



中华人民共和国国家标准

GB/T 25066—2020
代替 GB/T 25066—2010

信息安全技术 信息安全产品类别与代码

Information security technology—
Type and code of information security products

2020-04-28 发布

2020-11-01 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	I
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	1
5 类别与代码	2
5.1 类别	2
5.2 代码	2
5.3 类别与代码表	2
附录 A (规范性附录) 分类描述	6
附录 B (规范性附录) 领域属性描述	21
参考文献	22

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 25066—2010《信息安全技术 信息安全产品类别与代码》，与 GB/T 25066—2010 相比主要技术变化如下：

- 增加了缩略语(见第 4 章)；
- 修改了信息安全产品类别与代码表(见第 5 章,2010 年版的第 4 章)；
- 修改了附录 A 中的信息安全产品分类描述(见附录 A,2010 年版的附录 A)；
- 增加了附录 B,描述信息安全产品可具有适用领域属性的情况(见附录 B)。

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。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:公安部第三研究所、东软集团股份有限公司、上海市公安局、国家保密科技测评中心、中国信息安全测评中心、蓝盾信息安全技术股份有限公司、北京天融信科技有限公司、上海上讯信息技术股份有限公司、阿里云计算有限公司、启明星辰信息技术集团股份有限公司、中新网络信息安全股份有限公司、北京神州绿盟科技有限公司、北京威努特技术有限公司、深信服科技股份有限公司、中国电子科技集团公司第十五研究所、中国金融电子化公司、上海市信息安全测评认证中心、奇安信科技集团股份有限公司、北京安天网络安全技术有限公司、福建省网络与信息安全测评中心、上海交通大学。

本标准主要起草人:陆臻、李谦、顾健、祝国邦、章建国、陆磊、范春玲、刘利锋、李斌、刘强、王龔、刘德林、张大江、闻英友、路娜、赵志宏、徐雨晴、吴璇、杨传安、石凌志、伊玮珑、王峰、赵焕菊、刘健、倪又明、张俊彦、翟胜军、沈亮、俞优、宋好好、李毅、张笑笑、顾建新、陈妍、张艳、吴其聪、邹春明、杨元原、沈清泓、李旋、邓琦、韦湘、纪燕芳、银鹰。

本标准所代替标准的历次版本发布情况为：

- GB/T 25066—2010。

信息安全技术

信息安全产品类别与代码

1 范围

本标准规定了信息安全产品的主要类别与代码,包括物理环境安全类、通信网络安全类、区域边界安全类、计算环境安全类、安全管理支持类及其他类六个方面。

本标准适用于国家信息安全管理部门对信息安全产品(不包括涉密信息系统产品和仅提供密码算法运算的商用密码产品)进行分类管理,并可指导信息安全产品研制厂商的产品化工作和用户单位在信息化安全建设时的规划。

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 17859 计算机信息系统 安全保护等级划分准则

GB/T 25069 信息安全技术 术语

3 术语和定义

GB 17859、GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

信息安全产品 information security products

专门用于保障信息安全的软件、硬件或其组合体。

4 缩略语

下列缩略语适用于本文件。

ACL 访问控制列表(Access Control List)

AP 访问接入点(Access Point)

API 应用程序编程接口(Application Programming Interface)

APT 高级持续威胁(Advanced Persistent Threat)

CA 认证机构(Certification Authority)

COS 芯片操作系统(Chip Operating System)

CPU 中央处理器(Central Processing Unit)

FTP 文件传输协议(File Transfer Protocol)

IP 互联网协议(Internet Protocol)

IPSec 互联网协议安全(Internet Protocol Security)

KMC 密钥管理中心(Key Manage Center)

PKI	公钥基础设施(Public Key Infrastructure)
RA	注册机构(Registration Authority)
RFID	射频识别(Radio Frequency Identification)
URL	统一资源定位符(Uniform Resource Locator)
VLAN	虚拟局域网(Virtual Local Area Network)
WEB	万维网(World Wide Web)
Wi-Fi	无线保真(Wireless Fidelity)

5 类别与代码

5.1 类别

本标准以三级目录的形式将信息安全产品分为三级,其中一级分类包括六个类别:物理环境安全类、通信网络安全类、区域边界安全类、计算环境安全类、安全管理支持类和其他类。

物理环境安全类:用以保护环境、设备、设施以及介质免遭物理破坏(如地震、火灾等自然灾害以及物理上的窃取、毁损等人为破坏)的信息安全产品。

通信网络安全类:部署在网络中或通信终端上,用于监测、保护网络通信,保障网络通信的保密性、完整性和可用性的信息安全产品。

区域边界安全类:部署在安全域边界上,用于防御安全域外部对内部网络/设备进行攻击、渗透或安全域内部网络/设备向外部泄露敏感信息的信息安全产品。

计算环境安全类:部署在设备及其计算环境中,保护用户设备、计算或网络数据的完整性、保密性和可用性,或保障应用安全的信息安全产品。

安全管理支持类:为保障网络正常运行提供安全管理与支持,以及降低运行过程中安全风险的信息安全产品。

不能归入上述五类的信息安全产品暂归为其他类。

5.2 代码

一级分类代码为1位字母,二级分类代码为一级分类代码后增加1位数字(二级分类中的其他类,代码为一级分类代码后增加1位字母X),三级分类代码为二级分类代码后增加2位数字。

