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_04-019 0101—2006

信息安全技术
安全管理平台产品检验规范

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

为了规范全国安全管理平台产品的开发与应用，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，本规范对安全管理平台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 安全管理平台产品检验规范

1 范围

本规范规定了安全管理平台产品的安全功能要求和安全保证要求。

本规范适用于安全管理平台产品的开发及检测。

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 安全管理平台

安全管理平台就是为了解决各个安全产品之间的协作问题而建立起来的一个信息交换、信息存储、信息处理平台，通过该平台，能够对各安全产品进行控制管理。

4 产品安全功能要求

4.1 安全产品监管功能

4.1.1 所支持的安全设备

安全管理平台至少要能够支持两个不同类型的安全产品，能够对其进行远程管理。应提供扩展接口。

4.1.2 安全设备管理

管理员能够增加、删除受控设备。

4.1.3 运行状态监测

安全管理平台能够实时监测各受控产品的状态，比如是否在线，CPU使用率、内存占用率等。

4.1.4 日志报警信息收集

安全管理平台能够收集各受控产品所产生的报警和日志等信息，并存储于永久性介质内。

4.1.5 统一日志格式

所收集日志需要统一格式，并保证不丢弃日志的数据项。

4.1.6 远程控制

可对受控产品状态进行控制，比如重启、停止，以及一些基本参数的配置等。

4.1.7 策略配置管理

能够对具体的策略进行配置，比如IDS报警策略，扫描器规则，防火墙的数据包过滤规则等。

4.1.8 响应机制

系统能够对日志或报警信息提供一定的响应机制，比如email，声音报警等。

4.1.9 身份鉴别

要通过鉴别才能够对安全产品进行管理。

4.1.10 通讯安全

系统所有组件之间的管理数据不能以明文形式传输。

4.2 审计管理功能

4.2.1 日志生成

系统日志至少包括用户身份鉴别（包括成功和失败）、其它一些重要操作。

4.2.2 日志组合查询

应能够对日志进行组合查询，至少能按时间、设备名等进行组合。

4.2.3 查阅权限

只有授权的管理员才能够对日志进行查阅以及其它操作。包括系统日志。

4.2.4 日志管理

授权管理员能够对日志进行删除、备份、清空等操作。包括系统日志。

4.2.5 统计报表

能够按时间、设备、事件、协议等生成统计报表。

4.2.6 防止审计数据丢失

提供一定的机制，防止磁盘空间不够的情况下导致数据丢失。

4.3 自身安全功能

4.3.1 管理员身份鉴别

应保证只有授权管理员才有权使用产品的管理功能，对授权管理员应进行身份认证。

4.3.2 鉴别失败处理

要有一定的措施防止对管理员口令的暴力猜测。

4.3.3 管理员分级

管理员要求分级，至少两个级别

5 产品安全保证要求

保证要求按 GB/T 18336.3－2001 第二级执行。