

# 前 言

为了贯彻《中华人民共和国计算机信息系统安全保护条例》的精神,并配合计算机信息系统安全专用产品销售许可证制度的实施,公安部计算机管理监察司委托中国科学院中国科学技术大学研究生院信息安全国家重点实验室编写《计算机信息系统安全专用产品分类原则》。

本标准在技术内容上参照国内外相关内容,编写格式和方法按照《标准化工作导则 第1单元:标准的起草和表述规则》的要求制定。

本标准由公安部计算机管理监察司提出。

本标准由公安部信息标准化技术委员会归口。

本标准起草单位:信息安全国家重点实验室。

本标准主要起草人:柯云、戴英侠、赵战生、刘凤昌、高新宇、王学海。

中华人民共和国公共安全行业标准

计算机信息系统安全  
专用产品分类原则

GA 163—1997

Classification of security products in  
computer information systems

1 范围

本标准规定了计算机信息系统安全专用产品分类原则。  
本标准适用于保护计算机信息系统安全专用产品,涉及实体安全、运行安全和信息安全三个方面。  
实体安全包括环境安全、设备安全和媒体安全三个方面。  
运行安全包括风险分析、审计跟踪、备份与恢复、应急四个方面。  
信息安全包括操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密与鉴别七个方面。

2 分类原则

为了保证分类体系的科学性,遵循如下原则:

- a) 适度的前瞻性;
- b) 标准的可操作性;
- c) 分类体系的完整性;
- d) 与传统的兼容性;
- e) 按产品功能分类。

3 术语定义

本标准采用下列定义。

- 3.1 计算机信息系统 computer information system  
是指由计算机及其相关的和配套的设备、设施(含网络)构成的,按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。
- 3.2 计算机信息系统安全专用产品 security products in computer information systems  
是指用于保护计算机信息系统安全的专用硬件和软件产品。
- 3.3 实体安全 physical security  
保护计算机设备、设施(含网络)以及其他媒体免遭地震、水灾、火灾、有害气体和其他环境事故(如电磁污染等)破坏的措施、过程。
- 3.4 运行安全 operation security  
为保障系统功能的安全实现,提供一套安全措施(如风险分析、审计跟踪、备份与恢复、应急等)来保护信息处理过程的安全。
- 3.5 信息安全 information security

防止信息财产被故意的或偶然的非授权泄露、更改、破坏或使信息不可用的系统辨识、控制。即确保信息的完整性、保密性、可用性和可控性。

### 3.6 黑客 hacker

对计算机信息系统进行非授权访问的人员。

### 3.7 应急计划 contingency plan

在紧急状态下,使系统能够尽量完成原定任务的计划。

### 3.8 证书授权 certificate authority

通过证书的形式证明实体(如用户身份,用户的公开密钥等)的真实性。

### 3.9 安全操作系统 secure operation system

为所管理的数据和资源提供相应的安全保护,而有效控制硬件和软件功能的操作系统。

### 3.10 访问控制 access control

指对主体访问客体的权限或能力的限制,以及限制进入物理区域(出入控制)和限制使用计算机系统和计算机存储数据的过程(存取控制)。

### 3.11 防火墙 fire wall

设置在两个或多个网络之间的安全阻隔,用于保证本地网络资源的安全,通常是包含软件部分和硬件部分的一个系统或多个系统的组合。

### 3.12 计算机病毒 computer virus

是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据、影响计算机使用并能自我复制的一组计算机指令或程序代码。

## 4 类别体系

### 4.1 类别(A)实体安全

#### 4.1.1 类别(A10)环境安全

本类产品提供对计算机信息系统所在环境的安全保护,主要包括受灾防护和区域防护。

##### 4.1.1.1 类别(A11)受灾防护

本类产品提供受灾报警、受灾保护和受灾恢复等功能,目的是保护计算机信息系统免受水、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归纳为三个方面:

- a) 灾难发生时,对灾难的检测和报警;
- b) 灾难发生时,对正遭受破坏的计算机信息系统采取紧急措施,进行现场实时保护;
- c) 灾难发生后,对已经遭受某种破坏的计算机信息系统进行灾后恢复。任何提供以上一种或数种功能的产品均可归入本类。

