ICS 35 040
L80

中 华 人 民 共 和 国 国 家 标 准

GB/T 22239. 2—XXXX

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- Baseline for cybersecurity classified protection
Part 2: Security special requirements for cloud computing

点击此处添加与国际标准一致性程度的标识

（征求意见稿）

（本稿完成日期：2016-11-1）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前言 III
引言 IV
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　第二级安全要求 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
5.1.3　设备和计算安全 3
5.1.4　应用和数据安全 4
5.2　管理要求 5
5.2.1　安全管理机构和人员 5
5.2.2　系统安全建设管理 5
6　第三级安全要求 5
6.1　技术要求 5
6.1.1　物理和环境安全 5
6.1.2　网络和通信安全 5
6.1.3　设备和计算安全 6
6.1.4　应用和数据安全 7
6.2　管理要求 8
6.2.1　安全管理机构和人员 8
6.2.2　系统安全建设管理 9
6.2.3　系统安全运维管理 9
7　第四级安全要求 9
7.1　技术要求 9
7.1.1　物理和环境安全 10
7.1.2　网络和通信安全 10
7.1.3　设备和计算安全 11
7.1.4　应用和数据安全 12
7.2　管理要求 12

7.2.1 安全管理机构和人员 13
7.2.2 系统安全建设管理 13
7.2.3 系统安全运维管理 13
附录 A（资料性附录） 与 GB/T 22239.1 的关系 14
附录 B（资料性附录） 云计算平台面临的安全威胁 17
B.1 数据丢失、篡改或泄露 17
B.2 网络攻击 17
B.3 利用不安全接口的攻击 17
B.4 云服务中断 17
B.5 越权、滥用与误操作 17
B.6 滥用云服务 17
B.7 利用共享技术漏洞进行的攻击 17
B.8 过度依赖 18
B.9 数据残留 18
附录 C（资料性附录） 不同服务模式的安全管理责任主体 19
C.1 云服务的三种服务模式 19
C.2 不同服务模式下安全管理责任主体 19
附录 D（资料性附录） 本部分适用的对象 22
参考文献 23

图 1 云计算服务模式与控制范围的关系 3

表 A.1 GB/T 22239.2 与 GB/T 22239.1 关系表 14
表 C.1 IaaS 模式下云服务方与云租户的责任划分 19
表 C.2 PaaS 模式下云服务方与租户的责任划分 20
表 C.3 SaaS 模式下云服务方与租户的责任划分 21
表 D.1 云计算系统与传统信息系统保护对象差异 22

前　言

GB/T 22239《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GB/T 22239的第2部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分由全国信息安全标准化技术委员会提出。

本部分由全国信息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、张如辉。

引　言

国家标准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完善。

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。

本部分只对等级保护第二级到第四级云计算系统做出要求。

在本部分文本中，黑体字表示较低等级中没有出现或增强的要求。

本部分为GB/T 22239.1在云计算系统安全领域的扩展要求，对云计算系统应用GB/T 22239时应同时使用GB/T 22239.1和GB/T 22239.2的相关要求。

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

GB/T 22239的本部分规定了不同等级云计算系统的安全扩展要求。

本部分适用于指导分等级的非涉密云计算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，仅所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 22239.1 信息安全技术 网络安全等级保护基本要求 第1部分：安全通用要求

GB/T 22240—2008 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 22239.1、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。

3.1

云计算 cloud computing

一种通过网络提供计算资源的服务模式，在该模式下，云租户按需动态自助供给、管理各类计算资源。

3.2

网络策略控制器 network policy controller

在网络中，把网络配置信息转化为网络设备上的转发规则集，并对这些转发规则集进行管理的核心控制系统。

3.3

云计算平台 cloud computing platform

由云服务方提供的云计算基础设施及其上服务层软件的集合。（引自GB/T 31168—2014）

3.4

云服务方 cloud service provider
云服务的提供者，包括与云租户建立商业关系或没有商业关系的云服务提供者。

3.5

云租户 cloud tenant
租用或使用云计算资源的客户，包括计费的和不计费的云服务的机构和个人。

3.6

云服务 cloud service
由云服务方使用云计算提供的服务。（引自GB/T 31168—2014）

3.7

虚拟机监视器 hypervisor
一种运行在基础物理服务器和操作系统之间的中间软件层，可允许多个操作系统和应用共享硬件。

3.8

宿主机 host machine
运行虚拟机监视器的物理服务器。

4 云计算安全概述

4.1 云计算平台构成

本部分中将采用了云计算技术的信息系统，称为云计算平台。云计算平台由设施、硬件、资源抽象控制层、虚拟化计算资源、软件平台和应用软件等组成。软件即服务（SaaS）、平台即服务（PaaS）、基础设施即服务（IaaS）是三种基本的云计算服务模式。如图1所示，在不同的服务模式中，云服务方和云租户对计算资源拥有不同的控制范围，控制范围则决定了安全责任的边界。在基础设施即服务模式下，云计算平台由设施、硬件、资源抽象控制层组成；在平台即服务模式下，云计算平台包括设施、硬件、资源抽象控制层、虚拟化计算资源和软件平台；在软件即服务模式下，云计算平台包括设施、硬件、资源抽象控制层、虚拟化计算资源、软件平台和应用软件。

