C S A 云 安 全 联 盟 标 准

CSA 0001.3—2016

云计算安全技术要求
第 3 部分：PaaS 安全技术要求

Cloud ComputingSecurity Technology Requirements(CSTR)

Part 3:Security technology requirements of PaaS

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（草案）》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3部分。

本部分按照ISO/IEC 导则第2部分：国际标准的机构和编写规则起草。

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

本标准以公有云为主要场景，同时考虑了私有云、社区云、混合云等场景，适用于公有云、私有云、社区云、混合云产品和解决方案。

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云服务商的特定安全目标，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产品实际应用的场景。

云计算安全技术标准要求

第3部分：PaaS安全技术标准要求

1 范围

本部分描述了PaaS产品与解决方案应具备的安全技术能力。

本部分适用于PaaS产品与解决方案提供商在设计开发PaaS产品与解决方案时使用，也可供PaaS服务提供商选择PaaS产品与解决方案时参考，还可为客户选择PaaS服务时判断PaaS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 PaaS 云服务安全技术要求框架

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

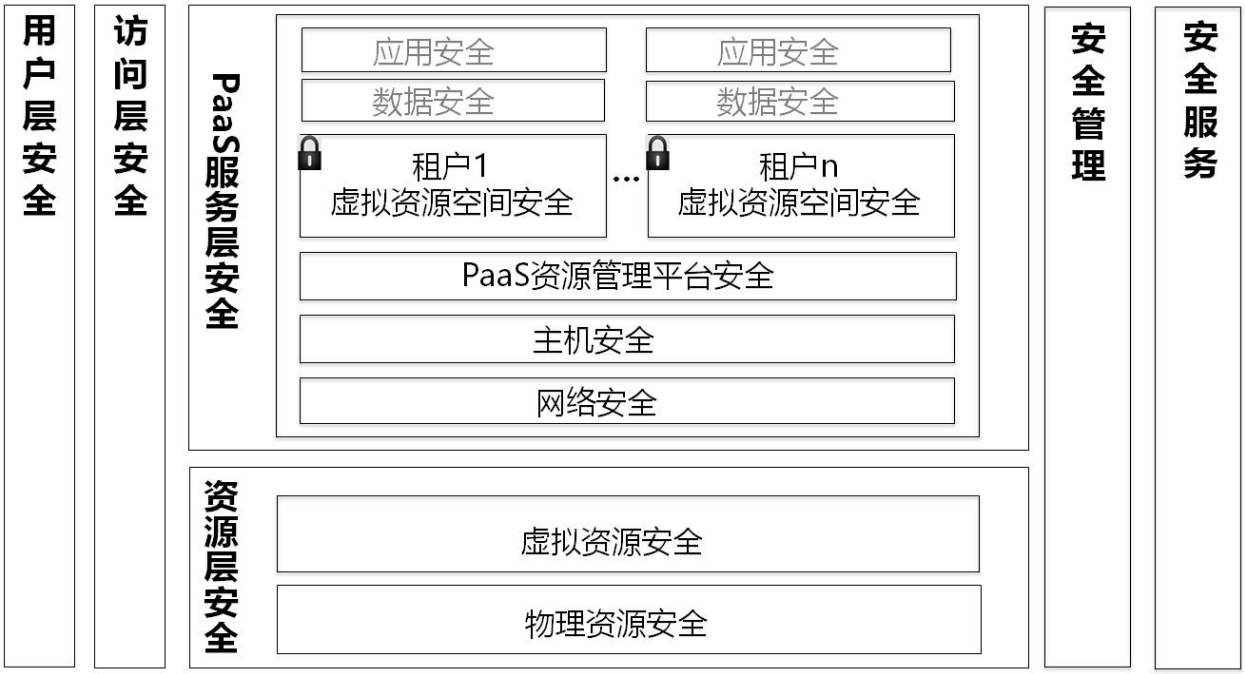

图 1 PaaS 云服务安全技术要求框架

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

PaaS 服务所需的基础资源可以由 IaaS 服务提供商提供，也可以由传统的数据中心提供。

-- 基础资源由 IaaS 服务提供商提供时，资源层安全责任由 IaaS 服务提供商承担，PaaS 服务提供商只需要选择安全能力满足自身业务需求的 IaaS 服务提供商。

