ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

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 technology requirements for intranet-host monitoring products

2010-10-30 发布　　2010-11-01 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、张奕、张笑笑、俞优、吴其聪、顾健。

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、自身安全功能要求、安全保证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 5271.8—2001 信息技术 词汇 第8部分：安全

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 18336.3—2008 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求

3 术语和定义

GB/T 5271.8—2001、GB 17859—1999 和 GB/T 18336.3—2008 界定的以及下列术语和定义适用于本文件。

3.1

内网主机 intranet-host

主要分为两类：受控主机，内网中安装了代理并受监控的主机；非受控主机，内网中除受控主机之外的所有主机。

3.2

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

采用代理(agent)/服务器(server)结构，对受控主机上的各项活动进行监控的产品。

3.3

非授权外联 non-authorized internet connection

内网主机访问未授权网络的行为。

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 在线状态监测

内网主机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) 设定范围内在线主机的代理安装情况。