



中华人民共和国公共安全行业标准

GA/T 1536—2018

信息安全技术 计算机主机安全检测产品测评准则

Information security technology—Testing and evaluation criteria for detection products of host computer security

2018-12-26 发布

2018-12-26 实施

中华人民共和国公安部 发布

目 次

前言 III

1 范围 1

2 规范化引用文件 1

3 术语和定义 1

4 受检要求 2

5 测试指标要求 2

6 功能要求 2

7 测试方法 4

8 报告格式 4

9 评级方法 4

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：国家计算机病毒应急处理中心、天津市公安局网络安全保卫总队、江苏通付盾信息安全技术有限公司、恒安嘉新(北京)科技股份公司、北京启明星辰信息安全技术有限公司、北京奇虎科技有限公司、北京天融信科技有限公司、南开大学、北京安天网络安全技术有限公司。

本标准主要起草人：陈建民、刘彦、杜振华、黄一斌、曹鹏、杨键、赵晓明、张韞菁、张瑞、张鑫、王文一、肖新光、赵焕菊、张振伟、崔婷婷、徐雨晴、王龔、贾春福、舒心、李菊、孙波、李冬。

信息安全技术

计算机主机安全检测产品测评准则

1 范围

本标准规定了计算机主机安全检测产品的受检要求、测试指标要求、功能要求、测试方法、报告格式及评级方法。

本标准适用于计算机主机安全检测产品的开发和检测。

2 规范化引用文件

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 18336.3—2015 信息技术 安全技术 信息技术安全评估准则 第3部分:安全保障组件

GA 243—2000 计算机病毒防治产品评级准则

GA/T 757—2008 程序功能检验方法

3 术语和定义

GB/T 18336.3—2015、GA 243—2000、GA/T 757—2008 界定的以及下列术语和定义适用于本文件。

3.1

操作系统安全 operating system security

操作系统所存储、传输和处理的信息的保密性、完整性和可用性的表征。

3.2

用户标识 user identification

用来标明用户的身份,确保用户在系统中的唯一性和可辨认性,一般用名称和用户标识符(UID)来标明系统中的一个用户。

3.3

用户鉴别 user authentication

用特定信息对用户身份的真实性进行确认。

3.4

安全策略 security policy

对计算机信息系统中与安全相关的资源,尤其是敏感信息进行管理、保护、控制和发布的规定和实施细则。

3.5

访问控制 access control

防止对资源的未授权使用,包括防止以未授权方式使用某一资源。

3.6

数据完整性 data integrity

数据没有遭受以未授权方式所做的篡改或破坏。