程中收集的应用方个人信息和重要数据在境内存储，采取了充分的保护措施，且向境外提供相关数据的流程符合国家规定。（2 分） 产品运行过程收集的应用方个人信息和重要数据不在境内存储，或未采取充分的保护措施，或向境外提供相关数据的流程不符合国家规定。（0 分）

知识星球https://t.zsxq.com/JmiaeUR

表 2（续）

指标项	考查内容	分值	评分说明
数据处理规范性	数据处理	2	产品供应方明确告知应用方个人信息和重要数据的处理目的，实际数据处理行为与预期一致，不侵犯应用方隐私，不危害国家安全和社会经济安全。（2 分） 产品供应方未告知应用方个人信息和重要数据的处理目的，或实际数据处理行为与预期不一致，或侵犯应用方隐私，或危害国家安全和社会经济安全。（0 分）
[a] 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。			

5.3 计分方法

具体计分方法如下：

a) 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 $s=\{s_1,s_2,\cdots,s_n\}$，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；

b) 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。

知识星球https://t.zsxq.com/JmiaeUR

参 考 文 献

[1] GB/T 17548—2008 信息技术 POSIX 标准符合性的测试方法规范和测试方法实现的要求和指南

[2] GB/T 20008—2005 信息安全技术 操作系统安全评估准则

[3] GB/T 20272—2006 信息安全技术 操作系统安全技术要求

[4] GB/T 32394—2015 信息技术 中文 Linux 操作系统运行环境扩充要求

[5] GB/T 32395—2015 信息技术 中文 Linux 操作系统应用编程接口(API)扩充要求

知识星球https://t.zsxq.com/JmiaeUR