ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 910—2020
代替 GA/T 910—2010

信息安全技术
内网主机监测产品安全技术要求

Information security technology—
Security technical requirements for intranet-host monitoring products

2020-03-03 发布　　2020-05-01 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。

本标准代替 GA/T 910—2010《信息安全技术　内网主机监测产品安全技术要求》，与 GA/T 910—2010 相比主要技术变化如下：

——修改了等级划分要求，将等级划分为基本级和增强级两级（见第 6 章，2010 年版的第 7 章）；

——修改了安全功能要求，将监测功能和控制功能分开（见 4.1、4.2，2010 年版的第 4 章）；

——修改了安全保障要求（见第 5 章，2010 年版的第 5 章）；

——增加了打印监测（见 4.1.7）；

——增加了主机安全策略监测和主机安全策略加固（见 4.1.11、4.2.7）；

——增加了受控主机管理要求（见 4.4）。

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：公安部计算机信息系统安全产品质量监督检验中心。

本标准主要起草人：邹春明、田原、刘瑞、俞优、陆臻、沈亮。

本标准的历次版本发布情况为：

——GA/T 910—2010。

信息安全技术
内网主机监测产品安全技术要求

1 范围

本标准规定了内网主机监测产品的安全功能要求、安全保障要求和等级划分要求。

本标准适用于内网主机监测产品的设计、开发及检测。

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/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

GB/T 25069—2010 信息安全技术 术语

3 术语和定义

GB/T 18336.3—2015 和 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

受控主机 controlled host

接受监控的内网主机。

3.2

内网主机监测产品 intranet-host monitoring product

对受控主机上的各项活动进行监测和/或控制的产品。

3.3

非授权外联 non-authorized internet connection

内网主机未授权访问外部网络的行为。

3.4

外围接口 external interface

计算机与外界进行数据交互的各种接口。

4 安全功能要求

4.1 安全监测功能

4.1.1 在线状态监测

产品应能对内网主机的以下状态进行监测：

a) 受控主机的在线状态、代理运行状态；

b) 设定IP地址范围内在线主机的代理安装情况。