5.3 类别与代码表

信息安全产品的类别与代码见表1。

综合型信息安全产品按照其主要功能,可同时属于多个三级分类。

三级分类的详细描述见附录A。

信息安全产品可具有适用领域属性,如适用于工业控制系统领域、云计算领域、移动互联领域、物联网领域和大数据领域等,领域属性描述见附录B。

表 1 信息安全产品类别与代码

一级分类		二级分类		三级分类		
代码	名称	代码	名称	代码	名称	
A	物理环境安全	A1	环境安全	A101	区域防护	
				A102	灾难防范与恢复	
				A103	容灾恢复计划辅助支持	
				A104	电磁干扰	
				A105	抗电磁干扰	
				A106	电磁泄漏防护	
		A2	物理安全	A201	防盗	
				A202	防毁	
				A203	防线路截获	
				A204	电源保护	
				A205	介质安全	
		AX	物理环境安全其他			
		B	通信网络安全	B1	通信安全	B101
B2	网络监测与控制			B201	网络入侵检测	
				B202	网络活动监测与分析	
				B203	流量控制	
				B204	上网行为管理	
				B205	反垃圾邮件	
				B206	信息过滤	
BX	通信网络安全其他					
C	区域边界安全	C1	隔离	C101	终端隔离	
				C102	网络隔离	
				C103	网络单向导入	
		C2	入侵防范	C201	网络入侵防御	
				C202	网络恶意代码防范	
				C203	抗拒绝服务攻击	
		C3	边界访问控制	C301	防火墙	
				C302	安全路由器	
				C303	安全交换机	
		C4	接入安全	C401	终端接入控制	
CX	区域边界安全其他					

表 1 (续)

一级分类		二级分类		三级分类	
代码	名称	代码	名称	代码	名称
D	计算环境安全	D1	计算环境防护	D101	可信计算
				D102	身份鉴别(主机)
				D103	主机入侵检测
				D104	主机访问控制
				D105	主机型防火墙
				D106	终端使用安全
				D107	移动存储设备安全管理
		D2	防恶意代码	D201	主机恶意代码防治
		D3	操作系统安全	D301	安全操作系统
				D302	操作系统安全部件
		D4	应用安全防护	D401	身份鉴别(应用)
				D402	WEB 应用防火墙
				D403	邮件安全防护
				D404	网站恢复
				D405	应用安全加固
		D5	应用安全支持	D501	业务流程监控
				D502	源代码审计
				D503	网站监测
				D504	应用软件安全管理
				D505	应用代理
				D506	负载均衡
				D507	数字签名
		D6	数据安全防护	D601	数据加密
				D602	数据泄露防护
				D603	数据脱敏
				D604	数据清除
				D605	数据备份与恢复
		D7	数据平台安全	D701	安全数据库
				D702	数据库安全部件
				D703	数据库防火墙
		DX	计算环境安全其他		

表 1 (续)

一级分类		二级分类		三级分类	
代码	名称	代码	名称	代码	名称
E	安全管理支持	E1	综合审计	E101	安全审计
		E2	应急响应支持	E201	应急响应辅助系统
		E3	密码管理	E301	密码设备
				E302	公钥基础设施
		E4	风险评估与处置	E401	系统风险评估
				E402	安全性检测分析
				E403	配置核查
				E404	漏洞挖掘
				E405	态势感知
				E406	高级持续威胁检测
				E407	舆情分析
		E5	安全管理	E501	安全管理平台
				E502	安全监控
				E503	运维安全管理
E504	统一身份鉴别与授权				
EX	安全管理支持其他				
X	其他				

附 录 A
(规范性附录)
分类描述

A.1 物理环境安全(A)

A.1.1 环境安全(A1)

A.1.1.1 区域防护(A101)

本类产品采用相关信息技术为支撑,对特定区域(包括固定或移动的)提供某种形式的保护和隔离,目的是保护特定区域的系统或设备免受直接人为破坏。

本类产品的安全功能可主要归纳为三个方面:

- a) 人员出入控制;
- b) 受保护资源控制;
- c) 传感器网络。

任何提供以上一种或数种功能,且该功能为主导性功能的产品,均可归入本类(A101)。

A.1.1.2 灾难防范与恢复(A102)

本类产品采用相关信息技术为支撑,提供受灾报警、受灾保护和受灾恢复等功能,目的是保护系统或设备免受水、火、有害气体、地震、雷击和静电的危害。

本类产品的安全功能可主要归纳为三个方面:

- a) 灾难发生前,对灾难的检测和报警;
- b) 灾难发生时,对正遭受破坏的系统或设备采取紧急措施,进行现场实时保护;
- c) 灾难发生后,对已经遭受破坏的系统或设备进行灾后恢复。

任何提供以上一种或数种功能,且该功能为主导性功能的产品,均可归入本类(A102)。

A.1.1.3 容灾恢复计划辅助支持(A103)

本类产品采用相关信息技术为支撑,为制定容灾恢复计划提供计算机辅助,以容灾恢复计划辅助软件的形式提供,目的是实现容灾恢复计划的半自动化生成。

本类产品的安全功能可主要归纳为三个方面:

- a) 受灾的影响分析;
- b) 受灾恢复计划的概要设计或详细制定;
- c) 受灾恢复计划的测试与完善。

任何提供以上一种或数种功能,且该功能为主导性功能的产品,均可归入本类(A103)。

A.1.1.4 电磁干扰(A104)

本类产品采用相关信息技术对电磁信号进行主动干扰,目的是在一定范围内阻断通过电磁信号进行的数据通信,防止利用电磁信号进行信息窃听或窃取活动。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(A104)。

A.1.1.5 抗电磁干扰(A105)

本类产品采用相关信息技术防止电磁干扰,目的是保护系统或设备的运行及数据的安全性。

本类产品的安全功能可主要归纳为两个方面：

- a) 对抗外界对系统的电磁干扰；
- b) 消除来自系统内部的电磁干扰。

任何提供以上一种或两种功能,且该功能为主导性功能的产品,均可归入本类(A105)。

A.1.1.6 电磁泄漏防护(A106)