##### 4.1.1.2 类别(A12)受灾恢复计划辅助软件

本类产品为制订受灾恢复计划提供计算机辅助,它主要是以受灾恢复计划辅助软件的形式提供。

本类产品的安全功能可归纳为三个方面:

- a) 灾难发生时的影响分析;
- b) 受灾恢复计划的概要设计或详细制订;
- 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的产品均可归入本类。

##### 4.1.1.3 类别(A13)区域防护

本类产品对特定区域提供某种形式的保护和隔离。

本类产品的安全功能可归纳为两个方面:

- a) 静止区域保护,如通过电子手段(如红外扫描等)或其他手段对特定区域(如机房等)进行某种形

式的保护(如监测和控制等);

b) 活动区域保护,对活动区域(如活动机房等)进行某种形式的保护。任何提供以上一种或两种功能的产品均可归入本类。

#### 4.1.2 类别(A20)设备安全

本类产品提供对计算机信息系统设备的安全保护。它主要包括设备的防盗和防毁,防止电磁信息泄漏,防止线路截获,抗电磁干扰以及电源保护等六个方面。

##### 4.1.2.1 类别(A21)设备防盗

本类产品提供对计算机信息系统设备的防盗保护。

本类产品所提供的安全功能可归纳为:

使用一定的防盗手段(如移动报警器、数字探测报警和部件上锁)用于计算机信息系统设备和部件,以提高计算机信息系统设备和部件的安全性。

任何提供以上功能的产品均可归入本类。

##### 4.1.2.2 类别(A22)设备防毁

本类产品提供对计算机信息系统设备的防毁保护。

本类产品所提供的安全功能可归纳为两个方面:

a) 对抗自然力的破坏,使用一定的防毁措施(如接地保护等)保护计算机信息系统设备和部件;

b) 对抗人为的破坏,使用一定的防毁措施(如防砸外壳)保护计算机信息系统设备和部件。

任何提供以上一种或两种功能的产品均可归入本类。

##### 4.1.2.3 类别(A23)防止电磁信息泄漏

本类产品用于防止计算机信息系统中的电磁信息的泄漏,从而提高系统内敏感信息的安全性。如防止电磁信息泄漏的各种涂料、材料和设备等都属于本类。

本类产品所提供的安全功能可归纳为三个方面:

a) 防止电磁信息的泄漏(如屏蔽室等防止电磁辐射引起的信息泄漏);

b) 干扰泄漏的电磁信息(如利用电磁干扰对泄漏的电磁信息进行置乱);

c) 吸收泄漏的电磁信息(如通过特殊材料/涂料等吸收泄漏的电磁信息)。

任何提供以上一种或数种功能的产品均可归入本类。

##### 4.1.2.4 类别(A24)防止线路截获

本类产品用于防止对计算机信息系统通信线路的截获和外界对计算机信息系统的通信线路的干扰。

本类产品的安全功能可归纳为四个方面:

a) 预防线路截获,使线路截获设备无法正常工作;

b) 探测线路截获,发现线路截获并报警;

c) 定位线路截获,发现线路截获设备工作的位置;

d) 对抗线路截获,防止线路截获设备的有效使用。

任何提供以上一种或数种功能的产品可归入本类。

##### 4.1.2.5 类别(A25)抗电磁干扰

本类产品用于防止对计算机信息系统的电磁干扰,从而保护系统内部的信息。

本类产品的安全功能可归纳为两个方面:

