ICS 35.040
L 80

中华人民共和国国家标准

GB/T 37090—2018

信息安全技术　病毒防治产品安全技术要求和测试评价方法

Information security technology—Security technical requirements, testing and evaluation methods for antivirus products

2018-12-28 发布　　2019-07-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

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:国家计算机病毒应急处理中心、国家网络与信息安全信息通报中心、公安部第一研究所、中国电子科技集团公司第十五研究所(信息产业信息安全测评中心)、国家信息中心、天津市公安局网络安全保卫总队。

本标准主要起草人:陈建民、杜振华、曹鹏、张瑞、张秀东、冯军亮、黄一斌、蒋勇、禄凯、刘健、王文一、张喆、李菊、舒心、徐超、胡光俊、刘威、王琚、王茗。

信息安全技术　病毒防治产品安全技术要求和测试评价方法

1　范围

本标准规定了病毒防治产品的技术要求，包括功能要求、安全要求和安全保障要求，并给出了测试评价方法。

本标准适用于病毒防治产品的设计、开发及检测。

2　术语和定义

下列术语和定义适用于本文件。

2.1

恶意软件　malware

能够影响计算机操作系统、应用程序和数据的完整性、可用性、可控性和保密性的计算机程序或代码的软件。

2.2

病毒　virus

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，影响计算机正常使用，并能自我复制的一组计算机指令或者程序代码。

2.3

文件感染型病毒　file viruses

以文件为宿主，能够通过将自身包含的恶意代码插入到目标文件中，实现对目标文件的感染。

2.4

宏病毒　macro viruses

利用文档中的宏代码编辑的恶意代码，在允许宏代码运行的条件下，可以在打开文档时运行。

2.5

蠕虫　worm

通过信息系统漏洞缺陷或信息系统使用者的弱点主动进行传播的恶意程序。

2.6

木马程序　trojan horses program

主动与攻击者通信，接收来自攻击者的指令，并能够根据指令对所在主机进行各种恶意操作的恶意程序。

2.7

间谍软件　spyware

不依赖攻击者指令，潜伏在主机中，按照事先设定的执行条件收集特定的敏感信息并隐蔽地传输给攻击者的恶意程序。

2.8

脚本恶意程序　malicious script program

使用脚本语言编写的，并在脚本执行环境中运行的恶意程序。