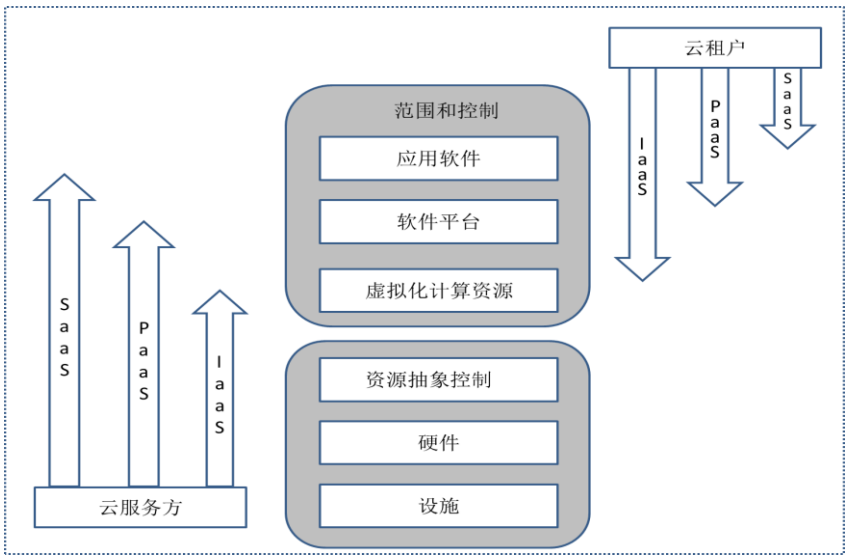

图1　云计算服务模式与控制范围的关系

4.2　云计算平台定级

在云计算环境中，应将云服务方侧的云计算平台单独作为定级对象定级，云租户侧的等级保护对象也应作为单独的定级对象定级。

对于大型云计算平台，应将云计算基础设施和有关辅助服务系统划分为不同的定级对象。

5　第二级安全要求

5.1　技术要求

5.1.1　物理和环境安全

物理和环境安全应符合以下要求：

a)　确保云计算服务器、承载云租户账户信息、鉴别信息、系统信息及运行关键业务和数据的物理设备均位于中国境内；

b)　IDC 应具有国家相关部门颁发的 IDC 运营资质。

5.1.2　网络和通信安全

5.1.2.1　网络架构

网络架构应符合以下要求：

a)　实现不同云租户之间网络资源的隔离，并避免网络资源的过量占用；

b)　绘制与当前运行情况相符的虚拟化网络拓扑结构图；

c)　保证虚拟机只能接收到目的地址包括自己地址的报文。

5.1.2.2　访问控制

访问控制应符合以下要求：

a)　避免虚拟机通过网络非授权访问宿主机；

b)　在虚拟化网络边界部署访问控制机制，并设置访问控制规则；

c)　保证当虚拟机迁移时，访问控制策略随其迁移；

d)　允许云租户设置不同虚拟机之间的访问控制策略。

5.1.2.3　远程访问

远程访问应符合以下要求：

a)　实时监视云计算平台的远程访问；

b)　对远程执行特权命令进行限制。

5.1.2.4　入侵防范

应能监测到云租户的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。

5.1.3　设备和计算安全

5.1.3.1　身份鉴别

应在网络策略控制器和网络设备（或设备代理）之间建立身份验证机制。

5.1.3.2 访问控制

当进行远程管理时，防止远程管理设备同时直接连接其他网络。

5.1.3.3 安全审计

安全审计应符合以下要求：

a) 根据云服务方和云租户的职责划分，收集各自控制部分的审计数据；
b) 保证云服务方对云租户系统和数据的操作可被云租户审计；
c) 保证审计数据的真实性和完整性。

5.1.3.4 入侵防范

入侵防范应能够检测以下内容：

a) 虚拟机对宿主机资源的异常访问；
b) 虚拟机之间的资源隔离失效，并进行告警。

5.1.3.5 资源控制

资源控制应符合以下要求：

a) 屏蔽虚拟资源故障，某个虚拟机崩溃后不影响虚拟机监视器及其他虚拟机；
b) 对物理资源和虚拟资源按照策略做统一管理调度与分配；
c) 保证虚拟机仅能使用为其分配的计算资源。

5.1.3.6 镜像和快照保护

镜像和快照保护应符合以下要求：

a) 提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；
b) 采取加密或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问；
c) 针对重要业务系统提供加固的操作系统镜像。

5.1.4 应用和数据安全

5.1.4.1 安全审计

安全审计应符合以下要求：

a) 根据云服务方和云租户的职责划分，收集各自控制部分的审计数据；
b) 保证云服务方对云租户系统和数据的操作可被云租户审计；
c) 保证审计数据的真实性和完整性。

5.1.4.2 资源控制

资源控制应符合以下要求：

a) 能够对应用系统的运行状况进行监测，并在发现异常时进行告警；
b) 保证不同云租户的应用系统及开发平台之间的隔离。

5.1.4.3 接口安全

应保证云计算服务对外接口的安全性。

5.1.4.4 数据完整性

应确保虚拟机迁移过程中，重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。

5.1.4.5 数据备份恢复

应提供查询云租户数据及备份存储位置的方式。

5.2 管理要求

5.2.1 安全管理机构和人员

应保证云服务方对云租户业务数据的访问或使用必须经过云租户的授权，授权必须保留相关记录。

5.2.2 系统安全建设管理

5.2.2.1 测试验收

应验证或评估所提供的安全措施的有效性。

5.2.2.2 云服务商选择

云服务商选择应符合以下要求：

a) 确保选择云服务商的过程符合国家有关规定；
b) 选择安全合规的云服务商，其所提供的云平台应具备与信息系统等级相应的安全保护能力；
c) 满足服务水平协议（SLA）要求；
d) 在服务水平协议（SLA）中规定云服务的各项服务内容和具体技术指标；
e) 在服务水平协议（SLA）中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；
f) 在服务水平协议（SLA）中规定云计算所能提供的安全服务的内容，并提供安全声明；
g) 在服务水平协议（SLA）中规定服务合约到期时，完整地返还云租户信息，并承诺相关信息均已在云计算平台上清除。

