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。

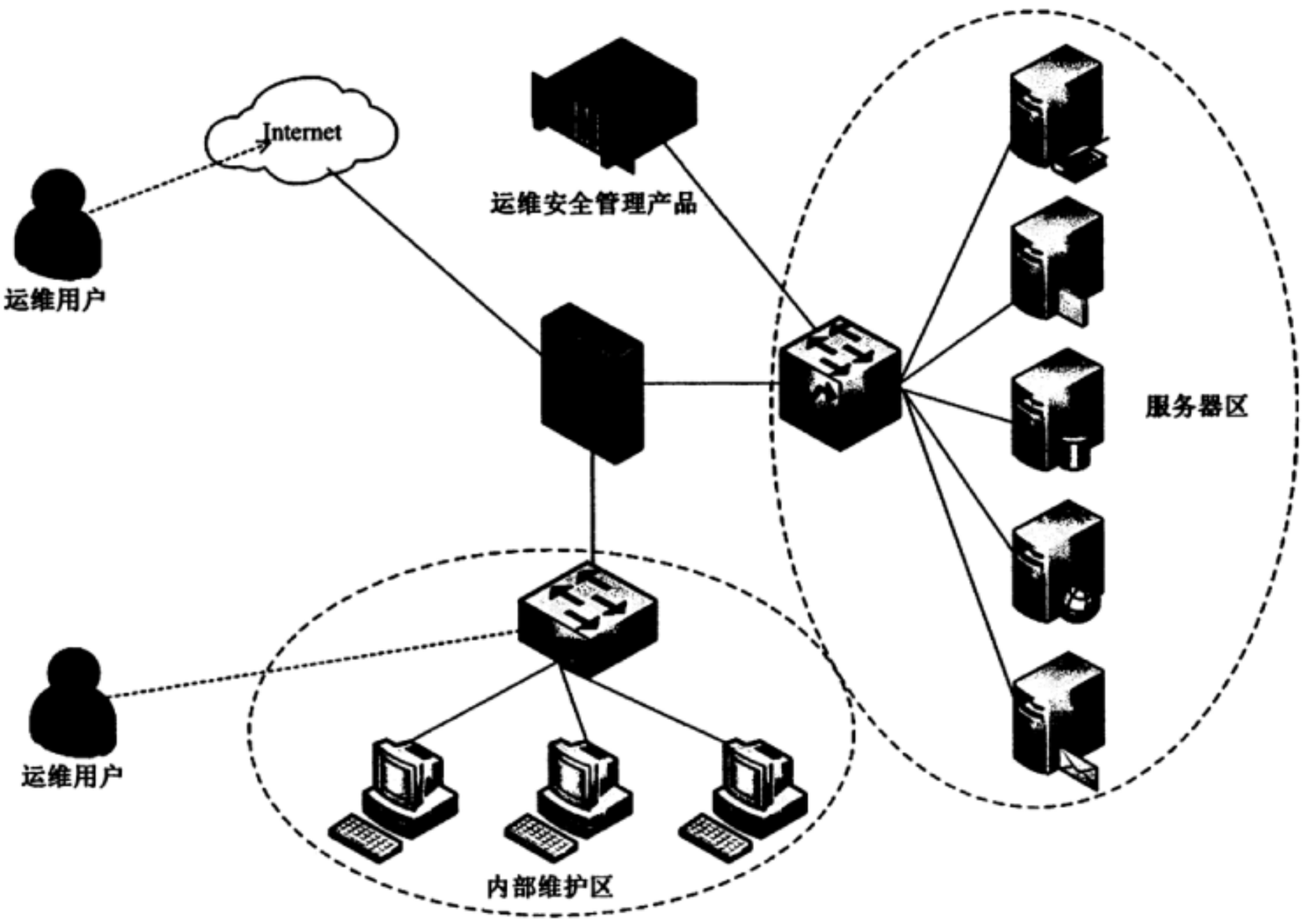

图 1　运维安全管理产品的典型运行环境

5　总体说明

5.1　安全技术要求分类

运维安全管理产品技术要求分为安全功能、安全保障要求两类。其中，安全功能要求是对运维安全管理产品应具备的安全功能提出具体要求，包括单点登录、访问权限控制、行为审计、身份鉴别、安全管理、审计日志等；安全保障要求针对运维安全管理产品的开发和使用文档的内容提出具体的要求，例如开发、指导性文档、生命周期支持、测试和脆弱性评定等。