本类产品采用相关信息技术防止电磁信号的泄漏,目的是在特定安全域内提高敏感信息的安全性。

本类产品的安全功能可主要归纳为两个方面：

- a) 降低或阻断电磁信号的泄漏；
- b) 干扰泄漏的电磁信号。

任何提供以上一种或两种功能,且该功能为主导性功能的产品,均可归入本类(A106)。

A.1.2 物理安全(A2)

A.1.2.1 防盗(A201)

本类产品采用相关信息技术为支撑,提供对设备或部件的防盗保护(如网络探测报警),目的是保护设备和部件免遭人为盗窃。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(A201)。

A.1.2.2 防毁(A202)

本类产品采用相关信息技术为支撑,提供对设备的防毁保护,目的是保护设备免遭自然力和人为毁坏。

本类产品所提供的安全功能可主要归纳为两个方面：

- a) 对抗自然力的破坏,使用一定的防毁措施(如网络远程控制防护)保护系统设备和部件；
- b) 对抗人为的破坏,使用一定的防毁措施(如网络远程防拆报警)保护系统设备和部件。

任何提供以上一种或两种功能,且该功能为主导性功能的产品,均可归入本类(A202)。

A.1.2.3 防线路截获(A203)

本类产品采用相关信息技术为支撑,防止通信线路中传输的信息被非授权截获,目的是提高敏感信息在传输过程中的安全性。

本类产品的安全功能可主要归纳为两个方面：

- a) 探测线路截获,发现线路截获并报警；
- b) 定位线路截获,发现线路截获设备工作的位置。

任何提供以上一种或两种功能,且该功能为主导性功能的产品,均可归入本类(A203)。

A.1.2.4 电源保护(A204)

本类产品采用相关信息技术为支撑,为系统设备的可靠运行提供电源保障,目的是保障系统运行的稳定性。

本类产品的安全功能可主要归纳为两个方面：

- a) 对工作电源的工作连续性的保护,如不间断电源；
- b) 对工作电源的工作稳定性的保护,如纹波抑制器。

任何提供以上一种或两种功能,且该功能为主导性功能的产品,均可归入本类(A204)。

A.1.2.5 介质安全(A205)

本类产品采用相关信息技术为支撑,提供对介质及其承载数据的防护或销毁,目的是防止数据被非授权访问、删除或者已删除的敏感数据被非授权恢复。

本类产品的安全功能可主要归纳为三个方面:

- a) 介质数据的防盗,如防止介质数据被非授权拷贝;
- b) 介质数据的销毁,包括介质的物理销毁和介质数据的彻底销毁(如消磁等),防止介质数据删除或销毁后被他人恢复而泄露信息;
- c) 介质数据的防毁,防止意外或故意的破坏使介质数据丢失。

任何提供以上一种或数种功能,且该功能为主导性功能的产品,均可归入本类(A205)。

A.1.3 物理环境安全其他(AX)

不能归为上述2类的物理环境安全类产品暂归为物理环境安全其他类(AX)。

A.2 通信网络安全(B)

A.2.1 通信安全(B1)

虚拟专用网(B101)

本类产品提供在公共通信基础网络上以逻辑方式隔离出安全通讯链路的基本功能,目的是在互联网链路或移动互联网链路等物理链路上建立专用的安全传输通道,保障数据网络传输的安全性。

本类产品的安全功能可主要归纳为五个方面:

- a) 通信方的身份鉴别;
- b) 密钥协商,通过协商产生工作密钥等;
- c) 安全传输隧道建立;
- d) 安全数据传输,通过对传输数据的分段、压缩及解压缩、加密及解密、完整性校验等保证数据的安全传输;
- e) 密钥动态更新。

任何提供以上全部功能,且该功能为主导性功能的产品,均可归入本类(B101)。

A.2.2 网络监测与控制(B2)

A.2.2.1 网络入侵检测(B201)

本类产品针对网络入侵进行监测,自动识别各种入侵行为并进行报警,目的是及时发现网络中违反安全策略的行为和被攻击的迹象。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(B201)。

A.2.2.2 网络活动监测与分析(B202)

本类产品对网络传输信息进行监测与分析,目的是为管理员进行网络管理提供支持。

本类产品的安全功能可主要归纳为两个方面:

- a) 根据不同的网络协议进行监测,对网络通信信息进行记录并还原;
- b) 通过流量分析等手段将网络活动信息与预先设置好的安全策略进行匹配,从而发现网络活动异常。

任何提供以上一种或两种功能,且该功能为主导性功能的产品,均可归入本类(B202)。

A.2.2.3 流量控制(B203)

本类产品是对安全域的网络进行流量监测和带宽控制的流量管理系统,可实现合理的带宽分配,目的是优化带宽资源的使用,避免网络拥塞,从而保护关键应用的带宽占用,提高带宽利用率。

本类产品的安全功能可主要归纳为两个方面:

- a) 流量监测,监测和分析网络流量的分布情况;
- b) 带宽控制,提供带宽限制、带宽预留、带宽保证等带宽管理功能。

任何提供以上全部功能,且该功能为主导性功能的产品,均可归入本类(B203)。

A.2.2.4 上网行为管理(B204)

本类产品用于审计和控制网络用户对网络的使用行为,进行网页访问过滤、网络应用控制、信息收发审计、用户行为分析等,目的是实时监控和管理网络资源使用情况,规范上网行为。

本类产品的安全功能可主要归纳为五个方面:

- a) 对上网用户进行身份认证或终端管理;
- b) 对网址、上网搜索内容或文件下载进行识别和控制;
- c) 对通过电子邮件、网页发帖、即时通信、FTP等方式上网的外发信息内容进行识别和控制;
- d) 对上网应用进行识别和控制;
- e) 对网络行为信息(用户身份、登录时间、访问域名/应用等)进行记录并留存。

