C S A 云 安 全 联 盟 标 准

CSA 0001.2—2016

云计算安全技术要求
第 2 部分：IaaS 安全技术要求

Cloud Computing Security Technology Requirements(CSTR)

Part 2:Security technology requirements of IaaS

V1.0

2016-10

2016 - 10 - 25 发布

CSA 云安全联盟大中华区发布

目　　次

前　言

CSA 0001-2016《云计算安全技术要求》分为四个部分：

—— 第1部分：总则；

—— 第2部分：IaaS安全技术要求；

—— 第3部分：PaaS安全技术要求；

—— 第4部分：SaaS安全技术要求；

本部分为CSA 0001-2016的第2部分。

本部分按照ISO/IEC 导则第2部分：国际标准的结构和编写规则起草。

本部分附录A的内容，是基于硬件的安全能力要求，超过当前业界的安全水平或业界没有成熟的解决方案，作为附录供参考。

本标准主要起草单位：华为技术有限公司、阿里云计算有限公司、腾讯云计算（北京）有限责任公司、中兴通讯股份有限公司、北京百度网讯科技有限公司、杭州安恒信息技术有限公司、北京神州绿盟信息安全科技股份有限公司、蓝盾信息安全技术股份有限公司、浪潮（北京）电子信息产业有限公司、金蝶国际软件集团有限公司、顺丰科技有限公司、西安四叶草信息技术有限公司、深圳华泰思安信息技术有限公司、北京江南天安科技有限公司、大唐高鸿信安（浙江）信息科技有限公司、上海优刻得信息科技有限公司、上讯信息技术股份有限公司、深圳云塔信息技术有限公司、上海有云信息技术有限公司、英特尔亚太研发有限公司、广州赛宝认证中心服务有限公司、中国科学院信息工程研究所（信息安全国家重点实验室）、武汉大学、中国移动研究院、公安部第三研究所、深圳市标准技术研究院。

本标准主要起草人：叶思海、李雨航、张喆、陈雪秀、郑云文、周苏静、郝轶、周俊、刘文懋、梁宁波、李卓、黄远辉、胡泽柱、朱利军、杨炳年、李国、郑驰、杨丹、李建民、周景川、江均勇、李彦、刘小茵、蔡一兵、陈驰、马红霞、严飞、樊佩茹、王鹃、任兰芳、陈妍、杜佳、潘瑶。

引　　言

本标准以公有云部署模型为主要应用场景，同时考虑了私有云、社区会、混合云等部署模型。因此，本标准适用于公有云、私有云、社区会、混合云等部署模型的应用场景。

本标准将安全技术要求分为基础要求和增强要求。基础要求指应该实现的基本要求，不实现可能给系统带来较大的安全风险或合规风险；增强要求指在基础要求上的补充和强化，可有效提升防护水平。

在具体的应用场景下，云服务开发者在满足安全要求的前提下，可根据具体场景对这些安全技术要求进行调整。调整的方式有：

— 删减：某项安全要求只有部分适用，对不适用部分进行删减。

— 补充：某项安全要求不足以满足特定的安全目标，故增加新的安全要求，或对标准中规定的某项安全要求进行强化。

— 替代：使用其他安全要求替代标准中规定的某项安全要求，以实现相同的安全能力。

— 不适用：某项安全要求不适用实际应用的场景。

云计算安全技术要求

--IaaS安全技术要求

1 范围

本部分描述了IaaS服务提供者采用的的云计算产品与解决方案应具备的安全技术能力。

本部分适用于IaaS云服务开发者在设计开发IaaS产品和解决方案时使用，也可供IaaS服务商选择IaaS产品与解决方案时参考，还可为云服务客户选择IaaS服务时作为判断IaaS服务提供商提供的安全能力是否满足自身业务安全需求提供参考。

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。然而，鼓励根据本部分达成协议的各方研究是否可适用这些文件的最新版本。凡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。

CSA Cloud Computing Security Technology Requirements(CSTR) Part1: General

ISO/IEC 17788-2014 Information technology -- Cloud computing -- Overview and vocabulary

ISO/IEC 17789-2014 Information technology -- Cloud computing -- Reference architecture

ISO 27017 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

CSA (Cloud Security Alliance) Security Guidance for Critical Areas of Focus in Cloud Computing

The Cloud Security Alliance Cloud Controls Matrix (CCM)

