ICS 35.240
A 90

GF

公安部计算机信息系统安全产品质量监督检验中心检验规范

MSTL_JGF_04-025 0101—2006

信息安全技术
主机文件监测产品检验规范

2006-01-01 发布　　2006-02-01 实施

公安部计算机信息系统安全产品质量监督检验中心 发布

目　　次

前　言

为了规范主机文件监测产品的开发与应用，保障公共信息网络安全，根据公安部公共信息网络安全监察局的要求，本规范对主机文件监测产品提出了安全功能要求和保证要求，作为对其进行检测的依据。

本规范由中华人民共和国公安部公共信息网络安全监察局批准。

本规范起草单位：公安部计算机信息系统安全产品质量监督检验中心。

公安部计算机信息系统安全产品质量监督检验中心负责对本规范的解释、提升和更改。

信息安全技术 主机文件监测产品检验规范

1 范围

本规范规定了主机文件监测产品的安全功能要求和保证要求。

本规范适用于主机文件监测产品的开发及检测。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 18336.3－2001 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（idt ISO/IEC 15408-3:1999）

3 术语和定义

3.1 主机文件监测

通过文件完整性检查、文件属性检查、关键字检查等手段对主机文件的修改行为做出监测。

3.2 文件监测安全策略

包括监测文件的范围设定，以及对修改行为的响应策略。

4 产品安全功能要求

4.1 安全策略定制

a) 产品应提供可有效对主机主要文件（如系统文件、配置文件）进行文件监测的默认策略；

b) 产品应对管理员提供策略增加、修改、删除与应用功能。

4.2 文件监测

a) 产品应提供对安全策略中指定文件进行监测的功能；

b) 对Windows系统，产品宜提供对注册表的键值进行监测的功能；

c) 对监测的结果应提供报警功能，报警策略可设置。

4.3 报表功能

a) 产品应对安全策略中指定文件增加、删除与修改作出明细报表；

b) 产品宜对安全策略中注册表键值的增加、删除与修改作出明细报表。

4.4 集中管理

产品宜提供对被检测主机的集中管理功能

4.5 产品自身安全

a) 提供策略下达与主机端报表的集中控制管理功能；

b) 产品对管理端与主机端的使用应提供口令保护功能；

c) 产品对被监测主机端模块应提供一定强度的自我保护功能，以防止安全功能被旁路；

d) 应保证网络传输数据的保密性与完整性。

5 产品安全保证要求

保证要求按 GB/T 18336.3－2001 第二级执行。