任何提供以上一种或数种功能,且该功能为主导性功能的产品,均可归入本类(B204)。

A.2.2.5 反垃圾邮件(B205)

本类产品根据预先定义的规则来识别垃圾邮件并进行处理,目的是阻止垃圾邮件扩散。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(B205)。

A.2.2.6 信息过滤(B206)

本类产品根据预先定义的规则来过滤网络信息,目的是对过滤策略中定义的网络流入/流出信息进行筛选控制。

本类产品的安全功能可主要归纳为四个方面:

- a) 文本过滤;
- b) 图片过滤;
- c) 多媒体流过滤;
- d) 其他信息过滤。

任何提供以上一种或数种功能,且该功能为主导性功能的产品,均可归入本类(B206)。

A.2.3 通信网络安全其他(BX)

不能归为上述2类的通信网络安全类产品暂归为通信网络安全其他类(BX)。

A.3 区域边界安全(C)

A.3.1 隔离(C1)

A.3.1.1 终端隔离(C101)

本类产品是同时连接两个不同安全域,采用物理断开技术在终端上实现安全域物理隔离的安全隔

离卡或安全隔离计算机。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(C101)。

A.3.1.2 网络隔离(C102)

本类产品是位于两个不同安全域之间,采用协议隔离技术在网络上实现安全隔离与信息交换的产品。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(C102)。

A.3.1.3 网络单向导入(C103)

本类产品位于两个不同安全域之间,通过物理方式构造信息单向传输的唯一通道,实现信息单向导入,并且保证只有安全策略允许传输的信息可以通过,同时反方向无任何信息传输或反馈。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(C103)。

A.3.2 入侵防范(C2)

A.3.2.1 网络入侵防御(C201)

本类产品在网络入侵行为进入被保护网络之前通过报警阻断或干扰隔离(如蜜罐技术)等措施为网络提供防护,目的是对网络入侵行为进行阻止。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(C201)。

A.3.2.2 网络恶意代码防范(C202)

本类产品侧重于防护网络系统资源,针对恶意代码(如木马、恶意脚本、病毒等)的网际传播提供过滤功能,目的是防止恶意代码通过网络进行扩散。

本类产品的安全功能可主要归纳为两个方面:

- a) 防病毒网关;
- b) 网际恶意代码防范。

任何提供以上一种或两种功能,且该功能为主导性功能的产品,均可归入本类(C202)。

A.3.2.3 抗拒绝服务攻击(C203)

本类产品用于识别和拦截攻击者通过消耗过量系统资源(如计算资源、带宽资源等)而导致系统不能及时执行合法用户任务的攻击,目的是保障系统可用性。

本类产品的安全功能可主要归纳为两个方面:

- a) 当遇到大量用户请求时,可以识别出合法用户的请求而给予响应;
- b) 当遇到大量用户请求时,可以动态分配资源从而保障通信畅通。

任何提供以上一种或两种功能,且该功能为主导性功能的产品,均可归入本类(C203)。

A.3.3 边界访问控制(C3)

A.3.3.1 防火墙(C301)

本类产品部署于不同安全域之间,针对系统的网络数据流入/流出提供深度内容检测和防御,目的是阻止安全域外部连接的非授权进入内部或者是内部的异常行为或流量外发,以及通过多元素、精细化的访问控制手段阻断特定的内外连接。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(C301)。

A.3.3.2 安全路由器(C302)

本类产品集成常规路由功能与网络安全功能,除普通路由功能以外,内置防火墙、IPSec 等模块,提供网络互连、流量控制、网络和信息安全维护等安全功能,目的是阻止安全域外部连接的非授权进入内部,以及保障网络通信的安全性。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(C302)。

A.3.3.3 安全交换机(C303)

本类产品在传统的交换功能的基础上,提供了基于 ACL 的报文过滤、CPU 过载保护、广播风暴控制、VLAN、基于 802.1X 的接入控制等安全功能,目的是保障安全域数据交换的安全性。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(C303)。

A.3.4 接入安全(C4)

终端接入控制(C401)

本类产品提供对接入网络的终端进行访问控制的功能,能发现终端接入网络的行为,并能根据访问控制策略采取行动(如允许授权终端接入、断开非授权的终端连接等),目的是通过对终端接入的控制,保障安全域边界安全。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(C401)。

A.3.5 区域边界安全其他(CX)

不能归为上述 4 类的区域边界安全类产品暂归为区域边界安全其他类(CX)。

A.4 计算环境安全(D)

A.4.1 计算环境防护(D1)

A.4.1.1 可信计算(D101)

本类产品利用可信计算平台模块,对主机用户进行身份鉴别以及信息加密,目的是提供可信计算环境。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(D101)。

A.4.1.2 身份鉴别(主机)(D102)

本类产品在主机设备的用户执行授权操作前,要求用户提供以电子信息或生物信息为载体的身份及鉴别信息,对其进行鉴别,目的是确认主机系统使用者的身份。

本类产品的安全功能可主要归纳为六个方面:

- a) 基于智能卡的身份鉴别,包括 COS、芯片和读卡器;
- b) PKI/CA 证书身份鉴别;
- c) 动态口令身份鉴别;
- d) 基于 RFID 的身份鉴别;
- e) 基于生物特征的身份鉴别,如手形、指纹/掌纹、脸形、虹膜、视网膜、脉搏、耳廓等;
- f) 基于行为特征的身份鉴别,如签字、语音、按键力度等。

任何提供以上一种或数种功能,且该功能为主导性功能的产品,均可归入本类(D102)。

A.4.1.3 主机入侵检测(D103)

本类产品对抵达主机的数据进行监测,从主机或服务器上采集包括操作系统日志、系统进程、文件访问和注册表访问等数据,并根据事先设定的策略判断数据是否异常,从而决定采取报警、控制等措施,目的是对入侵主机行为进行发现和阻止。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(D103)。