5.2　安全等级划分

按照运维安全管理产品安全功能要求强度划分安全功能要求的级别，按照 GB/T 18336.3—2015 划分安全保障要求的级别。安全等级突出安全特性，分为基本级和增强级，安全功能强弱和安全保障要求高低是等级划分的具体依据。

6　安全功能要求

6.1　单点登录

产品应提供统一的身份鉴别功能，实现运维用户的单点登录，运维用户仅需经过产品的身份鉴别后，即可访问授权范围内的资产。

6.2　访问控制

产品应根据以下条件对运维用户实施访问控制：

a)　主体：运维用户、源地址等；

b） 客体：运维对象及其账户等；
c） 管理方式；
d） 操作命令、操作时间等。

6.3 操作审计

6.3.1 审计记录

产品应对运维用户的操作进行审计，生成审计记录，应至少包括：
a） 操作时间；
b） 运维用户；
c） 源地址；
d） 运维对象；
e） 管理方式；
f） 操作内容；
g） 操作结果等其他信息。

6.3.2 审计查阅

产品应仅允许授权管理员查阅审计记录，支持条件查询并以通用格式导出，查询条件包括：
a） 操作时间；
b） 运维用户；
c） 源地址；
d） 运维对象；
e） 操作命令等。

6.4 会话监视

产品应提供对访问运维对象会话过程的图形化实时监视功能。

6.5 会话回放

产品应提供如下会话回放功能：
a） 对访问运维对象会话过程的回放；
b） 按操作命令或时间进行定位回放。

6.6 告警

产品应依据告警策略对运维用户的违规操作进行告警，告警信息应至少包括：
a） 操作时间；
b） 运维用户；
c） 源地址；
d） 运维对象；
e） 管理方式；
f） 事件描述；
g） 触发的策略等。

6.7 违规操作阻断

产品应依据安全策略，自动阻断违规操作，确保运维用户访问过程的合规性。

6.8 高可用性

当产品发生故障时，通过冗余或 bypass 等方式保证产品的高可用性。

6.9 标识与鉴别

6.9.1 身份标识

产品应为管理员和运维用户提供唯一的身份标识。

6.9.2 基本鉴别

产品应在执行任何与安全功能相关操作之前鉴别管理员/运维用户的身份，并符合以下要求：

a） 若采用静态口令方式，口令有复杂度要求并定期更换；

b） 支持两种及两种以上身份鉴别方式。

6.9.3 鉴别失败处理

当对管理员/运维用户鉴别尝试连续失败达到设定的次数后，产品应阻止管理员/运维用户进一步的鉴别请求；最大失败次数仅由授权管理员设定。

6.9.4 超时锁定或注销

产品应具有登录超时锁定或注销功能，在设定的时间段内没有任何操作的情况下，终止会话，需要再次进行身份鉴别才能够重新操作，最大超时时间仅由授权管理员设定。

6.10 安全管理

6.10.1 安全功能管理

产品应允许授权管理员对产品进行以下管理：

a） 查看和修改安全属性；

b） 制定和修改各种安全策略。

6.10.2 管理员角色

产品应对管理员角色进行区分：

a） 具有至少两种不同权限的管理员角色，例如操作员、安全员、审计员等；

b） 根据不同的功能模块，自定义各种不同权限角色，并可对管理员分配角色。

6.10.3 远程管理加密

若产品采用网络远程方式管理，应保证管理数据保密传输。

6.10.4 远程管理主机

若产品提供远程管理功能，应对可远程管理的主机地址进行限制。

6.10.5 鉴别数据保护

产品应保证管理员、运维用户和运维对象的管理账号等鉴别数据以非明文形式存储，不被未授权查阅或修改。

6.11 审计日志

6.11.1 审计日志生成

产品应对下列事件生成审计日志，审计日志的内容至少应包括事件发生的日期、时间、主体标识、事件描述和结果：

a） 管理员/运维用户的鉴别成功和失败；
b） 对安全策略进行更改的操作；
c） 对角色进行增加、删除和属性修改的操作；
d） 对审计日志的备份；
e） 管理员的其他操作。