5.2.2.3 供应链管理

供应链管理应符合以下要求：

a) 确保选择供应商的过程符合国家的有关规定；
b) 确保供应链安全事件信息或威胁信息能够及时传达到云租户。

6 第三级安全要求

6.1 技术要求

6.1.1 物理和环境安全

物理和环境安全应符合以下要求：

a) 确保云计算服务器、承载云租户账户信息、鉴别信息、系统信息及运行关键业务和数据的物理设备均位于中国境内；
b) IDC 应具有国家相关部门颁发的 IDC 运营资质。

6.1.2 网络和通信安全

6.1.2.1 网络架构

网络架构应符合以下要求：

a) 实现不同云租户之间网络资源的隔离，并避免网络资源的过量占用；
b) 绘制与当前运行情况相符的虚拟化网络拓扑结构图，**并能对虚拟化网络资源、网络拓扑进行实时更新和集中监控**；
c) 保证虚拟机只能接收到目的地址包括自己地址的报文；
d) **保证云计算平台管理流量与云租户业务流量分离；**
e) **能识别、监控虚拟机之间、虚拟机与物理机之间、虚拟机与宿主机之间的流量；**
f) **根据承载的业务系统安全保护等级划分不同安全级别的资源池区域，并实现资源池之间的网络隔离；**
g) **提供开放接口或开放性安全服务，允许云租户接入第三方安全产品或在云平台选择第三方安全服务。加强云租户虚拟机之间、安全区域之间的网络安全防护能力；**
h) **根据云租户的业务需求定义安全访问路径。**

6.1.2.2 访问控制

访问控制应符合以下要求：

a) 避免虚拟机通过网络非授权访问宿主机；
b) 在虚拟化网络边界部署访问控制机制，并设置访问控制规则；
c) 保证当虚拟机迁移时，访问控制策略随其迁移；
d) 允许云租户设置不同虚拟机之间的访问控制策略；
e) **在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。**

6.1.2.3 远程访问

远程访问应符合以下要求：

a) 实时监视云计算平台的远程访问，**并在发现未授权连接时，采取恰当的应对措施**；
b) 对远程执行特权命令进行限制**并进行审计**；
c) **当进行远程管理时，管理终端和云计算平台边界设备之间应建立双向身份验证机制。**

6.1.2.4 入侵防范

入侵防范应符合以下要求：

a) 能监测到云租户的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；
b) **向云租户提供互联网发布内容监测功能，便于云租户对其发布内容中的有害信息进行实时监测和告警。**

6.1.2.5 安全审计

安全审计应符合以下要求：

a) **根据云服务方和云租户的职责划分，收集各自控制部分的审计数据；**
b) **为安全审计数据的汇集提供接口，并可供第三方审计；**
c) **根据云服务方和云租户的职责划分，实现各自控制部分的集中审计。**

6.1.3 设备和计算安全

6.1.3.1 身份鉴别

应在网络策略控制器和网络设备（或设备代理）之间建立**双向**身份验证机制。

6.1.3.2 访问控制

访问控制应符合以下要求：

a) 当进行远程管理时，防止远程管理设备同时直接连接其他网络；
b) **确保只有在云租户授权下，云服务方或第三方才具有云租户数据的管理权限；**
c) **提供云计算平台管理用户权限分离机制，为网络管理员、系统管理员建立不同账户并分配相应的权限。**

6.1.3.3 安全审计

安全审计应符合以下要求：

a) 根据云服务方和云租户的职责划分，收集各自控制部分的审计数据；
b) 保证云服务方对云租户系统和数据的操作可被云租户审计；
c) 保证审计数据的真实性和完整性；
d) **为安全审计数据的汇集提供接口，并可供第三方审计；**
e) **根据云服务方和云租户的职责划分，实现各自控制部分的集中审计。**

6.1.3.4 入侵防范

入侵防范应能够检测以下内容：

a) 虚拟机对宿主机资源的异常访问，**并进行告警**；
b) 虚拟机之间的资源隔离失效，并进行告警；
c) **非授权新建虚拟机或者重新启用虚拟机，并进行告警。**

6.1.3.5 恶意代码防范

应能够检测恶意代码感染及在虚拟机间蔓延的情况，并提出告警。

6.1.3.6 资源控制

资源控制应符合以下要求：

a) 屏蔽虚拟资源故障，某个虚拟机崩溃后不影响虚拟机监视器及其他虚拟机；
b) 对物理资源和虚拟资源按照策略做统一管理调度与分配；
c) 保证虚拟机仅能使用为其分配的计算资源；
d) **保证虚拟机仅能迁移至相同安全等级的资源池；**
e) **保证分配给虚拟机的内存空间仅供其独占访问；**
f) **对虚拟机的网络接口的带宽进行设置，并进行监控；**
g) **为监控信息的汇集提供接口，并实现集中监控。**