A.4.1.4 主机访问控制(D104)

本类产品针对受控主机,统一分配用户对主机资源的访问权限,用户根据预先定义的访问控制策略对受控主机的资源(如系统登录权限、文件和文件夹、外设接口、应用程序、进程等)进行访问,目的是保护主机资源不被非授权访问和使用。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(D104)。

A.4.1.5 主机型防火墙(D105)

本类产品针对主机设备上的入站和出站网络连接提供保护功能,并能够通过预先定义的规则,执行基于网络地址和基于应用的访问控制,一般为软件,目的是对主机设备提供网络综合防护。一般运行于服务器上的主机型防火墙还可以对所有的节点进行统一控制,实施统一的安全策略与响应。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(D105)。

A.4.1.6 终端使用安全(D106)

本类产品提供对接入系统的终端进行保护的功能,目的是保障终端资源和运行环境的安全。

本类产品的安全功能可主要归纳为六个方面:

- a) 防止对终端的未授权使用(如终端使用口令保护等);
- b) 阻止恶意程序运行;
- c) 钓鱼检测与拦截;
- d) 软件升级与管理;
- e) 系统资源回收;
- f) 系统环境备份与恢复。

任何提供以上一种或数种功能,且该功能为主导性功能的产品,均可归入本类(D106)。

A.4.1.7 移动存储设备安全管理(D107)

本类产品通过对移动存储设备采取身份认证、访问控制、审计机制等管理手段,实现移动存储设备与主机设备之间的可信访问,以保护主机设备资源安全。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(D107)。

A.4.2 防恶意代码(D2)

主机恶意代码防治(D201)

本类产品提供对主机恶意代码的防治功能,侧重于防护本地主机资源。通过对内容或行为的判断建立系统保护机制,预防、检测、隔离、清除、删除主机恶意代码,目的是检测发现或阻止恶意代码的传播以及对主机操作系统、应用软件和用户文件的篡改、破坏和非法占有等。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(D201)。

A.4.3 操作系统安全(D3)

A.4.3.1 安全操作系统(D301)

本类产品是指从系统设计、实现和使用等各个阶段都遵循了一套完整的安全策略的操作系统,如嵌入式安全操作系统、移动智能终端安全操作系统等,目的是在操作系统层面保障系统安全。

任何具有不同安全级别的安全操作系统产品均可归入本类(D301)。

A.4.3.2 操作系统安全部件(D302)

本类产品以安全部件的形式增强现有操作系统的安全性,目的是在操作系统层面保障系统安全。

本类产品的安全功能可主要归纳为两个方面:

- a) 通过构造安全模块,增强现有操作系统的安全性;
- b) 通过构造安全外罩,增强现有操作系统的安全性。

任何提供以上一种或两种功能,且该功能为主导性功能的产品,均可归入本类(D302)。

A.4.4 应用安全防护(D4)

A.4.4.1 身份鉴别(应用)(D401)

本类产品在应用服务的用户执行授权操作前,要求用户提供以电子信息或生物信息为载体的身份及鉴别信息,对其进行鉴别,目的是确认应用系统使用者的身份。

本类产品的安全功能可主要归纳为六个方面:

- a) 基于智能卡的身份鉴别,包括 COS、芯片和读卡器;
- b) PKI/CA 证书身份鉴别;
- c) 动态口令身份鉴别;
- d) 基于 RFID 的身份鉴别;
- e) 基于生物特征的身份鉴别,如手形、指纹/掌纹、脸形、虹膜、视网膜、脉搏、耳廓等;
- f) 基于行为特征的身份鉴别,如签字、语音、按键力度等。

任何提供以上一种或数种功能,且该功能为主导性功能的产品,均可归入本类(D401)。

A.4.4.2 WEB 应用防火墙(D402)

本类产品部署于 WEB 应用和 WEB 服务器之前,通过分析 WEB 应用层协议,根据预先定义的过滤规则和防护策略,对所有 WEB 应用和服务器的访问请求与响应进行过滤,目的是实现对 WEB 应用及 WEB 服务器的安全防护。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(D402)。

A.4.4.3 邮件安全防护(D403)

本类产品提供对电子邮件的安全传输、安全存储、病毒防护、安全审计等功能,目的是实现邮件应用的安全防护。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(D403)。

A.4.4.4 网站恢复(D404)

本类产品提供对网站内容(包括静态网页文件、动态脚本文件、网页目录、网站数据库等)的实时保护,对网站内容的非授权更改进行识别,并能用备份文件进行自动恢复,目的是实现对网站内容的安全防护。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(D404)。

A.4.4.5 应用安全加固(D405)

本类产品采用相关信息技术实现对应用软件的安全加固,防止应用软件被通过逆向分析等手段非法破解,或被通过二次打包等手段非法篡改,目的是保护应用软件的源码、资源文件等免遭非法获取,应用软件免遭恶意侵犯(如盗版、提权、加载外挂等)。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(D405)。

A.4.5 应用安全支持(D5)

A.4.5.1 业务流程监控(D501)

本类产品是采用全流程视角,通过监控业务流程、业务行为和业务内容,实现对业务安全分析和定位,针对业务行为、业务内容设置访问控制策略,对检测到的攻击行为执行阻断或联动其他设备进行阻断,并采用行为分析技术检测网络攻击行为和保密性问题,实现有效检测 0Day 攻击和 APT 攻击。

本类产品的安全功能可主要归纳为三个方面:

- a) 业务流程监控;
- b) 业务行为监控;
- c) 网络攻击检测与监控。

任何提供以上全部功能,且该功能为主导性功能的产品,均可归入本类(D501)。

A.4.5.2 源代码审计(D502)