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的产品可归入本类。

##### 4.1.2.6 类别(A26)电源保护

本类产品为计算机信息系统设备的可靠运行提供能源保障,例如不间断电源、纹波抑制器、电源调

节软件等都属于本类。

本类产品的安全功能可归纳为两个方面：

- 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的产品均可归入本类。

#### 4.1.3 类别(A30)媒体安全

本类产品提供对媒体数据和媒体本身的安全保护。

##### 4.1.3.1 类别(A31)媒体的安全

本类产品提供对媒体的安全保管,目的是保护存储在媒体上的信息。

本类产品的安全功能可归纳为两个方面：

- a) 媒体的防盗；
- b) 媒体的防毁,如防霉和防砸等。

任何提供以上一种或数种功能的产品均可归入本类。

##### 4.1.3.2 类别(A32)媒体数据的安全

本类产品提供对媒体数据的保护。媒体数据的安全删除和媒体的安全销毁是为了防止被删除的或者被销毁的敏感数据被他人恢复。

本类产品的安全功能可归纳为三个方面：

- a) 媒体数据的防盗,如防止媒体数据被非法拷贝；
- b) 媒体数据的销毁,包括媒体的物理销毁(如媒体粉碎等)和媒体数据的彻底销毁(如消磁等),防止媒体数据删除或销毁后被他人恢复而泄露信息；
- c) 媒体数据的防毁,防止意外或故意的破坏使媒体数据的丢失。

任何提供以上一种或数种功能的产品均可归入本类。

#### 4.2 类别(B)运行安全

##### 4.2.1 类别(B10)风险分析

本类产品提供对计算机信息系统进行人工或自动的风险分析。它首先是对系统进行静态的分析(尤指系统设计前和系统运行前的风险分析),旨在发现系统的潜在安全隐患;其次是对系统进行动态的分析,即在系统运行过程中测试、跟踪并记录其活动,旨在发现系统运行期的安全漏洞;最后是系统运行后的分析,并提供相应的系统脆弱性分析报告。

本类产品的安全功能可归纳为四个方面：

- a) 系统设计前的风险分析 通过分析系统固有的脆弱性,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分析 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) 系统运行期的风险分析 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并及时通告安全管理员；
- d) 系统运行后的风险分析 分析系统运行记录,旨在发现系统的安全隐患,为改进系统的安全性提供分析报告。

任何提供以上一种或数种功能的产品均可归入本类。

##### 4.2.2 类别(B20)审计跟踪

本类产品对计算机 2 信息系统进行人工或自动的审计跟踪、保存审计记录和维护详尽的审计日志。

本类产品的安全功能可归纳为三个方面：

- a) 记录和跟踪各种系统状态的变化,如提供对系统故意入侵行为的记录和对系统安全功能违反的记录；
- b) 实现对各种安全事故的定位,如监控和捕捉各种安全事件；

c) 保存、维护和管理审计日志。

任何提供以上一种或数种功能的产品均可归入本类。

#### 4.2.3 类别(B30)备份与恢复

本类产品提供对系统设备和系统数据的备份与恢复,对系统数据的备份和恢复可以使用多种介质(如磁介质、纸介质、光盘、缩微载体等)。

本类产品的安全功能可归纳为三个方面:

a) 提供场点内高速度、大容量自动的数据存储、备份和恢复;

b) 提供场点外的数据存储、备份和恢复,如通过专用安全记录存储设施对系统内的主要数据进行备份;

c) 提供对系统设备的备份。

任何提供以上一种或数种功能的产品均可归入本类。

#### 4.2.4 类别(B40)应急

本类产品提供在紧急事件或安全事故发生时,保障计算机信息系统继续运行或紧急恢复所需要的一类产品,如应急计划辅助软件和应急设施两个方面。

##### 4.2.4.1 类别(B41)应急计划辅助软件

本类产品为制订应急计划提供计算机辅助,它主要是以应急计划辅助软件的形式提供。

本类产品的安全功能可归纳为三个方面:

a) 紧急事件或安全事故发生时的影响分析;

b) 应急计划的概要设计或详细制订;

c) 应急计划的测试与完善。

任何提供以上一种或数种功能的产品均可归入本类。

##### 4.2.4.2 类别(B42)应急设施

本类产品提供在紧急事件或安全事故发生时,计算机信息系统实施应急计划所需要的一类产品,它包括实时应急设施、非实时应急设施等。这些设施一般由专门厂商提供。实时应急设施、非实时应急设施的区别主要表现在对紧急事件发生时的响应时间长短上。

本类产品的安全功能可归纳为两个方面:

a) 提供实时应急设施,实现应急计划,保障计算机信息系统的正常安全运行;

b) 提供非实时应急设施,实现应急计划。

任何提供以上一种或两种功能的产品均可归入本类。

#### 4.3 类别(C)信息安全

##### 4.3.1 类别(C10)操作系统安全

本类产品提供对计算机信息系统的硬件和软件资源的有效控制,能够为所管理的资源提供相应的安全保护。它们或是以底层操作系统所提供的安全机制为基础构作安全模块,或者完全取代底层操作系统,目的是为建立安全信息系统提供一个可信的安全平台。