3 术语和定义

《云计算安全技术要求 第1部分：总则》界定的术语和定义适用于本文件。

4 IaaS 云服务安全技术要求框架

根据云计算安全技术要求框架，IaaS 云服务安全技术要求框架如图 1 所示。

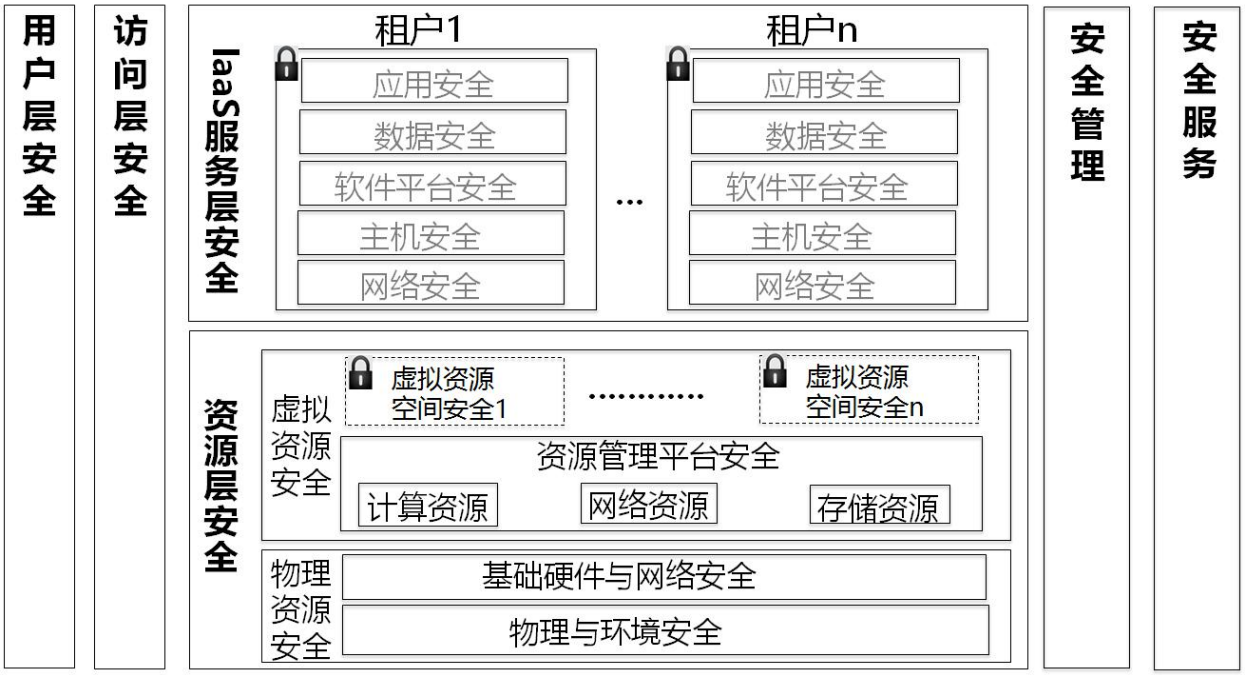

图 1 IaaS 云服务安全技术要求框架

4.1 用户层安全

用户层安全请参考《云计算安全技术要求 第 1 部分:总则》5.2.1 描述。

4.2 访问层安全

访问层安全请参考《云计算安全技术要求 第 1 部分:总则》5.2.2 描述。

4.3 资源层安全

资源层安全请参考《云计算安全技术要求 第 1 部分:总则》5.2.3 描述。

4.4 服务层安全

在 IaaS 服务类别，租户从 IaaS 云服务商获取计算、存储、网络资源，由云计算资源管理平台提供一个安全的虚拟资源空间，并把该空间的控制权交给租户。根据云计算安全责任模型，在租户虚拟资源私有空间内的安全由租户负责，IaaS 租户虚拟资源空间内的安全技术要求不在本标准范围之内，图 1 中呈现为灰色背景。