6.1.3.7 镜像和快照保护

镜像和快照保护应符合以下要求：

a) 提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；
b) 采取加密或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问；
c) 针对重要业务系统提供加固的操作系统镜像。

6.1.4 应用和数据安全

6.1.4.1 安全审计

安全审计应符合以下要求：

a) 根据云服务方和云租户的职责划分，收集各自控制部分的审计数据；
b) 保证云服务方对云租户系统和数据的操作可被云租户审计；
c) 保证审计数据的真实性和完整性；
d) **为安全审计数据的汇集提供接口，并可供第三方审计；**
e) **根据云服务方和云租户的职责划分，实现各自控制部分的集中审计。**

6.1.4.2 资源控制

资源控制应符合以下要求：

a) 能够对应用系统的运行状况进行监测，并在发现异常时进行告警；
b) 保证不同云租户的应用系统及开发平台之间的隔离。

6.1.4.3 接口安全

应保证云计算服务对外接口的安全性。

6.1.4.4 数据完整性

应确保虚拟机迁移过程中，重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。

6.1.4.5 数据保密性

数据保密性应符合以下要求：

a) **确保虚拟机迁移过程中，重要数据的保密性，防止在迁移过程中的重要数据泄露；**
b) **支持云租户部署密钥管理解决方案，确保云租户自行实现数据的加解密过程；**
c) **对网络策略控制器和网络设备（或设备代理）之间网络通信进行加密。**

6.1.4.6 数据备份恢复

a) **确保虚拟机迁移过程中，重要数据的保密性，防止在迁移过程中的重要数据泄露；**
b) **支持云租户部署密钥管理解决方案，确保云租户自行实现数据的加解密过程；**
c) **对网络策略控制器和网络设备（或设备代理）之间网络通信进行加密。**

6.1.4.7 数据备份恢复

数据备份恢复应符合以下要求：

a) **云租户应在本地保存其业务数据的备份；**
b) 提供查询云租户数据及备份存储位置的方式；
c) **保证不同云租户的审计数据隔离存放；**
d) **为云租户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。**

6.1.4.8 剩余信息保护

应保证虚拟机所使用的内存和存储空间回收时得到完全清除。

6.2 管理要求

6.2.1 安全管理机构和人员

应保证云服务方对云租户业务数据的访问或使用必须经过云租户的授权，授权必须保留相关记录。

6.2.2 系统安全建设管理

6.2.2.1 安全方案设计

云计算平台应提供开放接口或开放性安全服务，允许云租户接入第三方安全产品或在云平台选择第三方安全服务，支持异构方式对云租户的网络、主机、应用、数据层的安全措施进行实施。

6.2.2.2 测试验收

应验证或评估所提供的安全措施的有效性。

6.2.2.3 云服务商选择

云服务商选择应符合以下要求：

a) 确保选择云服务商的过程符合国家有关规定；
b) 选择安全合规的云服务商，其所提供的云平台应具备与信息系统等级相应的安全保护能力；
c) 满足服务水平协议（SLA）要求；
d) 在服务水平协议（SLA）中规定云服务的各项服务内容和具体技术指标；
e) 在服务水平协议（SLA）中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；
f) 在服务水平协议（SLA）中规定云计算所能提供的安全服务的内容，并提供安全声明；
g) 在服务水平协议（SLA）中规定服务合约到期时，完整地返还云租户信息，并承诺相关信息均已在云计算平台上清除；
h) **与选定的云服务商签署保密协议，要求其不得泄露云租户数据和业务系统的相关重要信息；**
i) **对可能接触到云租户数据的员工进行背景调查，并签署保密协议；**
j) **云服务商应接受云租户以外的第三方运行监管。**

6.2.2.4 供应链管理

供应链管理应符合以下要求：

a) 确保选择供应商的过程符合国家的有关规定；
b) 确保供应链安全事件信息或威胁信息能够及时传达到云租户；
c) **保证供应商的重要变更及时传达到云租户，并评估变更带来的安全风险，采取有关措施对风险进行控制。**

6.2.3 系统安全运维管理

监控和审计管理应符合以下要求：

a) **确保信息系统的监控活动符合关于隐私保护的相关政策法规；**
b) **确保提供给云租户的审计数据的真实性和完整性；**
c) **制定相关策略，对安全措施有效性进行持续监控；**
d) **云服务方应将安全措施有效性的监控结果定期提供给相关云租户。**

7 第四级安全要求

7.1 技术要求

7.1.1 物理和环境安全

物理和环境安全应符合以下要求：

a) 确保云计算服务器、承载云租户账户信息、鉴别信息、系统信息及运行关键业务和数据的物理设备均位于中国境内；
b) IDC 应具有国家相关部门颁发的 IDC 运营资质。

7.1.2 网络和通信安全

7.1.2.1 网络架构

网络架构应符合以下要求：

a) 实现不同云租户之间网络资源的隔离，并避免网络资源的过量占用；
b) 绘制与当前运行情况相符的虚拟化网络拓扑结构图，并能对虚拟化网络资源、网络拓扑进行实时更新和集中监控；
c) 保证虚拟机只能接收到目的地址包括自己地址的报文；
d) 保证云计算平台管理流量与云租户业务流量分离；
e) 能识别、监控虚拟机之间、虚拟机与物理机之间、虚拟机与宿主机之间的流量；
f) 根据承载的业务系统安全保护等级划分不同安全级别的资源池区域，并实现资源池之间的物理隔离；
g) 提供开放接口或开放性安全服务，允许云租户接入第三方安全产品或在云平台选择第三方安全服务。加强云租户虚拟机之间、安全区域之间的网络安全防护能力；
h) 根据云租户的业务需求定义安全访问路径；
i) **保证信息系统的外部通信接口经授权后方可传输数据。**

