ICS 35.040
CCS L 80

中华人民共和国国家标准

GB XXXXX—20XX

信息安全技术 网络安全专用产品安全技术要求

Information security technology—Security technical requirements of specialized cybersecurity products

（征求意见稿）

20XX－XX－XX 发布　　20XX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目 次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由公安部提出并归口。

引　言

为落实《中华人民共和国网络安全法》的第二十三条而制定本文件。网络安全专用产品应按照本文件的安全技术要求和对应产品的国家标准或行业标准的安全技术要求研发、测试和生产，测评机构也应按照本文件的安全技术要求和对应产品的国家标准或行业标准的安全技术要求对网络安全专用产品进行安全测评。

现有推荐性国家标准或行业标准主要是针对各类网络安全专用产品所需提供的不同安全功能要求和安全保障要求而提出，具体要求内容因产品类别的不同而有很大区别。本文件则是所有网络安全专用产品和其提供者均需满足的基线要求。

因此，本文件发布实施后，建议以本文件和各类不同的推荐性国家标准或行业标准相结合的方式对网络安全专用产品进行准入市场的检测和监督。

对于有相关配套推荐性国家标准或行业标准的网络安全专用产品，以本文件和对应的推荐性国家标准或行业标准为依据进行研发、测试、生产以及准入市场的检测和监督。

当本文件与推荐性国家标准或行业标准在内容要求上有不一致的地方时，以本文件为准。

信息安全技术 网络安全专用产品安全技术要求

1 范围

本文件规定了网络安全专用产品的安全功能要求、自身安全要求与安全保障要求。

本文件适用于指导在中华人民共和国境内销售或提供的网络安全专用产品的研发、测试、生产、服务以及准入市场的检测和监督等工作。

2 规范性引用文件

下列标准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 信息安全技术 术语

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

GB/T 35273—2020 信息安全技术 个人信息安全规范

3 术语和定义

GB/T 25069、GB/T 32921—2016和GB/T 35273—2020界定的以及下列术语和定义适用于本文件。

3.1

网络安全专用产品 specialized cybersecurity products

专门用于防范网络攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络和信息系统处于稳定可靠、可控运行的状态，以及保障网络数据完整性、保密性、可用性的硬件、软件或系统。

注：包括以服务形式提供防护能力的产品形态。

3.2

网络安全专用产品提供者 specialized cybersecurity products provider

网络安全专用产品的研发者、生产者或维护服务提供者。

3.3

用户信息 user information

与个人、法人或其他组织有关的信息，以及定义和描述此类信息的数据。

注：用户信息包括个人信息，用户生成的文档、程序、多媒体资料，用户通信的内容、地址、时间，产品的配置、运行及位置数据，系统运行过程产生的日志等。

3.4

恶意程序 malware

用于破坏网络和信息系统、干扰网络和信息系统正常使用、窃取或恶意加密网络和系统数据等网络攻击行为的程序。

注：恶意程序主要包括病毒、蠕虫、木马，以及其它影响主机、网络或系统安全、稳定运行的程序。

3.5

安全缺陷 security flaw

由设计、开发、配置、生产、运维等阶段中的错误引入，可能影响网络安全专用产品安全的弱点。

3.6

漏洞 vulnerability

网络安全专用产品中能够被威胁利用的弱点。

[来源：GB/T 25069—2010，2.3.30，有修改]

4 安全功能要求

4.1 边界控制

具有边界控制功能的网络安全专用产品应：

a) 能够根据访问控制策略允许或拒绝数据包进出网络边界；

b) 能够配置访问控制策略，默认情况下拒绝所有通信。

注：不同类型网络安全专用产品的访问控制策略不同。如：防火墙基于源地址、目的地址、源端口、目的端口和协议等设置访问控制策略；VPN基于用户等设置访问控制策略；网闸基于应用协议等设置访问控制策略。

4.2 入侵防范

具有入侵防范功能的网络安全专用产品应：

a) 能够对收集的信息进行分析，发现入侵事件；

b) 在检测到入侵事件时，能够采取记录事件、自动发出安全警告或阻断等安全措施。

4.3 安全审计

具有安全审计功能的网络安全专用产品应：

a) 能够监测、记录审计目标的网络运行状态、网络安全事件；

注：不同类型网络安全专用产品的安全审计目标不同，审计目标通常包括主机、网络、数据库、应用等。

b) 能够对事件进行比较分析以发现违规、异常等行为；

c) 将网络运行状态日志和网络安全事件日志存储于非易失性存储介质中，本地或外发日志保存时间不少于六个月。

4.4 防恶意程序

具有防恶意程序功能的网络安全专用产品应：

a) 能够对主机磁盘、主机内存、主机引导区、移动存储介质存储的信息或其他可能用于传输文件数据或程序代码的通信协议传输信息进行恶意程序检测；

b) 能够针对一种或多种恶意程序家族类型进行检测；

c) 能够对检测到的恶意程序进行阻止、删除、修复或隔离等一种或多种形式的处理。

5 自身安全要求

5.1 标识和鉴别

网络安全专用产品应：

a) 对用户身份进行标识和鉴别，身份标识具有唯一性；
b) 保障身份鉴别信息在传输和存储过程中的保密性和完整性；
c) 使用口令鉴别方式时，提供身份鉴别信息复杂度验证功能和定期更换设置功能，并支持首次管理产品时强制修改默认口令或设置口令。