4.5 安全管理

安全管理请参考《云计算安全技术要求 第 1 部分:总则》5.2.5 描述。

4.6 安全服务

安全服务请参考《云计算安全技术要求 第 1 部分:总则》5.2.6 描述。

5 访问层安全

5.1 网络访问安全

5.1.1 基础要求

云计算平台应符合的基础要求如下：

a) 应支持保护用户访问云计算中的资源时通信消息的完整性和机密性的能力；

b) 应支持用户访问云计算中的资源前通过用户鉴别和鉴权的能力；

5.1.2 增强要求

无。

5.2 API 访问安全

5.2.1 基础要求

云计算平台应符合的基础要求如下：

a) 应支持服务 API 调用前进行用户鉴别和鉴权的能力；

b) 应支持涉及租户资源操作的服务 API 调用前验证租户凭证的能力；

c) 应支持用户调用服务 API 的访问控制能力；

d) 应支持服务 API 接口的防范重放、代码注入、DoS/DDoS 等攻击的能力；

e) 应支持服务 API 接口安全传输能力；

f) 应支持服务 API 接口过载保护能力，要求实现不同服务等级用户间业务的公平性和系统整体处理能力的最大化；

g) 应支持服务 API 的调用日志记录能力。

5.2.2 增强要求

无。

5.3 Web 访问安全

5.3.1 基础要求

云计算平台应符合的基础要求如下：

a) 应支持Web代码安全机制的能力，包括对输入输出进行有效性检查，以及采取防范认证漏洞、权限漏洞、会话漏洞、Web服务漏洞、注入漏洞等代码漏洞的措施；

b) 应支持对用户通过Web访问资源进行访问控制的能力；

c) 应支持Web远程访问安全传输的能力。

5.3.2 增强要求

无。

6 资源层安全

6.1 物理资源安全

6.1.1 物理与环境安全

参考业界最佳实践，不在本标准范围之内。

6.1.2 基础硬件安全

6.1.2.1 基础要求

云计算平台应符合的基础要求如下：

a) 应支持物理主机外设管理的能力；

b) 应支持硬件部分损坏情况下数据恢复的能力。

6.1.2.2 增强要求

云计算平台应符合的增强要求如下：

a) 应支持检测服务器或存储设备硬件发生变更并予以提示的能力。

6.1.3 网络安全

6.1.3.1 网络架构安全

6.1.3.1.1 基础要求

云计算平台应符合的基础要求如下：

a) 应支持绘制与当前运行情况相符的网络拓扑结构图，支持对网络拓扑进行实时更新和集中监控的能力；

b) 应支持划分为不同的网络区域，并且不同区域之间实现逻辑隔离的能力；

c) 应支持云计算平台管理网络与业务网络逻辑隔离的能力；

d) 应支持云计算平台业务网络和管理网络与租户私有网络逻辑隔离的能力；

e) 应支持云计算平台业务网络和管理网络与租户业务承载网络逻辑隔离的能力；

f) 应支持租户业务承载网络与租户私有网络逻辑隔离的能力；

g) 应支持网络设备（包括虚拟化网络设备）和安全设备业务处理能力弹性扩展能力；

h) 应支持高可用性部署，在一个区域出现故障（包括自然灾害和系统故障）时，自动将业务转离受影响区域的能力。

6.1.3.1.2 增强要求

云计算平台应符合的增强要求如下：

a) 应支持指定带宽分配优先级别的能力；

b) 应支持虚拟化网络边界的访问控制；

c) 应支持区域边界的双向访问控制，控制从内往外和从外往内流量的能力。

6.1.3.2 网络边界安全

6.1.3.2.1 基础要求

云计算平台应符合的基础要求如下：

a) 应支持对进出云计算平台业务网络和管理网络的信息进行过滤的能力；

b) 应支持对云计算平台管理网络最大流量及单用户网络连接数的限制能力；

c) 应支持对云计算平台管理员访问管理网络的访问控制能力；

d) 应支持对云计算平台业务网络和管理网络的非法连接检测及阻断能力；

注：非法连接包括从外部网络非法连接到内部网络，以及从内部网络非法连接到外部网络两种情况；

e) 应支持对网络边界管理设备受控接口ACL策略支持自动化更新能力；

f) 应支持对恶意虚拟机的隔离能力，支持阻断恶意虚拟机与外部网络以及和其他虚拟机的通信能力；

g) 应支持对云计算平台 DDoS 攻击防护的能力；

h) 应支持对 Web 应用漏洞进行检测和防护的能力；

i) 应支持网络边界流量监控、攻击和入侵行为检测的能力；

j) 应支持对恶意代码进行检测和处置的能力；

k) 应支持在不同安全等级的区域之间通信时采用安全传输的能力。

6.1.3.2.2 增强要求

云计算平台应符合的增强要求如下：

a) 应支持接入第三方安全产品或服务进行不同网络区域之间、租户网络之间的网络安全防护能力；

b) 应支持对云计算平台内部虚拟机发起的攻击检测与防护能力，检测出发起攻击的虚拟机，并能记录攻击类型、攻击时间、攻击流量等。

注：内部虚拟机发起的攻击，包括对云计算平台业务网络、管理网络、租户业务承载网络、其他租户私有网络、外部网络等发起的攻击。

6.1.3.3 网络授权及审计

6.1.3.3.1 基础要求

云计算平台应符合的基础要求如下：

a) 应支持对网络设备（包括虚拟化网络设备）的管理员登录地址进行限制的能力；
b) 应支持登录网络设备（包括虚拟化网络设备）失败处理的能力；
c) 应支持网络设备（包括虚拟化网络设备）管理员登录采用两种或两种以上组合的鉴别技术来进行身份鉴别能力；
d) 应支持对网络设备（包括虚拟化网络设备）远程管理时采用安全传输能力；
e) 应支持对网络设备（包括虚拟化网络设备）远程管理时特权命令进行限制的能力；
f) 应支持对网络设备（包括虚拟化网络设备）管理员权限最小化的能力；
g) 应支持对网络设备（包括虚拟化网络设备）管理员登录时用户标识唯一能力；
h) 应支持区域边界处的网络设备（包括虚拟化网络设备）和安全设备的日志记录、审计报表能力。

6.1.3.3.2 增强要求

无。

6.2 虚拟资源安全

6.2.1 资源管理平台安全

6.2.1.1 计算资源管理平台安全

6.2.1.1.1 基础要求

计算资源管理平台应符合的基础要求如下：

a) 应支持对代码进行安全测试并进行缺陷修复的能力；
b) 应支持限制虚拟机对物理资源的直接访问，支持对物理资源层的调度和管理均受虚拟机监视器控制的能力；
c) 应支持对计算资源管理平台的攻击行为进行监测和告警的能力，检测到攻击行为时，应能够记录攻击的源IP、攻击的类型、攻击的目的、攻击的时间；
d) 应支持最小安装的原则，仅安装必要的组件和应用程序的能力；
e) 应支持禁用无需使用的硬件能力；
f) 应支持虚拟机和虚拟化平台间内部通信通道的受限使用能力;
g) 应支持组件间通信采用安全传输的能力；
h) 应支持管理命令采用安全传输的能力；
i) 应支持内核补丁更新、加固及防止内核提权的能力；
j) 应支持对恶意代码进行检测和处置的能力；
k) 应支持监视计算资源管理平台远程管理连接，中断未授权管理连接的能力；
l) 应支持对远程执行计算资源管理平台特权管理命令进行限制的能力；
m) 应支持资源监控的能力，资源监控的内容包括 CPU 利用率、带宽使用情况、内存利用率、存储使用情况等；
n) 应支持系统过载保护，保障业务公平性和系统资源利用率最大化的能力；
o) 应支持禁止计算资源管理平台管理员未授权操作租户资源的能力；