7.1.2.2 访问控制

访问控制应符合以下要求：

a) 避免虚拟机通过网络非授权访问宿主机；
b) 在虚拟化网络边界部署访问控制机制，并设置访问控制规则；
c) 保证当虚拟机迁移时，访问控制策略随其迁移；
d) 允许云租户设置不同虚拟机之间的访问控制策略；
e) 在不同等级的网络区域边界部署访问控制机制，设置访问控制规则；
f) **对进出网络的流量实施有效监控。**

7.1.2.3 入侵防范

入侵防范应符合以下要求：

a) 能监测到**并告警后及时处理**云租户的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；
b) 向云租户提供互联网发布内容监测功能，便于云租户对其发布内容中的有害信息进行实时监测**并告警后及时处理**。

7.1.2.4 安全审计

安全审计应符合以下要求：

a) 根据云服务方和云租户的职责划分，收集各自控制部分的审计数据；
b) 为安全审计数据的汇集提供接口，并可供第三方审计；

c） 根据云服务方和云租户的职责划分，实现各自控制部分的集中审计。

7.1.3 设备和计算安全

7.1.3.1 身份鉴别

应在网络策略控制器和网络设备（或设备代理）之间建立双向身份验证机制。

7.1.3.2 访问控制

访问控制应符合以下要求：

a） 当进行远程管理时，防止远程管理设备同时直接连接其他网络；
b） 确保只有在云租户授权下，云服务方或第三方才具有云租户数据的管理权限；
c） 提供云计算平台管理用户权限分离机制，为网络管理员、系统管理员建立不同账户并分配相应的权限。

7.1.3.3 安全审计

安全审计应符合以下要求：

a） 根据云服务方和云租户的职责划分，收集各自控制部分的审计数据；
b） 保证云服务方对云租户系统和数据的操作可被云租户审计；
c） 保证审计数据的真实性和完整性；
d） 为安全审计数据的汇集提供接口，并可供第三方审计；
e） 根据云服务方和云租户的职责划分，实现各自控制部分的集中审计。

7.1.3.4 入侵防范

入侵防范应能够检测以下内容：

a） 虚拟机对宿主机资源的异常访问，**并告警后及时处理**；
b） 虚拟机之间的资源隔离失效，**并告警后及时处理**；
c） 非授权新建虚拟机或者重新启用虚拟机的情况，**并告警后及时处理**。

7.1.3.5 恶意代码防范

应能够检测恶意代码感染及在虚拟机间蔓延的情况，**并告警后及时处理**。

7.1.3.6 资源控制

资源控制应符合以下要求：

a） 屏蔽虚拟资源故障，某个虚拟机崩溃后不影响虚拟机监视器及其他虚拟机；
b） 对物理资源和虚拟资源按照策略做统一管理调度与分配；
c） 保证虚拟机仅能使用为其分配的计算资源；
d） 保证虚拟机仅能迁移至相同安全等级的资源池；
e） 保证分配给虚拟机的内存空间仅供其独占访问；
f） 对虚拟机的网络接口的带宽进行设置，并进行监控；
g） 为监控信息的汇集提供接口，并实现集中监控。

7.1.3.7 镜像和快照保护

镜像和快照保护应符合以下要求：

a) 提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；
b) 采取加密或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问；
c) 针对重要业务系统提供加固的操作系统镜像。

7.1.4 应用和数据安全

7.1.4.1 安全审计

安全审计应符合以下要求：
a) 根据云服务方和云租户的职责划分，收集各自控制部分的审计数据；
b) 保证云服务方对云租户系统和数据的操作可被云租户审计；
c) 保证审计数据的真实性和完整性；
d) 为安全审计数据的汇集提供接口，并可供第三方审计；
e) 根据云服务方和云租户的职责划分，实现各自控制部分的集中审计。

7.1.4.2 资源控制

资源控制应符合以下要求：
a) 能够对应用系统的运行状况进行监测，并在发现异常时进行告警；
b) 保证不同云租户的应用系统及开发平台之间的隔离。

7.1.4.3 接口安全

应保证云计算服务对外接口的安全性。

7.1.4.4 数据完整性

应确保虚拟机迁移过程中，重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。

7.1.4.5 数据保密性

数据保密性应符合以下要求：
a) 确保虚拟机迁移过程中，重要数据的保密性，防止在迁移过程中的重要数据泄露；
b) 支持云租户部署密钥管理解决方案，确保云租户自行实现数据的加解密过程；
c) 对网络策略控制器和网络设备（或设备代理）之间网络通信进行加密。

7.1.4.6 数据备份恢复

数据备份恢复应符合以下要求：
a) 云租户应在本地保存其业务数据的备份；
b) 提供查询云租户数据及备份存储位置的方式；
c) 保证不同云租户的审计数据隔离存放；
d) 为云租户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。

