ICS 35.40
L 80

GA

中华人民共和国公共安全行业标准

GA/T 1390.2—2017

信息安全技术　网络安全等级保护基本要求　第2部分:云计算安全扩展要求

Information security technology—General requirements for classified protection of cyber security—Part 2:Special security requirements for cloud computing

2017-05-08 发布　　2017-05-08 实施

中华人民共和国公安部　　发 布

目　　次

前言 …… Ⅴ
引言 …… Ⅵ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　云计算安全概述 …… 2
4.1　云计算平台构成 …… 2
4.2　云计算平台定级 …… 3
5　第一级安全要求 …… 3
5.1　技术要求 …… 3
5.1.1　物理和环境安全 …… 3
5.1.2　网络和通信安全 …… 3
5.1.2.1　网络架构 …… 3
5.1.2.2　访问控制 …… 3
5.1.2.3　入侵防范 …… 4
5.1.2.4　安全审计 …… 4
5.1.3　设备和计算安全 …… 4
5.1.3.1　身份鉴别 …… 4
5.1.3.2　访问控制 …… 4
5.1.3.3　安全审计 …… 4
5.1.3.4　入侵防范 …… 4
5.1.3.5　资源控制 …… 4
5.1.3.6　镜像和快照保护 …… 4
5.1.4　应用和数据安全 …… 4
5.1.4.1　安全审计 …… 4
5.1.4.2　资源控制 …… 5
5.1.4.3　接口安全 …… 5
5.1.4.4　数据完整性 …… 5
5.1.4.5　数据保密性 …… 5
5.1.4.6　数据备份恢复 …… 5
5.1.4.7　剩余信息保护 …… 5
5.2　管理要求 …… 5
5.2.1　安全管理机构和人员 …… 5
5.2.1.1　授权 …… 5
5.2.1.2　人员录用 …… 5
5.2.2　安全建设管理 …… 5
5.2.2.1　测试验收 …… 5

5.2.2.2 云服务商选择 …… 5
5.2.2.3 供应链管理 …… 6
5.2.3 安全运维管理 …… 6
5.2.3.1 环境管理 …… 6
5.2.3.2 监控和审计管理 …… 6
6 第二级安全要求 …… 6
6.1 技术要求 …… 6
6.1.1 物理和环境安全 …… 6
6.1.2 网络和通信安全 …… 6
6.1.2.1 网络架构 …… 6
6.1.2.2 访问控制 …… 7
6.1.2.3 入侵防范 …… 7
6.1.2.4 安全审计 …… 7
6.1.3 设备和计算安全 …… 7
6.1.3.1 身份鉴别 …… 7
6.1.3.2 访问控制 …… 7
6.1.3.3 安全审计 …… 7
6.1.3.4 入侵防范 …… 7
6.1.3.5 资源控制 …… 7
6.1.3.6 镜像和快照保护 …… 7
6.1.4 应用和数据安全 …… 8
6.1.4.1 安全审计 …… 8
6.1.4.2 资源控制 …… 8
6.1.4.3 接口安全 …… 8
6.1.4.4 数据完整性 …… 8
6.1.4.5 数据保密性 …… 8
6.1.4.6 数据备份恢复 …… 8
6.1.4.7 剩余信息保护 …… 8
6.2 管理要求 …… 8
6.2.1 安全管理机构和人员 …… 8
6.2.1.1 授权 …… 8
6.2.1.2 人员录用 …… 8
6.2.2 安全建设管理 …… 9
6.2.2.1 测试验收 …… 9
6.2.2.2 云服务商选择 …… 9
6.2.2.3 供应链管理 …… 9
6.2.3 安全运维管理 …… 9
6.2.3.1 环境管理 …… 9
6.2.3.2 监控和审计管理 …… 9
7 第三级安全要求 …… 9
7.1 技术要求 …… 9
7.1.1 物理和环境安全 …… 9
7.1.2 网络和通信安全 …… 10

7.1.2.1 网络架构 …… 10
7.1.2.2 访问控制 …… 10
7.1.2.3 入侵防范 …… 10
7.1.2.4 安全审计 …… 10
7.1.3 设备和计算安全 …… 10
7.1.3.1 身份鉴别 …… 10
7.1.3.2 访问控制 …… 11
7.1.3.3 安全审计 …… 11
7.1.3.4 入侵防范 …… 11
7.1.3.5 恶意代码防范 …… 11
7.1.3.6 资源控制 …… 11
7.1.3.7 镜像和快照保护 …… 11
7.1.4 应用和数据安全 …… 11
7.1.4.1 安全审计 …… 11
7.1.4.2 资源控制 …… 12
7.1.4.3 接口安全 …… 12
7.1.4.4 数据完整性 …… 12
7.1.4.5 数据保密性 …… 12
7.1.4.6 数据备份恢复 …… 12
7.1.4.7 剩余信息保护 …… 12
7.2 管理要求 …… 12
7.2.1 安全管理机构和人员 …… 12
7.2.1.1 授权 …… 12
7.2.1.2 人员录用 …… 12
7.2.2 安全建设管理 …… 13
7.2.2.1 安全方案设计 …… 13
7.2.2.2 测试验收 …… 13
7.2.2.3 云服务商选择 …… 13
7.2.2.4 供应链管理 …… 13
7.2.3 安全运维管理 …… 13
7.2.3.1 环境管理 …… 13
7.2.3.2 配置管理 …… 13
7.2.3.3 监控和审计管理 …… 14
8 第四级安全要求 …… 14
8.1 技术要求 …… 14
8.1.1 物理和环境安全 …… 14
8.1.2 网络和通信安全 …… 14
8.1.2.1 网络架构 …… 14
8.1.2.2 访问控制 …… 14
8.1.2.3 入侵防范 …… 15
8.1.2.4 安全审计 …… 15
8.1.3 设备和计算安全 …… 15
8.1.3.1 身份鉴别 …… 15