注：租户资源包括已分配给租户的网络、数据库、存储空间、租户虚拟机以及租户虚拟机上的

OS、应用程序等。

p) 应支持计算资源管理平台镜像文件完整性保护的能力；

q) 应支持第三方安全产品或服务接入的API接口能力。

6.2.1.1.2 增强要求

计算资源管理平台应符合的增强要求如下：

a) 应支持对核心软件源代码进行审查并识别后门的能力；

b) 应支持重要程序安全启动的能力；

注：安全启动的软件应该是与预期软件版本一致，没有被篡改。

c) 应支持对重要配置文件完整性检测的能力；

d) 应支持软件白名单的能力；

e) 应支持对非授权组件或设备（包括软件、硬件和固件）的检测，检测到非授权的组件或设备时应支持禁止其网络访问或对其进行隔离或告警的能力；

f) 应支持对重要程序运行状态下完整性保护的能力；

g) 应支持虚拟机启动过程的完整性保护的能力；

h) 应支持虚拟机运行过程的完整性保护的能力。

6.2.1.2 存储资源管理平台安全

6.2.1.2.1 基础要求

存储资源管理平台应符合的基础要求如下：

a) 应支持对代码进行安全测试并进行缺陷修复的能力；

b) 应支持对攻击行为进行监测和告警的能力，检测到攻击行为时，能够记录攻击的源IP、攻击的类型、攻击的目的、攻击的时间；

c) 应支持组件间通信采用安全传输的能力；

d) 应支持管理命令采用安全传输的能力；

e) 应支持内核补丁更新、加固及防止内核提权的能力；

f) 应支持对恶意代码进行检测和处置的能力；

g) 应支持监视存储资源管理平台远程管理连接，发现未授权管理连接时中断连接的能力；

h) 应支持对远程执行存储资源管理平台特权管理命令进行限制的能力；

i) 应支持资源监控的能力，资源监控的内容包括 CPU 利用率、带宽使用情况、内存利用率、存储使用情况等；

j) 应支持系统过载保护，保障业务公平性和系统资源利用率最大化的能力；

k) 应支持禁止平台管理员未授权操作租户资源的能力；

l) 应支持数据存储机密性保护的能力；

m) 应支持数据存储完整性保护的能力；

n) 应支持数据存储可用性保护的能力；

o) 应支持数据的异地备份和备份数据一致性的能力；

p) 应支持租户访问存储的安全传输的能力。

6.2.1.2.2 增强要求

存储资源管理平台应符合的增强要求如下：

a) 应支持对核心软件源代码进行审查并识别后门的能力；

b) 应支持对重要程序安全启动的能力；

注：安全启动的软件应该是与预期软件版本一致，没有被篡改的。

c) 应支持对重要配置文件完整性检测的能力；

d) 应支持对非授权组件或设备（包括软件、硬件和固件）的检测，检测到非授权的组件或设备时应支持禁止其网络访问或对其进行隔离或告警的能力。

e) 应支持软件白名单的能力；
f) 应支持对用户上传的数据进行加密的能力；
g) 应支持对用户的密钥管理的能力；
h) 应支持对用户的密钥由租户自管理或第三方管理的能力；
i) 应支持数据多副本存储的能力，支持不同副本数据至少分布存储在两个机架上；
j) 应支持异地备份的能力，支持自动跨集群的数据同步能力；
k) 应支持存储层面的跨数据中心的同步或异步复制的能力。

6.2.2 虚拟资源空间安全

6.2.2.1 虚拟化计算安全

6.2.2.1.1 基础要求

云计算平台应符合的基础要求如下：

a) 应支持在虚拟机之间以及虚拟机与宿主机之间 CPU 安全隔离的能力，包括如下要求；
   1) 在某个虚拟机发生异常（包括崩溃）后不影响其他虚拟机和宿主机；
   2) 虚拟机不能访问其他虚拟机或宿主机的CPU寄存器信息。
b) 应支持在虚拟机之间以及虚拟机与宿主机之间内存安全隔离的能力，包括如下要求；
   1) 分配给虚拟机的内存空间，其他虚拟机和宿主机不能访问；
   2) 防止虚拟机占用过多内存资源，超过设定的规格，影响其他虚拟机正常运行；
   3) 某个虚拟机发生异常（包括崩溃）后不影响其他虚拟机和宿主机；
   4) 能够禁止虚拟机和其他虚拟机、宿主机之间拷贝或粘贴动作，如通过剪贴板的共享和复制。
c) 应支持在虚拟机之间以及虚拟机与宿主机之间存储空间安全隔离的能力，包括如下要求；
   1) 分配给虚拟机的存储空间，其他虚拟机和宿主机不能访问；
   2) 防止虚拟机占用过多存储资源，超过设定规格，影响其他虚拟机正常运行；
   3) 某个虚拟机发生异常（包括崩溃）后不影响其他虚拟机和宿主机。
d) 应支持一个虚拟机逻辑卷同一时刻只能被一个虚拟机挂载的能力；
e) 应支持根据租户所选择的服务级别进行虚拟机存储位置分配的能力；
f) 应支持实时的虚拟机监控，对虚拟机的运行状态、资源占用、迁移等信息进行监控和告警的能力。

