ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1394—2017

信息安全技术　运维安全管理产品安全技术要求

Information security technology—Security technical requirements for security operation and maintenance management 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

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、张笑笑、邹春明、赵婷、沈亮、李毅。

信息安全技术　运维安全管理产品安全技术要求

1　范围

本标准规定了运维安全管理产品的安全功能要求、安全保障要求及等级划分要求。

本标准适用于运维安全管理产品的设计、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

运维用户　operation and maintenance user

对服务器、网络设备和数据库等信息系统的重要资产进行运行维护的人员。

3.2

运维安全管理产品　security operation and maintenance management product

对信息系统重要资产的维护过程实现单点登录、集中授权、集中管理和审计的产品。

3.3

运维对象　operation and maintenance object

受运维安全管理产品保护的资产。

4　运维安全管理产品描述

运维安全管理产品为运维用户提供统一的身份认证接口、多种远程运维管理方式，对资产及其账号等进行集中管理和授权，监控和审计运维操作过程，并对违规操作行为进行报警、阻断。该类产品保护的对象是服务器、网络设备、安全产品、数据库、应用系统等信息系统重要资产。此外，运维安全管理产品本身及其内部的重要数据也是受保护的对象。

运维安全管理产品通常以旁路方式部署。运维安全管理产品的典型运行环境见图1。