ICS 35.040
L 80

GA

中华人民共和国公共安全行业标准

GA/T 1539—2018

信息安全技术
网络病毒监控系统
安全技术要求和测试评价方法

Information security technology—Security technical requirements and evaluation approaches for virus detection system products

2018-12-27 发布　　2018-12-27 实施

中华人民共和国公安部　　发 布

目　　次

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、公安部十一局七处、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、北京工业大学、北京瑞星信息技术有限公司、北京安天网络安全技术有限公司、北京启明星辰信息安全技术有限公司、恒安嘉新（北京）科技股份公司、北京神州绿盟信息安全科技股份有限公司、北京天融信科技有限公司。

本标准主要起草人：陈建民、杜振华、张俊兵、陆磊、曹鹏、张喆、张瑞、刘彦、黄一斌、李冬、孟彬、张鑫、刘健、禄凯、王冠、王世玉、叶荣军、赵焕菊、杨绍波、徐雨晴、崔婷婷、焦玉峰、王龑。

信息安全技术
网络病毒监控系统
安全技术要求和测试评价方法

1 范围

本标准规定了网络病毒监控系统的功能要求、安全要求、性能要求及安全保障要求，并给出了测试评价方法。

本标准适用于网络病毒监控系统的设计、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

网络病毒监控系统 virus detection system

用旁路方式监听网络内的数据包并进行分析，以发现网络中传播的病毒及其相关行为的系统。

2.2

病毒 virus

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，包括文件型病毒、蠕虫、木马程序、宏病毒、脚本病毒等恶意程序。

2.3

病毒捕获 virus capture

网络病毒监控系统为保留病毒或疑似病毒样本以及受感染的文件，而将从网络上捕获的相应文件存储在特定的受限制存储空间的处理方式。

2.4

内部网络 internal network

通过防火墙/网络病毒监控系统隔离的可信任区域或保护区域。

2.5

外部网络 external network

通过防火墙/网络病毒监控系统隔离的不可信任区域或非保护区域。

2.6

线速 wire speed

网络病毒监控系统所监控网络环境理论上能达到的最大转发速率。

2.7

负载量 peak load

网络病毒监控系统在不丢包的情况下处理监控数据的能力，一般以能达到的线速(或称通过速率)的百分比来表示。

2.8

恶意 URL malicious URL

指向的资源中含有病毒的 URL。