6.11.2 审计日志存储

产品应提供以下功能对审计日志进行存储：

a） 存储于掉电非易失性存储介质中；
b） 当存储空间达到阈值时，能通知授权管理员；
c） 当存储空间将要耗尽时，采取相应的防止审计日志丢失的技术措施。

6.11.3 审计日志管理

产品应提供下列审计日志管理功能：

a） 只允许授权管理员访问审计日志；
b） 对审计日志的条件查询功能；
c） 对审计日志的备份功能。

7 安全保障要求

7.1 开发

7.1.1 安全架构

开发者应提供产品安全功能的安全架构描述，安全架构描述应满足以下要求：

a） 与产品设计文档中对安全功能实施抽象描述的级别一致；
b） 描述与安全功能要求一致的产品安全功能的安全域；
c） 描述产品安全功能初始化过程为何是安全的；
d） 证实产品安全功能能够防止被破坏；
e） 证实产品安全功能能够防止安全特性被旁路。

7.1.2 功能规范

开发者应提供完备的功能规范说明，功能规范说明应满足以下要求：

a） 完全描述产品的安全功能；
b） 描述所有安全功能接口的目的与使用方法；
c） 标识和描述每个安全功能接口相关的所有参数；
d） 描述安全功能接口相关的安全功能实施行为；
e） 描述由安全功能实施行为处理而引起的直接错误消息；
f） 证实安全功能要求到安全功能接口的追溯；

g） 描述安全功能实施过程中，与安全功能接口相关的所有行为；
h） 描述可能由安全功能接口的调用而引起的所有直接错误消息。

7.1.3 实现表示

开发者应提供全部安全功能的实现表示，实现表示应满足以下要求：
a） 提供产品设计描述与实现表示实例之间的映射，并证明其一致性；
b） 按详细级别定义产品安全功能，详细程度达到无须进一步设计就能生成安全功能的程度；
c） 以开发人员使用的形式提供。

7.1.4 产品设计

开发者应提供产品设计文档，产品设计文档应满足以下要求：
a） 根据子系统描述产品结构；
b） 标识和描述产品安全功能的所有子系统；
c） 描述安全功能所有子系统间的相互作用；
d） 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的安全功能接口；
e） 根据模块描述安全功能；
f） 提供安全功能子系统到模块间的映射关系；
g） 描述所有安全功能实现模块，包括其目的及与其他模块间的相互作用；
h） 描述所有实现模块的安全功能要求相关接口、其他接口的返回值、与其他模块间的相互作用及调用的接口；
i） 描述所有安全功能的支撑或相关模块，包括其目的及与其他模块间的相互作用。

7.2 指导性文档

7.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每一种用户角色的描述应满足以下要求：
a） 描述在安全处理环境中被控制的用户可访问的功能和特权，包含适当的警示信息；
b） 描述如何以安全的方式使用产品提供的可用接口；
c） 描述可用功能和接口，尤其是受用户控制的所有安全参数，适当时指明安全值；
d） 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变安全功能所控制实体的安全特性；
e） 标识产品运行的所有可能状态（包括操作导致的失败或者操作性错误），以及它们与维持安全运行之间的因果关系和联系；
f） 充分实现安全目的所必须执行的安全策略。

7.2.2 准备程序

开发者应提供产品及其准备程序，准备程序描述应满足以下要求：
a） 描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；
b） 描述安全安装产品及其运行环境必需的所有步骤。

7.3 生命周期支持

7.3.1 配置管理能力

开发者的配置管理能力应满足以下要求：

a) 为产品的不同版本提供唯一的标识。
b) 使用配置管理系统对组成产品的所有配置项进行维护，并唯一标识配置项。
c) 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法。
d) 配置管理系统提供一种自动方式来支持产品的生成，通过该方式确保只能对产品的实现表示进行已授权的改变。
e) 配置管理文档包括一个配置管理计划，配置管理计划描述如何使用配置管理系统开发产品。实施的配置管理与配置管理计划相一致。
f) 配置管理计划描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。

7.3.2 配置管理范围

开发者应提供产品配置项列表，并说明配置项的开发者。配置项列表应包含以下内容：
a) 产品、安全保障要求的评估证据和产品的组成部分；
b) 实现表示、安全缺陷报告及其解决状态。

7.3.3 交付程序

开发者应使用一定的交付程序交付产品，并将交付过程文档化。在给用户方交付产品的各版本时，交付文档应描述为维护安全所必需的所有程序。

7.3.4 开发安全

开发者应提供开发安全文档。开发安全文档应描述在产品的开发环境中，为保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