本类产品是针对系统开发过程中的源代码进行安全审计检测,检测缓冲区溢出、代码注入、跨站脚本、输入验证、API 误用等缺陷,检测编码规范性,目的是对源代码安全问题进行分析和验证。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(D502)。

A.4.5.3 网站监测(D503)

本类产品针对大规模网站进行持续、多维度(如 WEB 系统扫描监控、网站防钓鱼监控、网页木马监测、网页篡改监测、网页敏感信息监测、暗链检测、网站应用监测、域名监测等)安全监测,并可结合安全风险评估模型实时进行网站安全风险评估,目的是实时了解所有 WEB 资产面临的风险,实现快速故障定位。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(D503)。

A.4.5.4 应用软件安全管理(D504)

本类产品基于应用软件安全管理策略(如软件白名单、证书签名、服务端策略等)对设备上的应用软件安装、运行等进行安全管理,目的是保障设备上应用软件的安全和可控。

本类产品的安全功能可主要归纳为三个方面:

- a) 对设备上应用软件的安装进行管理;
- b) 对设备上应用软件的启动进行管理;
- c) 对设备上应用软件所能访问的设备资源进行权限控制。

任何提供以上一种或数种功能,且该功能为主导性功能的产品,均可归入本类(D504)。

A.4.5.5 应用代理(D505)

本类产品为应用提供代理服务,实现对应用层通信流的协议剥离、数据落地、内容审计、异常告警、

协议转换及数据缓存等功能,目的是提高内外网络之间应用服务的安全性。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(D505)。

A.4.5.6 负载均衡(D506)

本类产品提供链路负载均衡、服务器负载均衡、网络流量优化和智能处理等功能,目的是降低负载,优化网络性能,提高服务运行的稳定性,提高资源利用率、应用性能和用户体验。

本类产品的安全功能可主要归纳为两个方面:

- a) 将用户的访问请求根据一定的算法合理分摊到不同的网络线路上传输,保障传输的可靠性,提升传输效率;
- b) 将用户的访问请求根据一定的算法合理分摊到不同的服务器上处理,保障应用的可靠性和连续性,优化服务器处理性能。

任何提供以上一种或两种功能,且该功能为主导性功能的产品,均可归入本类(D506)。

A.4.5.7 数字签名(D507)

本类产品提供签名验签、完整性和不可否认性鉴别等功能,目的是保障应用数据的完整性与不可否认性。

本类产品的安全功能可主要归纳为两个方面:

- a) 签名:提取数据的摘要信息,并使用用户的私钥对摘要信息进行签名;
- b) 验签:使用用户的公钥对签名信息进行验证,并以此验证原始信息的完整性与不可否认性。

任何提供以上两种功能,且该功能为主导性功能的产品,均可归入本类(D507)。

A.4.6 数据安全防护(D6)

A.4.6.1 数据加密(D601)

本类产品用于防御攻击者窃取以文件等形式存储的数据,目的是保障存储数据的安全。

本类产品的安全功能可主要归纳为两个方面:

- a) 采用密码技术对存储的数据进行加密(如文件加密、整盘加密等手段),确保攻击者即使获取数据仍无法解析出明文;
- b) 采用信息隐藏技术实现数据的隐蔽存储,确保攻击者即使获取数据仍无法获取隐藏的信息。

任何提供以上一种或两种功能,且该功能为主导性功能的产品,均可归入本类(D601)。

A.4.6.2 数据泄露防护(D602)

本类产品在主机、文印设备、网络中通过对安全域内部敏感信息输出的主要途径进行控制和审计,目的是防止安全域内部敏感信息被非授权泄露。

本类产品的安全功能可主要归纳为三个方面:

- a) 外设接口输出控制和审计;
- b) 文印设备(如打印机、复印机、扫描仪、刻录机等)输出控制和审计;
- c) 网络输出控制和审计(控制点包括网络边界出口或主机)。

任何提供以上一种或数种功能,且该功能为主导性功能的产品,均可归入本类(D602)。

A.4.6.3 数据脱敏(D603)

本类产品针对敏感数据基于脱敏规则进行改造,实现数据变形,目的是防范敏感信息外泄。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(D603)。

A.4.6.4 数据清除(D604)

本类产品采用信息技术(如覆写)进行逻辑级底层数据清除,实现对存储介质所承载数据的彻底销毁,目的是防止已删除的敏感数据被非授权恢复导致数据外泄。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(D604)。

A.4.6.5 数据备份与恢复(D605)

本类产品对系统中的数据(如数据库、数据卷、文件、操作系统等的数据、结构和状态)进行备份与恢复,并对备份与恢复的策略管理、作业等事件进行安全审计,目的是保障数据安全。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(D605)。

A.4.7 数据平台安全(D7)

A.4.7.1 安全数据库(D701)

本类产品是指从系统设计、实现、使用和管理等各个阶段都遵循一套完整的系统安全策略的数据库系统,目的是在数据库层面保障数据安全。

任何具有不同安全级别的安全数据库系统均可归入本类(D701)。

A.4.7.2 数据库安全部件(D702)

本类产品是以现有数据库系统所提供的功能为基础构造安全模块,以安全部件的形式增强现有数据库系统的安全性,目的是在数据库层面保障数据安全。

本类产品的安全功能可主要归纳为两个方面:

- a) 通过构造安全模块,增强现有数据库系统的安全性;
- b) 通过构造安全外罩,增强现有数据库系统的安全性。

任何提供以上一种或两种功能,且该功能为主导性功能的产品,均可归入本类(D702)。

A.4.7.3 数据库防火墙(D703)

本类产品基于数据库协议分析与防火墙控制技术提供对数据库的访问控制、语句拦截、操作阻断、行为审计等功能,目的是保障数据库系统的安全。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(D703)。

A.4.8 计算环境安全其他(DX)

不能归为上述7类的计算环境安全类产品暂归为计算环境安全其他类(DX)。

A.5 安全管理支持(E)