7.1.4.7 剩余信息保护

应保证虚拟机所使用的内存和存储空间回收时得到完全清除。

7.2 管理要求

7.2.1 安全管理机构和人员

应保证云服务方对云租户业务数据访问或使用必须经过云租户的授权，授权必须保留相关记录。

7.2.2 系统安全建设管理

7.2.2.1 安全方案设计

云计算平台应提供开放接口或开放性安全服务，允许云租户接入第三方安全产品或在云平台选择第三方安全服务，支持异构方式对云租户的网络、主机、应用、数据层的安全措施进行实施。

7.2.2.2 测试验收

应验证或评估所提供的安全措施的有效性。

7.2.2.3 云服务商选择

应避免选择社会化的云服务。

7.2.2.4 供应链管理

供应链管理应符合以下要求：

a) 确保选择供应商的过程符合国家的有关规定；
b) 确保供应链安全事件信息或威胁信息能够及时传达到云租户；
c) 保证供应商的重要变更及时传达到云租户，并评估变更带来的安全风险，采取有关措施对风险进行控制。

7.2.3 系统安全运维管理

监控和审计管理应符合以下要求：

a) 确保信息系统的监控活动符合关于隐私保护的相关政策法规；
b) 确保提供给云租户的审计数据的真实性和完整性；
c) 制定相关策略，对安全措施有效性进行持续监控；
d) 云服务方应将安全措施有效性的监控结果定期提供给相关云租户。

附 录 A
（资料性附录）
与 GB/T 22239.1 的关系

采用云计算技术的信息系统首先应实现GB/T 22239.1《信息安全技术 网络安全等级保护基本要求 第1部分：安全通用要求》提出的对信息系统的通用安全要求，在此基础上进一步实现本部分提出的扩展安全要求。

本部分与GB/T 22239.1的关系如表A.1。

表A.1 GB/T 22239.2 与 GB/T 22239.1 关系表

类	子类	第一级	第二级	第三级	第四级
物理和环境安全	物理位置选择	/	扩展	扩展	扩展
	物理访问控制	继承	继承	继承	继承
	防盗窃和防破坏	继承	继承	继承	继承
	防雷击	继承	继承	继承	继承
	防火	继承	继承	继承	继承
	防水和防潮	继承	继承	继承	继承
	防静电	/	继承	继承	继承
	温湿度控制	继承	继承	继承	继承
	电力供应	继承	继承	继承	继承
	电磁防护	/	继承	继承	继承
网络和通信安全	网络架构	继承	扩展	扩展	扩展
	通信传输	继承	继承	继承	继承
	边界防护	继承	继承	继承	继承
	访问控制	继承	扩展	扩展	扩展
	入侵防范	/	扩展	扩展	扩展
	恶意代码防范	/	/	继承	继承
	安全审计	/	继承	扩展	扩展
	集中管控	/	/	继承	继承
设备和计算安全	身份鉴别	继承	扩展	扩展	扩展
	访问控制	继承	扩展	扩展	扩展
	安全审计	/	扩展	扩展	扩展

表A.1（续）

类	子类	第一级	第二级	第三级	第四级
	入侵防范	继承	扩展	扩展	扩展
	恶意代码防范	继承	继承	扩展	扩展
	资源控制	/	扩展	扩展	扩展
	镜像和快照保护	/	增加	增加	增加
应用和数据安全	身份鉴别	继承	继承	继承	继承
	访问控制	继承	继承	继承	继承
	安全审计	/	扩展	扩展	扩展
	软件容错	继承	继承	继承	继承
	资源控制	/	扩展	扩展	扩展
	接口安全	/	增加	增加	增加
	数据完整性	继承	扩展	扩展	扩展
	数据保密性	/	/	扩展	扩展
	数据备份恢复	继承	扩展	扩展	扩展
	剩余信息保护	/	继承	扩展	扩展
	个人信息保护	/	继承	继承	继承
安全策略和管理制度	安全策略	/	/	继承	继承
	管理制度	继承	继承	继承	继承
	制定和发布	继承	继承	继承	继承
	评审和修订	/	继承	继承	继承
安全管理机构和人员	岗位设置	继承	继承	继承	继承
	人员配备	继承	继承	继承	继承
	授权和审批	继承	扩展	扩展	扩展
	沟通和合作	/	继承	继承	继承
	审核和检查	/	继承	继承	继承
	人员录用	继承	继承	继承	继承
	人员离岗	继承	继承	继承	继承
	安全意识教育和培训	继承	继承	继承	继承
	外部人员访问管理	继承	继承	继承	继承
系统安全建设管理	系统定级和备案	继承	继承	继承	继承

表A.1（续）

类	子类	第一级	第二级	第三级	第四级
	安全方案设计	继承	继承	扩展	扩展
	产品采购和使用	继承	继承	继承	继承
	自行软件开发	/	继承	继承	继承
	外包软件开发	/	继承	继承	继承
	工程实施	继承	继承	继承	继承
	测试验收	继承	扩展	扩展	扩展
	系统交付	继承	继承	继承	继承
	等级测评	/	继承	继承	继承
	服务供应商选择	继承	继承	继承	继承
	云服务商选择	/	增加	增加	增加
	供应链管理	/	增加	增加	增加
系统安全运维管理	环境管理	继承	继承	继承	继承
	资产管理	/	继承	继承	继承
	介质管理	继承	继承	继承	继承
	设备维护管理	继承	继承	继承	继承
	漏洞和风险管理	继承	继承	继承	继承
	网络和系统安全管理	继承	继承	继承	继承
	恶意代码防范管理	继承	继承	继承	继承
	配置管理	/	继承	继承	继承
	密码管理	/	继承	继承	继承
	变更管理	/	继承	继承	继承
	备份与恢复管理	继承	继承	继承	继承
	安全事件处置	继承	继承	继承	继承
	应急预案管理	/	继承	继承	继承
	外包运维管理	/	继承	继承	继承
	监控和审计管理	/	/	增加	增加