7.3.5 生命周期定义

开发者应建立一个生命周期模型对产品的开发和维护进行的必要控制，并提供生命周期定义文档描述用于开发和维护产品的模型。

7.3.6 工具和技术

开发者应明确定义用于开发产品的工具，并提供开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

7.4 测试

7.4.1 测试覆盖

开发者应提供测试覆盖文档，测试覆盖描述应满足以下要求：
a) 表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能间的对应性；
b) 表明上述对应性是完备的，并证实功能规范中的所有安全功能接口都进行了测试。

7.4.2 测试深度

开发者应提供测试深度的分析。测试深度分析描述应满足以下要求：
a) 证实测试文档中的测试与产品设计中的安全功能子系统和实现模块之间的一致性；
b) 证实产品设计中的所有安全功能子系统、实现模块都已经进行过测试。

7.4.3 功能测试

开发者应测试产品安全功能，将结果文档化并提供测试文档。测试文档应包括以下内容：
a) 测试计划，标识要执行的测试，并描述执行每个测试的方案，这些方案包括对于其他测试结果

的任何顺序依赖性；

b） 预期的测试结果，表明测试成功后的预期输出；

c） 实际测试结果和预期的一致性。

7.4.4 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源，以用于安全功能的抽样测试。

7.5 脆弱性评定

基于已标识的潜在脆弱性，产品能够抵抗以下攻击行为：

a） 具有基本攻击潜力的攻击者的攻击；

b） 具有增强型基本攻击潜力的攻击者的攻击。

8 等级划分要求

8.1 概述

运维安全管理产品的安全功能要求和安全保障要求划分为基本级和增强级。

8.2 安全功能要求等级划分

运维安全管理产品的安全功能要求等级划分如表 1 所示。

表 1 运维安全管理产品安全功能要求等级划分

安全功能要求		基本级	增强级
单点登录		6.1	6.1
访问控制		6.2a)～6.2c)	6.2
操作审计	审计记录	6.3.1a)～6.3.1f)	6.3.1
	审计查阅	6.3.2a)～6.3.2d)	6.3.2
会话监视		—	6.4
会话回放		6.5a)	6.5
告警		6.6a)～6.6f)	6.6
违规操作阻断		6.7	6.7
高可用性		—	6.8
标识与鉴别	身份标识	6.9.1	6.9.1
	基本鉴别	6.9.2a)	6.9.2
	鉴别失败处理	—	6.9.3
	超时锁定或注销	6.9.4	6.9.4
安全管理	安全功能管理	6.10.1	6.10.1
	管理员角色	6.10.2a)	6.10.2
	远程管理加密	6.10.3	6.10.3
	远程管理主机	—	6.10.4
	鉴别数据保护	6.10.5	6.10.5

表 1（续）

安全功能要求		基本级	增强级
审计日志	审计日志生成	6.11.1a)～6.11.1c)	6.11.1
	审计日志存储	6.11.2a)	6.11.2
	审计日志管理	6.11.3a)、6.11.3b)	6.11.3

8.3 安全保障要求等级划分

运维安全管理产品的安全保障要求等级划分如表 2 所示。

表 2 运维安全管理产品安全保障要求等级划分

安全保障要求		基本级	增强级
开发	安全架构	7.1.1	7.1.1
	功能规范	7.1.2a)～7.1.2f)	7.1.2
	实现表示	—	7.1.3
	产品设计	7.1.4a)～7.1.4d)	7.1.4
指导性文档	操作用户指南	7.2.1	7.2.1
	准备程序	7.2.2	7.2.2
生命周期支持	配置管理能力	7.3.1a)～7.3.1c)	7.3.1
	配置管理范围	7.3.2a)	7.3.2
	交付程序	7.3.3	7.3.3
	开发安全	—	7.3.4
	生命周期定义	—	7.3.5
	工具和技术	—	7.3.6
测试	测试覆盖	7.4.1a)	7.4.1
	测试深度	—	7.4.2
	功能测试	7.4.3	7.4.3
	独立测试	7.4.4	7.4.4
脆弱性评定		7.5a)	7.5b)

中华人民共和国公共安全
行 业 标 准
信息安全技术 运维安全管理产品
安全技术要求
GA/T 1394—2017
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1 字数 22 千字
2017年11月第一版 2017年11月第一次印刷
*
书号:155066·2-31897 定价 18.00元

GA/T 1394-2017