6.2.2.1.2 增强要求

云计算平台应符合的增强要求如下：

a) 应支持对虚拟机所在物理机范围进行指定或限定的能力。

6.2.2.2 虚拟化网络安全

6.2.2.2.1 基础要求

云计算平台应符合的基础要求如下：

a) 应支持不同租户的虚拟化网络之间安全隔离的能力；
b) 应支持租户的虚拟化网络与云计算平台的业务和管理网络之间安全隔离的能力，包括如下要求；
   1) 云计算平台管理员，无法通过云计算平台的业务和管理网络访问租户私有网络；
   2) 租户无法通过私有网络访问云计算平台的业务和管理网络；
   3) 租户无法通过私有网络访问宿主机。
c) 应支持虚拟私有云 VPC 的能力，包括如下要求；
   1) 租户完全控制 VPC 虚拟网络，包括能够选择自有 IP 地址范围、创建子网，以及配置路由表和网关；
   2) 租户可以在自己定义的 VPC 虚拟网络中启动云服务的资源，如虚拟机实例；

3) 对 VPC 的操作，如创建或删除 VPC，变更路由、安全组和 ACL 策略等，需要验证租户凭证。

d) 应支持 VPC 之间连接的能力，包括同一个租户的不同 VPC 之间和不同租户 VPC 之间的连接能力；

e) 应支持安全组，提供虚拟化网络安全隔离和控制的能力，包括如下要求；

1) 可以过滤虚拟机实例出入口的流量，控制的规则可以由租户自定义；

2) 支持根据 IP 协议、服务端口及 IP 地址进行限制的能力。

f) 应支持网络访问控制列表 ACL，提供虚拟化网络安全隔离和控制的能力，要求基于 IP 协议、服务端口和源或目的 IP 地址，允许或拒绝流量；

g) 应支持虚拟私有网关，提供 VPC 与其他网络建立 VPN 私有连接的能力；

h) 应支持互联网网关，提供 NAT 功能，支持 VPC 与互联网连接的能力；

i) 应支持租户虚拟化网络关闭混杂模式的能力；

j) 应支持防止虚拟机使用虚假的 IP 或 MAC 地址对外发起攻击的能力；

k) 应支持防虚拟机 VLAN 或 VXLAN 跳跃攻击的能力；

l) 应支持不同租户的虚拟机之间以及虚拟机与宿主机之间网络流量监控的能力；

m) 应支持租户对其所拥有的不同虚拟机之间网络流量进行监控的能力。

6.2.2.2.2 增强要求

无。

6.2.2.3 虚拟化存储安全

6.2.2.3.1 基础要求

云计算平台应符合的基础要求如下：

a) 应支持租户设置虚拟化存储数据的访问控制策略的能力；

b) 应支持租户本地数据与虚拟化存储之间的安全上传和下载的能力；

c) 应支持租户间的虚拟化存储空间安全隔离，其他租户或者云计算平台管理员非授权不能访问的能力；

d) 应支持根据租户所选择的服务级别进行存储位置分配的能力。

6.2.2.3.2 增强要求

无。

6.2.2.4 迁移安全

6.2.2.4.1 基础要求

云计算平台应符合的基础要求如下：

a) 应支持虚拟机的安全策略随虚拟机的迁移而迁移的能力；

b) 应支持虚拟机迁移机密性保护的能力；

c) 应支持虚拟机迁移完整性保护的能力。

6.2.2.4.2 增强要求

无。

6.2.2.5 虚拟化组件安全加固

6.2.2.5.1 基础要求

云计算平台应符合的基础要求如下：

a) 应支持租户对云计算平台提供的镜像文件模板加固的能力；

b) 应支持租户镜像文件访问控制，其他租户或者云计算平台管理员非授权不能访问的能力；

c) 应支持租户快照文件访问控制能力，其他租户或者云计算平台管理员非授权不能访问的能力；

d) 应支持租户虚拟机镜像文件完整性保护的能力；

e) 应支持租户快照文件完整性保护的能力。

6.2.2.5.2 增强要求

云计算平台应符合的增强要求如下：

a) 应支持镜像文件的安全传输的能力；

b) 应支持租户虚拟机镜像文件加密的能力。

6.2.2.6 剩余数据保护

6.2.2.6.1 基础要求

云计算平台应符合的基础要求如下：

a) 应支持虚拟机所使用的内存回收时完全清除的能力；
注：完全清除指采用非物理手段无法恢复。

b) 应支持虚拟机所使用的存储空间回收时完全清除的能力；

c) 应支持租户虚拟机删除时，租户数据完全清除的能力；
租户虚拟机删除时，需要清除的数据包括租户镜像文件、快照文件、备份等数据；

d) 应支持租户虚拟化存储数据完全清除的能力；
虚拟化存储数据完全清除，包括虚拟化存储空间上的数据，备份的数据，也包括在租户完成本地数据与虚拟化存储之间安全上传、下载数据后存储网关等辅助设备上的数据等。

