



中华人民共和国公共安全行业标准

GA/T 1393—2017

信息安全技术 主机安全加固系统 安全技术要求

Information security technology—Security technical requirements for
computer security reinforcement systems

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 主机安全加固系统描述 1
- 5 总体说明 2
 - 5.1 安全技术要求分类 2
 - 5.2 安全等级 2
- 6 安全功能要求 2
 - 6.1 身份鉴别 2
 - 6.2 安全标记 2
 - 6.3 强制访问控制 3
 - 6.4 安全审计 3
 - 6.5 完整性保护 3
 - 6.6 剩余信息保护 3
 - 6.7 管理员安全管理 4
 - 6.8 组件安全 4
 - 6.9 审计日志管理 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 7
- 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 8

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：宋好好、邱梓华、沈亮、陆臻、俞优、顾健。

信息安全技术 主机安全加固系统 安全技术要求

1 范围

本标准规定了主机安全加固系统的安全功能要求、安全保障要求和等级划分要求。
本标准适用于主机安全加固系统的设计、开发及测试。

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 界定的术语和定义适用于本文件。

4 主机安全加固系统描述

主机安全加固系统是在通用操作系统的基础上,通过对操作系统主客体进行安全标记、增加强制访问控制、完整性保护等技术手段,对操作系统进行安全功能增强,弥补通用操作系统安全性不高的缺陷,提高了操作系统的安全保护能力。

主机安全加固系统一般采用服务器、客户端部署模式;服务器用于存储各种安全管理策略、管理数据和审计数据,并将安全管理策略下发到客户端;客户端安装在需要被加固的通用操作系统上,并执行安全功能。其保护的资产是操作系统,此外主机安全加固系统本身及其内部的重要数据也是受保护的资产。

主机安全加固系统的典型部署运行环境见图1。