注：“/”代表此级别的控制点没有要求项；“继承”代表此级别的控制点要求项完全继承 22239.1；“扩展”代表此级别的控制点要求项对于 22239.1 有扩展；“增加”代表此级别的控制点对于 22239.1 为新增控制点。

附 录 B
（资料性附录）
云计算平台面临的安全威胁

B.1 数据丢失、篡改或泄露

在云计算环境下，数据的实际存储位置往往不受云租户控制，云租户的数据可能存储在境外，易造成数据泄露。

云计算平台聚集了大量云租户的应用系统和数据资源，因而更容易成为被攻击的目标。一旦遭受攻击，会导致严重的数据丢失、篡改或泄露。

B.2 网络攻击

云计算基于网络提供服务，应用系统都放置于云端。一旦攻击者获取到用户的身份验证信息，假冒合法用户，那么用户的云中数据将面临被窃取、篡改等威胁。另外，DDoS攻击也是云计算环境最主要的安全威胁之一，攻击者通常是发起一些关键性操作来消耗大量的系统资源，如进程、内存、硬盘空间、网络带宽等，导致云服务反应变得极为缓慢或者完全没有响应。

B.3 利用不安全接口的攻击

攻击者利用非法获取的接口访问密钥，将能够直接访问用户数据，导致敏感数据泄露；通过接口实施注入攻击，可能篡改或者破坏用户数据；通过接口的漏洞，攻击者可绕过虚拟机监视器的安全控制机制，获取到系统管理权限，将给云租户带来无法估计的损失。

B.4 云服务中断

云服务基于网络提供服务，当云租户把应用系统迁移到云计算平台后，一旦与云计算平台的网络连接中断或者云计算平台出现故障，造成服务中断，将影响到云租户应用系统的正常运行。

B.5 越权、滥用与误操作

云租户的应用系统和业务数据处于云计算环境中，云计算平台的运营管理和运维管理归属于云服务方，运营管理和运维管理等人员的恶意破坏或误操作在一定程度上会造成云租户应用系统的运行中断和数据丢失、篡改或泄露。

B.6 滥用云服务

面向公众提供的云服务可向任何人提供计算资源，如果管控不严格，不考虑使用者的目的，很可能被攻击者利用，如通过租用计算资源发动拒绝服务攻击。

B.7 利用共享技术漏洞进行的攻击

由于云服务是多租户共享，如果云租户之间的隔离措施失效，一个云租户有可能侵入另一个云租户的环境，或者干扰其他云租户应用系统的运行。而且，很有可能出现专门从事攻击活动的人员绕过隔离措施，干扰、破坏其他云租户应用系统的正常运行。

B.8 过度依赖

由于缺乏统一的标准和接口，不同云计算平台上的云租户数据和应用系统难以相互迁移，同样也难以从云计算平台迁移回云租户的数据中心。另外，云服务方出于自身利益考虑，往往不愿意为云租户的数据和应用系统提供可移植能力。这种对特定云服务方的过度依赖可能导致云租户的应用系统随云服务方的干扰或停止服务而受到影响，也可能导致数据和应用系统迁移到其他云服务方的代价过高。

B.9 数据残留

云租户的大量数据存放在云计算平台上的存储空间中，如果存储空间回收后剩余信息没有完全清除，存储空间再分配给其他云租户使用容易造成数据泄露。

当云租户退出云服务时，由于云服务方没有完全删除云租户的数据，包括备份数据等，带来数据安全风险。

附 录 C
（资料性附录）
不同服务模式的安全管理责任主体

C.1 云服务的三种服务模式

云服务的服务模式包括基础设施即服务（IaaS）、平台即服务（PaaS）、软件即服务（SaaS），具体如下：

a) 基础设施即服务 Infrastructure As A Service(IaaS)。云服务方向云租户提供可动态申请或释放的计算资源、存储资源、网络资源等基础设施的服务模式；
b) 平台即服务 Platform As A Service(PaaS)。云服务方向云租户提供应用软件所需的支撑平台，包括用户应用程序的运行环境和开发环境,供云租户在此基础上开发和提供相关应用的服务模式；
c) 软件即服务 Software As A Service(SaaS)。云服务方向云租户提供运行在云基础设施之上的应用软件的服务模式。

C.2 不同服务模式下安全管理责任主体

不同服务模式下云服务方和云租户的安全管理责任主体有所不同，具体如表 C.1、C.2 和 C.3 所示：

表C.1 IaaS 模式下云服务方与云租户的责任划分

层面	安全要求	安全组件	责任主体
物理和环境安全	物理位置选择	数据中心及物理设施	云服务方
网络和通信安全	网络结构、访问控制、远程访问、入侵防范、安全审计	物理网络及附属设备、虚拟网络管理平台	云服务方
		云租户虚拟网络安全域	云租户
设备和计算安全	身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、资源控制、镜像和快照保护	物理网络及附属设备、虚拟网络管理平台、物理宿主机及附属设备、虚拟机管理平台、镜像等	云服务方
		云租户虚拟网络设备、虚拟安全设备、虚拟机等	云租户
应用和数据安全	安全审计、资源控制、接口安全、数据完整性、数据保密性、数据备份恢复	云管理平台（含运维和运营）、镜像、快照等	云服务方
		云租户应用系统及相关软件组件、云租户应用系统配置、云租户业务相关数据等	云租户