e) 应支持租户备份存储空间释放时，对应存储空间上租户数据完全清除的能力；

f) 应支持虚拟机迁移时原存储空间数据完全清除的能力。

6.2.2.1.2 增强要求

无。

7 服务层安全

根据云计算安全责任模型，在租户虚拟资源私有空间内的安全由租户负责，IaaS 租户虚拟资源私有空间内的安全定义技术要求不在本标准范围之内。

8 安全管理

8.1 身份鉴别和访问管理

8.1.1 基础要求

云计算平台应符合的基础要求如下：

a) 应支持租户身份和访问管理，实现集中管理租户账户（主账户）以及主账户下的个人用户（子账户）的能力，对子账户的管理，应满足如下要求；
1) 主账户可以创建多个子账户，并管理每个子账户的权限；
2) 支持主账户对子账户的分组授权，如基于角色、用户组授权。
注：个人用户可以是通过程序、管理控制台、 CLI 或 API 接口与云服务资源互动的任何个人、系统或应用。

b) 应支持租户账户下的子账户权限最小化配置的能力；

c) 应支持租户密码策略管理的能力，密码策略管理包括如下要求；
1) 应支持密码复杂度策略；
2) 应支持设置密码有效期；
3) 租户账号的初始密码应支持随机生成，租户首次登录支持强制修改初始密码。

d) 应支持为租户随机生成虚拟机的登录口令，或租户自行输入登录口令的能力；

e) 应支持在以密钥对方式登录租户虚拟机的场景下，租户自主选择由云计算平台生成密钥对或租

户上传密钥对的能力；

f) 应支持集中管理租户鉴别凭证的能力；

g) 应支持租户鉴别凭证的机密性和完整性保护的能力；

h) 应支持修改租户鉴别凭证前验证租户身份的能力；

i) 应支持租户账户异常检测并通知租户的能力；

j) 应支持多种租户身份鉴别方式的能力；

k) 应支持租户自主选择主账号采用两种或两种以上的组合机制进行身份鉴别的能力；

l) 应支持与租户自建身份认证中心对接的能力；

m) 应支持将云计算平台管理员的角色及其相应权限分配给不同账户的能力；

n) 应支持云计算平台管理员用户首次登录时强制修改初始密码的能力；

o) 应支持云计算平台管理员权限分离机制的能力；

p) 应支持云计算平台管理员权限最小化的能力；

q) 应支持多种云计算平台管理员身份鉴别方式的能力；

r) 应支持云计算平台管理员采用两种或两种以上的组合机制进行身份鉴别的能力。

8.1.2 增强要求

云计算平台应符合的增强要求如下：

a) 应支持云计算平台管理员特权账号管理的能力，特权账号管理包括如下要求：

1) 特权账号在授权时间内才能使用，授权时间支持分钟或小时的粒度；

2) 给特权账号授权的账号自身无法使用特权账号的业务操作权限。

b) 应支持用户身份证书状态有效性验证的能力；

a) 应支持租户授予原本无权访问租户资源的用户或实体临时访问租户资源的能力。

8.2 安全审计

8.2.1 基础要求

云计算平台应符合的基础要求如下：

a) 应支持审计记录信息产生的能力，审计记录信息的产生包括如下要求：

1) 记录云计算平台管理员和租户登录信息和身份鉴别信息；

2) 记录云计算平台管理员对基础设施和虚拟资源的管理操作信息，如架构调整、策略变更、安全功能的开启关闭、虚拟资源申请、虚拟机迁移、虚拟资源调度、虚拟资源分配、虚拟资源的异常使用和重要系统命令的使用等；

3) 记录云计算平台管理员对租户资源的操作信息，如：对租户虚拟化实例的建立、变更、回收，对虚拟存储设备进行挂卷、卸卷等变更操作；。

4) 记录租户通过云计算平台对租户资源的操作信息；

5) 记录云计算平台运行过程的系统日志信息；

6) 记录其他与云计算平台安全有关的事件或专门定义的可审计事件信息。

b) 应支持审计记录包括安全事件的主体、客体、时间、类型和结果等内容的能力；

c) 应支持审计记录时间由云计算平台唯一确定的时钟产生的能力；

d) 应支持云计算平台管理员对审计记录进行查询、分类和分析的功能，并支持生成相关审计报表的能力；

e) 应支持租户间审计记录信息相互隔离的能力；

f) 应支持租户收集和查看与本租户资源相关的审计记录信息的能力；

g) 应支持审计信息保护，禁止非授权的用户或实体获取审计信息，避免受到未预期的删除、修改或覆盖和丢失的能力；

h) 应支持审计信息的保存期限满足法律法规及云服务提供者和租户的信息留存要求的能力；

i) 应支持实时监控和处置安全事件审计信息的能力；
包括支持设置规则监控审计事件，并根据这些规则判断安全侵害，当检测到有安全侵害事件时，支持自动进行审计响应的能力。