A.5.1 综合审计(E1)

安全审计(E101)

本类产品针对系统的活动信息进行审计记录及分析,目的是通过安全审计挖掘安全事件,并加以分析,得到相关信息。

本类产品的安全功能可主要归纳为五个方面:

- a) 主机安全审计,针对主机进程调用、文件使用等事件进行审计;
- b) 网络安全审计,针对网络通信事件进行审计;

- c) 数据库安全审计,针对数据库活动进行审计;
- d) 应用系统安全审计,针对用户访问、管理应用系统或应用系统服务异常等事件进行审计;
- e) 日志分析,针对指定审计数据的数据分析与挖掘。

任何提供以上一种或数种功能,且该功能为主导性功能的产品,均可归入本类(E101)。

A.5.2 应急响应支持(E2)

应急响应辅助系统(E201)

本类产品为应急响应提供计算机辅助,目的是实现应急响应的半自动化支持。

本类产品的安全功能可主要归纳为三个方面:

- a) 紧急事件或安全事件发生时的影响分析;
- b) 应急响应的概要设计或详细制定;
- c) 应急响应的测试与完善。

任何提供以上一种或数种功能,且该功能为主导性功能的产品,均可归入本类(E201)。

A.5.3 密码管理(E3)

A.5.3.1 密码设备(E301)

本类产品提供密码信息存储并执行密码算法运算,目的是为保障信息的保密性提供基础设施支持,如商用加密机、加密卡等。相关要求均应遵照国家有关密码政策执行。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(E301)。

A.5.3.2 公钥基础设施(E302)

本类产品支持公钥管理体制的基础设施,提供鉴别、加密、完整性和不可否认服务。组件一般包括认证机构 CA、注册机构 RA、密钥管理中心 KMC、证书目录服务等关键组件。

任何提供以上功能或组件的产品,均可归入本类(E302)。

A.5.4 风险评估与处置(E4)

A.5.4.1 系统风险评估(E401)

本类产品提供对系统进行半自动或自动的风险评估,目的是提高系统安全性。

本类产品的安全功能可主要归纳为三个方面:

- a) 系统设计前的风险评估,通过分析业务系统固有的脆弱性,旨在发现系统设计前潜在的安全隐患;
- b) 系统试运行前的风险评估,根据系统试运行期的运行状态和结果,分析系统的潜在安全隐患,旨在发现系统设计的安全漏洞;
- c) 系统运行期的风险评估,提供系统运行记录,跟踪系统状态的变化,分析系统运行期的安全隐患,旨在发现系统运行期的安全漏洞。

任何提供以上一种或数种功能,且该功能为主导性功能的产品,均可归入本类(E401)。

A.5.4.2 安全性检测分析(E402)

本类产品针对系统特定对象进行安全性检测分析,该分析过程一般包括脆弱性扫描、分析与建议三个过程,目的是提高系统安全性。

本类产品的安全功能可主要归纳为七个方面:

- a) 操作系统安全性检测分析;

- b) 数据库及数据库管理系统安全性检测分析；
- c) 传输、网络系统安全性检测分析；
- d) 应用系统安全性检测分析；
- e) 硬件系统安全性检测分析；
- f) 软件源代码安全性检测分析；
- g) 攻击性和渗透性检测分析。

任何提供以上一种或数种功能,且该功能为主导性功能的产品,均可归入本类(E402)。

A.5.4.3 配置核查(E403)

本类产品基于安全配置要求实现对资产(如服务器、网络设备、安全产品、操作系统、数据库、应用系统等)的安全配置检测和合规性分析,生成安全配置建议和合规性报告,目的是发现并指导消除资产中因安全配置不当导致的安全隐患。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(E403)。

A.5.4.4 漏洞挖掘(E404)

本类产品针对系统或单个产品进行安全性检测分析,通过自动化构造的测试用例,检测分析系统的源码、目的代码、运行内存和通信状态等,发现系统或产品的未知安全漏洞,并能给出初步分析,从而帮助提高系统或产品的安全性。

本类产品的安全功能可主要归纳为五个方面:

- a) 操作系统漏洞挖掘分析；
- b) 数据存储相关系统漏洞挖掘分析；
- c) 网络通信系统漏洞挖掘分析；
- d) 应用系统漏洞挖掘分析；
- e) 硬件系统漏洞挖掘分析。

任何提供以上一种或数种功能,且该功能为主导性功能的产品,均可归入本类(E404)。

A.5.4.5 态势感知(E405)

本类产品通过采集网络环境要素(如网络流量、计算环境、业务应用、资产、审计日志、运行状况、脆弱性、安全事件和威胁情报等),利用大数据技术和机器学习技术,分析网络当前状态和变化趋势,获取、理解、回溯、显示能够引起网络态势变化的安全要素,预测网络安全态势发展趋势,对网络整体安全进行监测、分析和预警。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(E405)。

A.5.4.6 高级持续威胁检测(E406)

本类产品针对网络中的文件进行深度、智能、持续性的分析,识别各类已知、未知的安全威胁,对可能用于 APT 攻击的文件进行行为揭示,并通过文件分析报告呈现鉴定分析结果。目的是帮助用户掌握网络威胁状况,提高网络安全威胁检测和响应能力。

本类产品所提供的安全功能可主要归纳为五个方面:

- a) 静态检测,如格式识别解析、Shellcode 发现、堆喷射检测、字符串信息提取以及漏洞检测等；
- b) 动态检测,如将未知文件投放到虚拟执行环境中运行,利用系统监控和网络监控等手段,监控记录其运行的本地行为,或通过代码结构及 API 调用指令等信息的分析提取潜在行为；
- c) 病毒特征库检测,基于病毒特征库,对已知威胁进行识别；
- d) 关联分析,基于文件结构包含或行为后果关联关系(如文件释放、压缩包包含、资源节包含等关