8.1.3.2 访问控制 …… 15
8.1.3.3 安全审计 …… 15
8.1.3.4 入侵防范 …… 15
8.1.3.5 恶意代码防范 …… 15
8.1.3.6 资源控制 …… 16
8.1.3.7 镜像和快照保护 …… 16
8.1.4 应用和数据安全 …… 16
8.1.4.1 安全审计 …… 16
8.1.4.2 资源控制 …… 16
8.1.4.3 接口安全 …… 16
8.1.4.4 数据完整性 …… 16
8.1.4.5 数据保密性 …… 16
8.1.4.6 数据备份恢复 …… 17
8.1.4.7 剩余信息保护 …… 17
8.2 管理要求 …… 17
8.2.1 安全管理机构和人员 …… 17
8.2.1.1 授权 …… 17
8.2.1.2 人员录用 …… 17
8.2.2 安全建设管理 …… 17
8.2.2.1 安全方案设计 …… 17
8.2.2.2 测试验收 …… 17
8.2.2.3 云服务商选择 …… 17
8.2.2.4 供应链管理 …… 18
8.2.3 安全运维管理 …… 18
8.2.3.1 环境管理 …… 18
8.2.3.2 配置管理 …… 18
8.2.3.3 监控和审计管理 …… 18
附录 A（资料性附录） 云计算平台面临的安全威胁 …… 19
附录 B（规范性附录） 不同服务模式的安全管理责任主体 …… 21
附录 C（规范性附录） 本部分适用的对象 …… 24
参考文献 …… 25

前　言

GA/T 1390《信息安全技术　网络安全等级保护基本要求》已经或计划发布以下部分：

——第1部分：安全通用要求；

——第2部分：云计算安全扩展要求；

——第3部分：移动互联安全扩展要求；

——第4部分：物联网安全扩展要求；

——第5部分：工业控制安全扩展要求；

——第6部分：大数据安全扩展要求。

本部分为GA/T 1390的第2部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分由公安部网络安全保卫局提出。

本部分由公安部信息系统安全标准化技术委员会归口。

本部分起草单位：公安部信息安全等级保护评估中心、国家信息中心、阿里云计算有限公司、中科院信息工程研究所、杭州华三通信技术有限公司、华为技术有限公司、启明星辰信息技术有限公司。

本部分主要起草人：张振峰、丁朝晖、李明、任卫红、胡娟、申永波、苏艳芳、陈峰、李宇、刘静、章恒、陈雪秀、高亚楠、陈驰、于晶、姚国富、黄敏、段伟恒、郭春梅。

引　言

GB/T 22239—2008《信息安全技术　信息系统安全等级保护基本要求》在开展信息安全等级保护工作的过程中起到了非常重要的作用，被广泛应用于各个行业和领域开展信息安全等级保护的建设整改和等级测评等工作，但是随着信息技术的发展，GB/T 22239—2008 在时效性、易用性、可操作性上需要进一步提高。

为了适应移动互联、云计算、大数据、物联网和工业控制等新技术、新应用情况下信息安全等级保护工作的开展，需对 GB/T 22239—2008 进行修订，修订的思路和方法是针对移动互联、云计算、大数据、物联网和工业控制等新技术、新应用领域提出扩展的安全要求。

信息安全技术　网络安全等级保护基本要求　第2部分:云计算安全扩展要求

1　范围

GA/T 1390的本部分规定了不同安全保护等级云计算平台及云租户业务应用系统的安全保护要求。

本部分适用于指导分等级的非涉密云计算平台及云租户业务应用系统的安全建设和监督管理。

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 17859—1999　计算机信息系统安全保护等级划分准则

GB/T 22239　信息安全技术　信息系统安全等级保护基本要求

GB/T 22240　信息安全技术　信息系统安全等级保护定级指南

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 17859—1999、GB/T 25069—2010和GB/T 31168—2014界定的以及下列术语和定义适用于本文件。为了便于使用,以下重复列出GB/T 31168—2014中的部分术语和定义。

3.1

云计算　cloud computing

通过网络访问可扩展的、灵活的物理或虚拟共享资源池,并可按需自助获取和管理资源的模式。

[GB/T 31168—2014,定义3.1]

3.2

云计算基础设施　cloud computing infrastructure

由硬件资源和资源抽象控制组件构成的支撑云计算的基础设施。

注1:硬件资源包括所有的物理计算资源,包括服务器(CPU、内存等)、存储组件(硬盘等)、网络组件(路由器、防火墙、交换机、网络连接和接口等)及其他物理计算基础元素。资源抽象控制组件对物理计算资源进行软件抽象,云服务商通过这些组件提供和管理对物理计算资源的访问。

注2:改写GB/T 31168—2014,定义3.5。

3.3

云计算平台　cloud computing platform

云服务商提供的云计算基础设施及其上的服务软件的集合。

注:改写GB/T 31168—2014,定义3.6。