8.2.2 增强要求

云计算平台应符合的增强要求如下：

a) 应支持云计算平台审计信息集中审计的能力；
b) 应支持租户使用第三方审计系统或接口，实现租户职责范围内集中审计的能力；
c) 应支持第三方审计系统或接口获取云计算平台固件和关键软件启动过程中版本信息的能力；
d) 应支持第三方审计系统或接口获取云计算平台初始配置信息的能力；
e) 应支持第三方审计系统或接口获取云计算平台关键软件运行过程中版本信息的能力；
f) 应支持第三方审计系统或接口获取云计算平台关运行过程中关键配置信息的能力；
g) 应支持第三方审计系统或接口获取云计算平台关运行过程中审计信息的能力。

8.3 存储与备份管理

8.3.1 基础要求

云计算平台应符合的基础要求如下：

a) 应支持租户系统和数据的备份，并支持租户根据所备份信息进行系统和数据恢复的能力。

8.3.2 增强要求

云计算平台应符合的增强要求如下：

a) 应支持对云计算平台的备份系统和备份数据进行周期性测试，识别故障和备份重建的能力；
b) 应支持租户查询数据和备份数据存储位置的能力。

8.4 安全运维

8.4.1 基础要求

云计算平台应符合的基础要求如下：

a) 应支持安全策略的集中管理和自动下发能力；
b) 应支持统一的运维入口的能力。
统一的运维入口要求支持运维人员的权限控制，并支持对所有活动记录日志的能力。

8.4.2 增强要求

无。

8.5 威胁与脆弱性管理

8.5.1 基础要求

云计算平台应符合的基础要求如下：

a) 应支持定期对云计算平台运行的硬件和软件系统进行安全性检测，识别与鉴别、鉴权、授权、访问控制和系统完整性设置相关的特定安全脆弱性的能力；
b) 应支持统一的补丁管理机制，支持识别云计算资源管理平台、主机、网络、存储等虚拟和物理资源的补丁状态，并支持自动化补丁安装的能力；
c) 应支持云计算平台系统镜像文件安全补丁管理措施，对非工作状态的虚拟机镜像应支持补丁触发或定期升级方式进行系统补丁升级的能力；
d) 应支持实时监控云计算平台各安全组件的运行情况，当发现网络攻击、病毒入侵、网络异常及未授权访问等安全威胁时，发出告警信息的能力。

8.5.2 增强要求

云计算平台应符合的增强要求如下：

a) 应支持内核补丁升级不中断租户业务的能力；
b) 应支持安全威胁预警的能力
注：安全威胁预警指对云计算平台的基础信息、静态的配置信息、动态的系统运行信息、网络流量信息、用户访问行为、安全事件日志、漏洞信息等能引发云计算平台网络安全态势发生变化的要素进行全面、快速和准确地捕获，通过关联回溯、大数据分析及安全建模等技术提前发现可能引发安全事件的威胁，实现对威胁的提前预警。

8.6 密钥与证书管理

8.6.1 基础要求

云计算平台应符合的基础要求如下：
a) 应支持云计算平台所使用数字证书，以及租户与云计算平台进行业务交互时所使用的数字证书统一管理的能力；
注：数字证书统一管理是指对证书全生命周期进行统一管理，包括证书的颁发、验签、撤消等。
b) 应支持对云计算平台所使用密钥统一管理的能力。
注：密钥统一管理是指对密钥的全生命周期进行统一管理，包括密钥产生、分发、更新、使用、备份和销毁等。

8.6.2 增强要求

云计算平台应符合的增强要求如下：
a) 应支持租户与云计算平台进行业务交互时所使用的数字证书导入专用安全硬件（例如：USBkey、SmartCard 等）的能力；
b) 应支持使用统一的密钥管理系统，实现密钥统一管理的能力；
c) 应支持由硬件安全模块实现密钥全生命周期管理的能力。

9 安全服务

9.1 网络安全服务

9.1.1 基础要求

云计算平台应符合的基础要求如下：
a) 应支持为租户提供基本的DDoS防御服务的能力。

9.1.2 增强要求

云计算平台应符合的增强要求如下：
a) 应支持为租户提供增强的DDoS防御服务的能力；
b) 应支持为租户提供入侵检测或入侵防御服务的能力。

9.2 主机安全服务

9.2.1 基础要求

无。

9.2.2 增强要求

云计算平台应符合的增强要求如下：
a) 应支持为租户的虚拟机提供防病毒服务的能力；
b) 应支持为租户提供版本漏洞及补丁检测服务的能力；
版本漏洞及补丁检测服务提供检测系统服务组件及各类中间件的版本漏洞，提醒版本升级或补丁更新。

c) 应支持为租户的操作系统提供安全的软件源升级服务的能力；
d) 应支持为租户系统提供安全配置检查与提醒服务的能力；
安全配置检查与提醒服务检查包括但不限于服务与端口的开启、帐号登录策略、口令强度策略、主机防火墙策略、日志开启策略等，发现异常提醒；
e) 应支持为租户虚拟机提供消除安全防护间隙服务的能力；
f) 应支持为租户提供系统账号安全服务的能力；
系统账号安全服务提供检测并提醒租户关于操作系统帐号的高危操作，如异地登录行为，以及对其进行暴力破解的行为；
g) 应支持为租户提供数据库安全服务的能力；
数据库安全服务提供数据库加固、审计、扫描、访问控制、加密等服务。