系)对关联文件进行分析判定;

- e) 对发现的安全威胁提供识别结果,如相关的文件、域名、IP、URL、互斥量等具备实际响应操作支撑作用的信息。

任何提供以上全部功能,且该功能为主导性功能的产品,均可归入本类(E406)。

A.5.4.7 舆情分析(E407)

本类产品基于采集的海量网络舆情信息,对某个特定问题的舆情进行监测、汇总和分析,识别其中的关键信息,形成舆情报表或报告,目的是得到舆情相关的结论。

本类产品的安全功能可主要归纳为三个方面:

- a) 舆情监测;
- b) 舆情分析;
- c) 舆情预测、预警。

任何提供以上一种或数种功能,且该功能为主导性功能的产品,均可归入本类(E407)。

A.5.5 安全管理(E5)

A.5.5.1 安全管理平台(E501)

本类产品是一个信息交换、存储和处理平台,能够对安全信息进行控制管理,目的是对信息安全资产进行统一管理,增强资产管理的时效性、可控性和全面性。

本类产品的安全功能可主要归纳为七个方面:

- a) 安全产品管理,该平台允许授权主体对安全属性(访问控制列表、能力表等)进行查看或修改;提供对角色的统一管理;对日志信息进行统一收集和处理;
- b) 补丁管理,对操作系统和安全软件的补丁安装情况设置统一的策略,进行统一的管理;
- c) 升级管理,对操作系统和安全软件的版本升级情况设置统一的策略,进行统一的管理;
- d) 对资产(包括网络设备、安全设备和服务器等)进行监控;
- e) 对安全设备进行配置、管理,监测网络上的数据通信;
- f) 对安全系统的整体状态进行监测;
- g) 其他信息安全相关的资产管理。

任何提供以上一种或数种功能,且该功能为主导性功能的产品,均可归入本类(E501)。

A.5.5.2 安全监控(E502)

本类产品针对系统信息流进行安全性监测和控制,目的是发现和阻止系统和网络资源的非授权使用。

本类产品的安全功能可主要归纳为三个方面:

- a) 远程或本地监测,对受控主机的在线状态、系统资源、软件安装、服务、进程、外设使用、上网等情况进行实时监测;
- b) 非授权外联监控,对受保护网络内部主机在安全策略允许之外通过调制解调器、多网卡、无线设备等非授权途径与外部网络进行连接的情况加以监测、报警及阻断;
- c) 违规内联检查,在安全策略允许之外通过无线 AP、随身 Wi-Fi 等非授权途径进入受保护网络内部进行连接的情况进行检测、报警与阻断。

任何提供以上一种或数种功能,且该功能为主导性功能的产品,均可归入本类(E502)。

A.5.5.3 运维安全管理(E503)

本类产品针对系统重要资产的维护过程实现单点登录、集中授权、集中管理和审计,运维安全管理

产品为运维用户提供统一的身份认证接口、多种远程运维管理方式,对资产及其账号等进行集中管理和授权,监控和审计运维操作过程,并对违规操作行为进行报警、阻断。该类产品保护的对象是服务器、网络设备、安全产品、数据库等系统重要资产。

任何提供以上功能,且该功能为主导性功能的产品,均可归入本类(E503)。

A.5.5.4 统一身份鉴别与授权(E504)

本类产品针对应用系统进行集中管理,目的是实现一次登录后就可访问所有有权限访问的应用系统。

本类产品所提供的安全功能可主要归纳为两个方面:

- a) 鉴别管理,通过构建统一用户信息数据库,实现对服务、组织、人员、组、策略以及其他资源的集中、分层、分组管理;
- b) 授权管理,可授权指定的应用系统给指定的人员访问或使用,并可针对其访问权限进行时间、网段等策略级别控制。

任何提供以上两种功能,且该功能为主导性功能的产品,均可归入本类(E504)。

A.5.6 安全管理支持其他(EX)

不能归为上述 5 类的安全管理支持类产品暂归为安全管理支持其他类(EX)。

A.6 其他(X)

不能归为上述 5 类的信息安全产品暂归为其他类(X)。

附录 B
(规范性附录)
领域属性描述

信息安全产品可具有适用领域属性,领域属性代码为 1 位字母,见表 B.1。

表 B.1 信息安全产品适用领域属性与代码

代码	领域属性	领域属性简称
A	传统	—
B	工业控制系统	工控
C	云计算	云
D	移动互联	移动
E	物联网	物联网
F	大数据	大数据
G	人工智能	人工智能
H	区块链	区块链

对于三级分类产品具有特定适用领域属性的情况,可在三级分类代码后增加领域属性代码,产品名称默认为三级分类产品名称前增加其领域属性简称(有特殊命名方式的不作说明)。

以防火墙产品(三级分类代码为 C301)为例,当需要说明其具有特定适用领域时,可使用代码 C301B 代表该产品是适用于工业控制系统领域的防火墙,C301C 代表该产品是适用于云计算领域的防火墙,C301D 代表该产品是适用于移动互联领域的防火墙(目前尚未有适用于物联网领域和大数据领域的防火墙产品,因此 C301E 和 C301F 未列出)。

若三级分类产品同时适用于多个领域,可在三级分类代码后依序增加所有适用领域的属性代码。

以防火墙产品(三级分类代码为 C301)为例,若该产品同时适用于传统领域和工业控制系统领域,则其代码为 C301AB;若该产品同时适用于工业控制系统领域和移动互联领域,则其代码为 C301BD;若该产品同时适用于传统领域、工业控制系统领域和移动互联领域,则其代码为 C301ABD。

参 考 文 献

- [1] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求
 - [2] 中华人民共和国网络安全法,2016年11月7日.
-