ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1527—2018

信息安全技术　云计算安全综合防御产品安全技术要求

Information security technology—Security technical requirements for cloud computing security comprehensive defense products

2018-11-05 发布　　2018-11-05 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：宋好好、陈妍、邹春明、陆臻、沈亮、邱梓华、顾健。

信息安全技术　云计算安全综合防御产品安全技术要求

1　范围

本标准规定了云计算安全综合防御产品的安全功能要求、安全保障要求及等级划分要求。

本标准适用于云计算安全综合防御产品的设计、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

GB/T 31167—2014　信息安全技术　云计算服务安全指南

GB/T 31168—2014　信息安全技术　云计算服务安全能力要求

3　术语和定义

GB/T 25069—2010、GB/T 31167—2014 和 GB/T 31168—2014 界定的以及下列术语和定义适用于本文件。

3.1

云计算平台　cloud computing platform

由云服务商提供的云基础设施及其上的服务层软件的集合。

4　云计算安全综合防御产品描述

云计算安全综合防御产品是基于云计算平台构建的、可弹性扩展的、主要对云计算平台和云计算服务及上层业务应用进行综合安全防护的产品，具备防御来自云平台外部、虚拟机之间以及虚拟机对外部的恶意攻击的功能。该产品的安全能力主要体现在与云计算平台的联动及响应，以及各安全模块之间的联动及响应上，并且该产品的安全模块是可扩展的，至少包括抗拒绝攻击模块、虚拟机异常行为监测和识别模块、WEB 应用安全扫描模块、WEB 应用安全防护模块等。图 1 为云计算安全综合防御产品典型运行环境。