表C.1（续）

层面	安全要求	安全组件	责任主体
安全管理机构和人员	授权和审批	授权和审批流程、文档等	云服务方
系统安全建设管理	安全方案设计、测试验收、云服务商选择、供应链管理	云计算平台接口、安全措施、供应链管理流程、安全事件和重要变更信息	云服务方
		云服务商选择及管理流程	云租户
系统安全运维管理	监控和审计管理	监控和审计管理的相关流程、策略和数据	云服务方、云租户

表C.2　PaaS 模式下云服务方与租户的责任划分

层面	安全要求	安全组件	责任主体
物理和环境安全	物理位置选择	数据中心及物理设施	云服务方
网络和通信安全	网络结构、访问控制、远程访问、入侵防范、安全审计	物理网络及附属设备、虚拟网络管理平台、虚拟网络安全域	云服务方
设备和计算安全	身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、资源控制、镜像和快照保护	物理网络及附属设备、虚拟网络管理平台、物理宿主机及附属设备、虚拟机管理平台、镜像、虚拟机、虚拟网络设备、虚拟安全设备等	云服务方
应用和数据安全	安全审计、资源控制、接口安全、数据完整性、数据保密性、数据备份恢复	云管理平台（含运维和运营）、镜像、快照等	云服务方
		云租户应用系统及相关软件组件、云租户应用系统配置、云租户业务相关数据等	云租户
安全管理机构和人员	授权和审批	授权和审批流程、文档等	云服务方
系统安全建设管理	安全方案设计、测试验收、云服务商选择、供应链管理	云计算平台接口、安全措施、供应链管理流程、安全事件和重要变更信息	云服务方
		云服务商选择及管理流程	云租户
系统安全运维管理	监控和审计管理	监控和审计管理的相关流程、策略和数据	云服务方

表C.3 SaaS模式下云服务方与租户的责任划分

层面	安全要求	安全组件	责任主体
物理和环境安全	物理位置选择	数据中心及物理设施	云服务方
网络和通信安全	网络结构、访问控制、远程访问、入侵防范、安全审计	物理网络及附属设备、虚拟网络管理平台、虚拟网络安全域	云服务方
设备和计算安全	身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、资源控制、镜像和快照保护	物理网络及附属设备、虚拟网络管理平台、物理宿主机及附属设备、虚拟机管理平台、镜像、虚拟机、虚拟网络设备、虚拟安全设备等	云服务方
应用和数据安全	安全审计、资源控制、接口安全、数据完整性、数据保密性、数据备份恢复	云管理平台（含运维和运营）、镜像、快照等、应用系统及相关软件组件	云服务方
		云租户应用系统配置、云租户业务相关数据等	云租户
安全管理机构和人员	授权和审批	授权和审批流程、文档等	云服务方
系统安全建设管理	安全方案设计、测试验收、云服务商选择、供应链管理	云计算平台接口、安全措施、供应链管理流程、安全事件和重要变更信息	云服务方
		云服务商选择及管理流程	云租户
系统安全运维管理	监控和审计管理	监控和审计管理的相关流程、策略和数据	云服务方

附 录 D
（资料性附录）
本部分适用的对象

云计算系统的保护对象与传统信息系统的保护对象存在差异，具体如表D.1所示：

表D.1 云计算系统与传统信息系统保护对象差异

层面	云计算系统保护对象	传统信息系统保护对象
物理和环境安全	机房及基础设施	机房及基础设施
网络和通信安全	网络结构、网络设备、安全设备、虚拟化网络结构、虚拟网络设备、虚拟安全设备	传统的网络设备、传统的安全设备、传统的网络结构
设备和计算安全	网络设备、安全设备、虚拟网络设备、虚拟安全设备、物理机、宿主机、虚拟机、虚拟机监视器、云管理平台、数据库管理系统、终端	传统主机、数据库管理系统、终端
应用和数据安全	应用系统、云应用开发平台、中间件、云业务管理系统、配置文件、镜像文件、快照、业务数据、用户隐私、鉴别信息等	应用系统、中间件、配置文件、业务数据、用户隐私、鉴别信息等
系统安全建设管理	云计算平台接口、云服务商选择过程、SLA、供应链管理过程等	N/A

参 考 文 献

[1] MSTL_JGF_04—035 0101—2013 信息安全技术 云操作系统安全检验要求

[2] GB/T 19716—2005 信息技术 信息安全管理实用规则

[3] NIST Special Publication 800—53

[4] Cloud Security Alliance,Top Threats Working Group,“The notorious nine: cloud computing top threats in 2013”. February 2013

[5] Wayne Jansen, Timothy Grance. Guidelines on Security and Privacy in Public Cloud Computing[EB/OL]. National Institute of Standards and Technology.Special Publication 800.144, http://csrc.nist.gov/publications/nistpubs/800.144/SP800.144.pdf, 2011. 01

[6] Cloud Computing Information Assurance Framework