9.3 应用安全服务

9.3.1 基础要求

无。

9.3.2 增强要求

云计算平台应符合的增强要求如下：
a) 应支持为租户系统提供Web安全防护服务的能力；
b) 应支持为租户系统提供Web漏洞扫描服务的能力；
c) 应支持为租户提供移动应用安全服务的能力。

9.4 数据安全服务

9.4.1 基础要求

无。

9.4.2 增强要求

云计算平台应符合的增强要求如下：
a) 应支持为租户提供文件加密服务的能力；
b) 应支持为租户提供数据卷加密服务的能力；
c) 应支持为租户提供系统卷加密服务的能力；
d) 应支持为租户提供密钥管理服务的能力；
e) 应支持租户密钥由租户自管理或第三方管理的能力；
f) 应支持为租户提供备份和恢复服务的能力；
g) 应支持为租户数据提供完整性验证服务的能力。

9.5 审计与合规安全服务

9.5.1 基础要求

云计算平台应符合的基础要求如下：
a) 应支持为租户提供安全日志服务的能力，安全日志包括登录日志、资源请求日志、API调用日志等。

9.5.2 增强要求

云计算平台应符合的增强要求如下：
a) 应支持为租户提供内容安全服务的能力，提供对敏感内容的检测；
b) 应支持为租户系统提供运维审计服务的能力；
c) 应支持为租户内部网络提供安全监控服务的能力；
注：安全监控服务为租户提供租户内部网络安全监控；

d) 应支持为租户提供安全审计服务的能力；

注：安全审计服务是根据租户业务需求或合规性需求，提供租户包括但不限于审计日志收集、存储、分析、查阅和审计响应的功能服务，并可定期出具审计分析报告。

9.6 安全情报服务

9.6.1 基础要求

无。

9.6.2 增强要求

云计算平台应符合的增强要求如下：

a) 应支持为租户提供安全情报或安全态势感知服务的能力。

附录 A（资料性附录）

A.1 基础硬件安全

云计算平台应符合的要求如下：

a) 应支持以服务器或存储设备的硬件级部件（安全芯片或安全固件）作为系统信任根，为云计算平台机密性和完整性保护提供支持的能力；

b) 应支持硬件唯一标识符，为云计算平台及上层应用提供拥有硬件标识的身份证书的能力；

c) 应支持服务器或存储设备安全启动的能力。

注：服务器或存储设备安全启动，指服务器或存储设备上电到操作系统启动过程中涉及到的所有软件模块（包括BIOS、固件、操作系统内核等，安全芯片或安全固件内的软件模块除外）经过完整性验证。启动过程中发现某部件完整性破坏，支持按安全策略暂停或继续系统启动。

A.2 计算资源管理平台安全

计算资源管理平台应符合的要求如下：

a) 应支持对重要程序基于硬件级的安全启动；

b) 应支持对重要程序运行状态下基于硬件级的完整性保护；

c) 应支持对重要配置文件基于硬件级的完整性保护；

d) 应支持虚拟机启动过程基于硬件级的完整性保护；

e) 应支持虚拟机运行过程基于硬件级的完整性保护。

A.3 存储资源管理平台安全

存储资源管理平台应符合的要求如下：

a) 应支持对重要程序运行状态下完整性保护；

b) 应支持对重要程序基于硬件级的安全启动；

c) 应支持对重要程序运行状态下基于硬件级的完整性保护；

d) 应支持对重要配置文件基于硬件级的完整性保护。

A.4 安全审计

云计算平台应符合的要求如下：

a) 应支持第三方审计系统或接口获取的系统固件和关键软件启动过程中版本信息采用了基于云计算平台硬件能力的完整性保护和云计算平台身份证书签名的能力；

b) 应支持第三方审计系统或接口获取的系统初始配置信息采用了基于云计算平台硬件能力的完整性保护和云计算平台身份证书签名的能力；

c) 应支持第三方审计系统或接口获取的系统软件运行过程中版本信息采用了基于云计算平台硬件能力的完整性保护和云计算平台身份证书签名，上报频率满足策略要求的能力；

d) 应支持第三方审计系统或接口获取的系统运行过程关键配置信息采用了基于云计算平台硬件能力的完整性保护和云计算平台身份证书签名，上报频率满足策略要求的能力；

e) 应支持第三方审计系统或接口获取的系统运行过程中的审计信息采用了云计算平台硬件能力的完整性保护和云计算平台身份证书签名，上报频率满足策略要求的能力。

参考文献

[1] FedRAMP Security Controls Baseline Version 1.1

[2]NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations V4.0

[3] NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing

[4]GB/T 31168-2014 信息安全技术云计算服务安全能力要求(Information security technology -- Security capability requirements of cloud computing services)

[5]GB/T 32399-2015 信息技术云计算参考架构(Information technology -- Cloud computing -- Reference architecure)

[6]GB/T 32400-2015 信息技术云计算概览与词汇(Information technology -- Cloud computing -- Overview and vocabulary)