##### 4.3.1.1 类别(C11)安全操作系统

本类产品是安全操作系统,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。

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。

##### 4.3.1.2 类别(C12)操作系统安全部件

本类产品是操作系统安全部件,目的是增强现有操作系统的安全性。

本类产品的安全功能可归纳为两个方面:

a) 通过构作安全模块,增强现有操作系统的安全性;

b) 通过构作安全外罩,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的产品均可归入本类。

#### 4.3.2 类别(C20)数据库安全

本类产品对数据库系统所管理的数据和资源提供安全保护。它一般采用多种安全机制与操作系统相结合,实现数据库的安全保护。

##### 4.3.2.1 类别(C21)安全数据库系统

本类产品是安全数据库系统,即从系统设计、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安全数据库系统。

任何具有不同安全级别的安全数据库系统均可归入本类。

##### 4.3.2.2 类别(C22)数据库系统安全部件

本类产品是数据库系统安全部件,是以现有数据库系统所提供的功能为基础构造安全模块,旨在增强现有数据库系统的安全性。

本类产品的安全功能可归纳为两个方面:

- 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的产品均可归入本类。

#### 4.3.3 类别(C30)网络安全

本类产品提供访问网络资源或使用网络服务的安全保护。

##### 4.3.3.1 类别(C31)网络安全管理

本类产品为网络的使用提供安全管理。

本类产品的安全功能可归纳为四个方面:

- a) 帮助协调网络的使用,预防安全事故的发生;
- b) 跟踪并记录网络的使用,监测系统状态的变化。如提供对网络系统故意入侵行为的记录和对违反网络安全管理行为的记录;
- c) 实现对各种网络安全事故的定位,探测网络安全事件发生的确切位置;
- d) 提供某种程度的对紧急事件或安全事故的故障排除能力。

任何提供以上一种或数种功能的产品均可归入本类。

##### 4.3.3.2 类别(C32)安全网络系统

本类产品对网络资源的访问和网络服务的使用提供一套完整的安全保护。

本类产品是安全网络系统,即从网络系统的设计、实现、使用和管理各个阶段遵循一套完整的安全策略的网络系统。

任何具有不同安全级别的安全网络系统均可归入本类。

##### 4.3.3.3 类别(C33)网络系统安全部件

本类产品是网络系统安全部件,是对网络系统的某个过程、部分或服务提供安全保护,旨在增强整个网络系统的安全性。

本类产品的安全功能可归纳为三个方面:

- a) 对网络资源访问的某一过程提供安全保护,例如身份认证是对登录过程的保护,旨在防止黑客对网络资源的访问;
- b) 对网络资源的某一部分提供安全保护,例如防火墙是对网络资源的某个部分(本地网络资源)的保护;
- c) 对网络系统提供的某种服务提供安全保护,例如安全电子邮件服务是对网络系统提供的电子邮件服务的保护。

任何提供以上一种或数种功能的产品均可归入本类。

#### 4.3.4 类别(C40)计算机病毒防护

本类产品提供对计算机病毒的防护。病毒防护包括单机系统的防护和网络系统的防护。

单机系统的防护侧重于防护本地计算机资源,而网络系统的防护侧重于防护网络系统资源。计算机病毒防护产品是通过建立系统保护机制,预防、检测和消除病毒。

#### 4.3.4.1 类别(C41)单机系统病毒防护

本类产品提供对单机系统的病毒防护,既可以是软件产品,也可以是硬件产品。

本类产品安全功能可归纳为五个方面:

- a) 预防计算机病毒侵入系统;
- b) 检测已侵入系统的计算机病毒;
- c) 定位已侵入系统的病毒;
- d) 防止病毒在系统中的传染;
- e) 清除系统中已发现的计算机病毒。

任何提供以上一种或数种功能的产品均可归入本类。

#### 4.3.4.2 类别(C42)网络系统病毒防护

本类产品提供对网络系统的病毒防护。

本类产品安全功能可归纳为五个方面:

- a) 预防计算机病毒侵入网络系统;
- b) 检测已侵入网络系统的病毒;
- c) 定位已侵入网络系统的病毒;
- d) 防止网络系统中病毒的传染;
- e) 清除网络系统中已发现的病毒。

任何提供以上一种或数种功能的产品均可归入本类。

#### 4.3.5 类别(C50)访问控制

本类产品保证系统的外部用户或内部用户对系统资源的访问以及对敏感信息的访问方式符合组织安全策略。本类产品主要包括:出入控制和存取控制。

##### 4.3.5.1 类别(C51)出入控制

本类产品主要用于阻止非授权用户进入机构或组织。一般是以电子技术、生物技术或者电子技术与生物技术结合阻止非授权用户进入。

本类产品包括:

- a) 物理通道的控制,例如利用重量检查控制通过通道的人数;
- b) 门的控制,例如双重门、陷阱门等。

凡是采用电子技术、生物特征技术以及与其他技术相结合以实现出入控制的安全产品均可归入本类。

##### 4.3.5.2 类别(C52)存取控制

本类产品提供主体访问客体时的存取控制,如通过对授权用户存取系统敏感信息时进行安全性检查,以实现对授权用户的存取权限的控制。

本类产品提供的安全功能可归纳为四个方面:

- a) 提供对口令字的管理和控制功能,例如提供一个弱口令字库,禁止用户使用弱口令字,强制用户更换口令字等;
- b) 防止入侵者对口令字的探测;
- c) 监测用户对某一分区或域的存取;
- d) 提供系统中主体对客体访问权限的控制。

任何提供以上一种或数种功能的产品均可归入本类。

#### 4.3.6 类别(C60)加密



本类产品提供数据加密和密钥管理。

#### 4.3.6.1 类别(C61)加密设备

本类产品提供对数据的加密。

本类产品提供的安全功能可归纳为三个方面：

- a) 对文字的加密；
- b) 对语音的加密；
- c) 对图像、图形的加密。

任何提供以上一种或数种功能的产品均可归入本类。

#### 4.3.6.2 类别(C62)密钥管理

本类产品提供对密钥的管理。例如证书授权中心(提供对用户的公开密钥的管理)和密钥恢复,都属于本类。

本类产品的安全功能可归纳为六个方面：

- a) 密钥分发或注入；
- b) 密钥更新；
- c) 密钥回收；
- d) 密钥归档；
- e) 密钥托管；
- f) 密钥审计。

任何提供以上一种或数种功能的产品均可归入本类。

#### 4.3.7 类别(C70)鉴别

本类产品提供身份鉴别和信息鉴别,身份鉴别是提供对信息收发方(包括用户、设备和进程)真实身份的鉴别;信息鉴别是提供对信息的正确性、完整性和不可否认性的鉴别。本类产品亦提供防伪性。

##### 4.3.7.1 类别(C71)身份鉴别

本类产品提供对用户的身份鉴别,主要用于阻止非授权用户对系统资源的访问。一般是以电子技术、生物技术或者电子技术与生物技术结合鉴别授权用户身份的真实性。

本类产品的安全功能可归纳为三个方面：

- a) 根据用户的生物特征来鉴别其真伪；
- b) 根据用户所持物品来鉴别其真伪；
- c) 根据用户所知来鉴别其真伪。

任何提供以上一种或数种功能的产品均可归入本类。

##### 4.3.7.2 类别(C72)信息完整性鉴别

本类产品提供信息完整性鉴别,使得用户、设备、进程可以证实接收到的信息的完整性。

本类产品的安全功能可归纳为：

证实信息内容未被非法修改或遗漏,如完整性校验设备。

任何提供以上功能的产品均可归入本类。

#### 4.3.7.3 类别(C73)不可否认性鉴别

本类产品提供不可否认性鉴别,使得信息发送者不可否认对信息的发送和信息接收者不可否认对信息的接收。

本类产品安全功能可归纳为两个方面:

- a) 证实发方发送的信息确实为收方接收,收方不可否认;
- b) 证实收方接收的信息确实为发方发送,发方不可否认。

任何提供以上一种或两种功能的产品均可归入本类。

---