



# 中华人民共和国公共安全行业标准

GA/T 1392—2017

---

## 信息安全技术 主机文件监测产品 安全技术要求

Information security technology—Security technical requirements for  
hosts file monitoring products

2017-04-19 发布

2017-04-19 实施

---

中华人民共和国公安部 发布

## 目 次

前言 .....	III
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 主机文件监测产品描述 .....	1
5 总体说明 .....	2
5.1 安全技术要求分类 .....	2
5.2 安全等级划分 .....	2
6 安全功能要求 .....	2
6.1 安全策略定制 .....	2
6.2 文件监测 .....	2
6.3 报表 .....	2
6.4 操作系统支持 .....	2
6.5 报警功能 .....	2
6.6 自动恢复 .....	3
6.7 行为审计 .....	3
6.8 安全管理 .....	3
6.9 自身保护 .....	3
6.10 审计日志 .....	4
6.11 远程管理加密 .....	4
6.12 集中分组管理 .....	4
6.13 系统告警 .....	4
7 安全保障要求 .....	5
7.1 开发 .....	5
7.2 指导性文档 .....	6
7.3 生命周期支持 .....	6
7.4 测试 .....	7
7.5 脆弱性评定 .....	8
8 等级划分要求 .....	8
8.1 概述 .....	8
8.2 安全功能要求等级划分 .....	8
8.3 安全保障要求等级划分 .....	9

## 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、公安部第三研究所。

本标准主要起草人：张艳、郭运尧、陆臻、张笑笑、俞优、邹春明。

# 信息安全技术 主机文件监测产品 安全技术要求

## 1 范围

本标准规定了主机文件监测产品的安全功能要求、安全保障要求及等级划分要求。  
本标准适用于主机文件监测产品的设计、开发与测试。

## 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

#### 主机文件 **hosts file**

存放在计算机主机上的重要系统文件、配置文件及预定义的其他文件。

### 3.2

#### 主机文件监测 **hosts file monitoring**

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进行监测。

### 3.3

#### 用户 **user**

能够接触主机文件的人,并且此人不具有能影响主机文件监测安全策略执行的权限。

### 3.4

#### 文件监测安全策略 **security policy of file monitoring**

对主机文件的检测范围,以及对修改行为的响应措施进行设定的策略。

### 3.5

#### 授权管理员 **authorized administrator**

具备主机文件监测产品管理权限的用户,负责对产品中的系统配置、安全策略以及审计日志等进行管理。

## 4 主机文件监测产品描述

主机文件监测产品依据预先定义的安全策略,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(包括存放在主机上的重要系统文件、配置文件,以及预定义的其他文件)的状态、修改行为等作出监测并报警,从而保证主机上的文件资源不被未经授权访问和操作。