5.2 访问控制

网络安全专用产品应：

a) 对用户分配账户和权限，区分管理员角色，实现管理权限相互制约；
b) 由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。

5.3 自身审计

网络安全专用产品应：

a) 监测、记录产品自身运行状态和重要操作；
b) 对审计日志进行保护，避免受到未预期的删除、修改、覆盖或丢失；
c) 将审计日志存储于非易失性存储介质中，本地或外发审计日志保存时间不少于六个月。

5.4 通信安全

网络安全专用产品应提供安全措施保障产品远程管理以及各组件间网络通信数据的保密性和完整性。

5.5 安全支撑系统

网络安全专用产品不应包含已知的中、高风险漏洞。

5.6 产品升级

网络安全专用产品应：

a) 提供升级产品组件的功能，包括但不限于主程序、特征库、策略库；
b) 保证升级安全，避免得到错误的、伪造的升级包。

5.7 用户信息安全

网络安全专用产品应：

a) 仅收集实现产品功能所必需的用户信息；
b) 在收集用户信息前向管理员用户明示与收集信息相关的功能、收集信息的种类及用途，取得产品管理员用户的同意，并提供撤回同意的方式；
c) 在产品界面明示所能采集的用户信息的目的、方式、范围和存储位置；
d) 保障用户信息在传输和存储过程中的保密性；
e) 提供对超出保存期限个人信息的处理功能。

注：对超出保存期限的个人信息的处理方式应与用户授权的处理方式一致，如采取删除或匿名化处理措施。

5.8 密码要求

本文件凡涉及密码算法的相关内容，按国家有关规范实施。

6 安全保障要求

6.1 供应链安全

网络安全专用产品提供者应：

a) 制定外包商、合作伙伴、子供应商等供应商选择、评定和日常管理的程序，将开发环境、规范和人员、开发工具、安全测试和安全验证机制等安全要求传递给供应商，以确保其提供的关键部件满足安全要求，并保存对供应商的选择、评价和日常管理记录；

b) 建立供应链各环节核心要素的追溯体系，保障核心要素供应稳定；

注：核心要素包括核心技术知识产权、工具及部件等。核心技术知识产权如软件代码、软硬件设计图等；工具如开发软件、编译软件、测试软件、测试仪表、管理软件、拷机软件等；部件如硬件机箱、操作系统等。

c) 投入资源进行安全意识和能力的建设。

6.2 设计与开发

网络安全专用产品提供者应：

a) 识别网络安全专用产品设计和开发环节的安全风险，进行威胁建模，制定安全策略，保障开发环境安全、制定安全开发制度和流程，内容包括但不限于代码编写规范、研发环境安全管理制度、研发人员安全管理制度、内部交付制度等；

b) 提供网络安全专用产品安全功能的设计文档，该文档与安全功能应当一致；

c) 为网络安全专用产品确定唯一的版本号，为配置项确定唯一标识，形成配置项列表，并提供配置项列表，其中配置项包括但不限于源代码、工具、文档、组件、配置信息；

d) 不得在产品中设置恶意程序、隐蔽接口或未明示功能模块等，并通过用户协议、产品说明书等途径告知用户；

e) 对网络安全专用产品进行安全性测试，包括但不限于漏洞扫描、病毒扫描、代码审计、渗透测试和安全功能验证。

6.3 生产和交付

网络安全专用产品提供者应：

a) 建立和执行规范的产品完整性检测流程，采取措施防范自制或采购的组件被篡改、伪造等风险；

b) 建立内部交付和外部交付的控制程序，确保网络安全专用产品交付过程中不被破坏或篡改；

c) 向用户明示包含在产品中的所有功能模块、外部接口和私有协议；告知用户产品中预置的所有账户和默认口令。

6.4 运维服务保障

网络安全专用产品提供者应：

a) 在法律法规规定或与用户约定的期限内，为产品提供持续的安全维护，不因业务变更、产权变更等原因单方面中断或终止安全维护；

b) 保护用户对软件（包含固件）安装和升级等的知情权和选择权，安装和升级软件时应明示用户并获得用户同意；

c) 建立和执行针对产品安全缺陷、漏洞的应急响应机制和流程，对发现的产品安全缺陷和漏洞

采取修复或替代方案等补救措施，及时告知用户安全风险，并向有关主管部门报告。

6.5 用户信息保护

网络安全专用产品提供者应：

a) 在产品指导性文档中明示所需采集的用户信息的种类及信息处理方式；

b) 建立和执行用户信息管理制度和流程，在产品设计、生产、升级等各阶段保障用户信息的安全，不得超范围使用用户信息；

c) 保证运行过程中产生的用户数据在境内存储，未经允许不应传出境外。

参 考 文 献

[1] 《中华人民共和国网络安全法》
[2] 《中华人民共和国密码法》
[3] 《中华人民共和国数据安全法》
[4] 《中华人民共和国产品质量法》
[5] 《中华人民共和国消费者权益保护法》
[6] 《中华人民共和国个人信息保护法》
[7] 《中华人民共和国信息系统安全保护条例》
[8] 《关键信息基础设施安全保护条例》
[9] 国发〔2020〕8号《国务院关于印发新时期促进集成电路产业和软件产业高质量发展若干政策的通知》
[10]国办发〔2002〕47号 《国务院办公厅转发国务院信息化工作办公室关于振兴软件产业行动纲要的通知》
[11] GB 17859-1999《计算机信息系统安全保护等级划分准则》
[12] GB/T 30279-2020《信息安全技术 网络安全漏洞分类分级指南》