-- 基础资源由传统数据中心提供时，基础资源的安全由 PaaS 服务提供商负责，基础资源的安全技术要求请参考业界最佳实佳，不在本标准范围之内。

4.4 服务层安全

在 PaaS 服务类别，根据云计算安全责任模型，PaaS 服务提供商负责 PaaS 平台安全，包括网络、主机、软件平台的安全。同时为 PaaS 租户提供一个安全的虚拟资源空间，并把该空间的控制权交给 PaaS 租户。在 PaaS 租户虚拟资源私有空间内的安全由租户负责，PaaS 租户虚拟资源私有空间内的安全技术要求不在本标准范围之内，图 1 中显示为灰色背景。

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

PaaS 系统应符合的基础要求如下：

a) 应支持保护用户访问 PaaS 系统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 PaaS 系统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

PaaS 系统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，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

PaaS 系统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

基础资源由IaaS服务提供商提供时，IaaS安全技术标准参考《云计算安全技术要求 第3部分：IaaS安全技术要求》。

7 服务层安全

7.1 网络安全

7.1.1 基础要求

PaaS 系统应符合的基础要求如下：

a) 应支持划分为不同的网络区域，以及不同区域之间逻辑隔离的能力；
b) 应支持PaaS系统管理网络与PaaS系统业务网络逻辑隔离的能力；
c) 应支持PaaS系统业务和管理网络与PaaS租户业务网络逻辑隔离的能力；
d) 应支持主要网络设备（包括虚拟化网络设备）以及安全设备业务处理能力弹性扩展的能力；
e) 应支持网络高可用性部署，在系统出现部分故障时，自动将业务转离受影响系统的能力；
f) 应支持系统管理员登录管理网络访问控制的能力；
g) 应支持对管理网络最大流量及单用户网络连接数限制的能力；
h) 应支持对进出PaaS系统业务和管理网络的信息内容进行过滤的能力；
i) 应支持对PaaS系统管理网络远程管理时特权命令进行限制的能力；
j) 应支持对PaaS系统网络边界管理设备受控接口ACL策略自动化更新的能力；
k) 应支持绘制与当前运行情况相符的网络拓扑结构图，并能对网络资源、网络拓扑进行实时更新和集中监控的能力；
l) 应支持对 PaaS 系统 DDoS 攻击防护的能力；
m) 应支持对 PaaS 系统网络边界流量监控、攻击和入侵行为检测的能力；
n) 应支持PaaS租户采用VPN通道访问PaaS服务的能力；
o) 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；
p) 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；
q) 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；
r) 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的能力；
s) 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的能力；
t) 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；
u) 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的能力；
v) 应支持区域边界处的网络设备和安全设备的日志记录、审计报表的能力。

7.1.2 增强要求

PaaS 系统应符合的增强要求如下：

a) 应支持对PaaS系统业务和管理网络的非法连接检测及阻断的能力。

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。

7.2 主机安全

7.2.1 基础要求

PaaS 系统应符合的基础要求如下：

a) 应支持主机安全加固的能力；
b) 应支持主机生命周期管理能力；
c) 应支持主机入侵检测和防范的能力；
d) 应支持主机恶意代码防护的能力。

7.2.2 增强要求

PaaS 系统应符合的增强要求如下：

a) 应支持主机安全启动的能力；

注：安全启动指启动时的版本和预期是一致的，完整性没有受到破坏。

b) 应支持主机重要配置文件完整性保护的能力；

c) 应支持主机运行过程完整性保护的能力。

7.3PaaS 资源管理平台安全

7.3.1 基础要求

PaaS 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) 应支持安全加固的能力；

c) 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；

d) 应支持对恶意代码进行检测和处置的能力；

e) 应支持对 Web 应用漏洞进行检测和防护的能力；

f) 应支持监视远程管理连接，中断未授权管理连接的能力；

g) 应支持对远程执行PaaS平台软件特权管理命令进行限制的能力；

h) 应支持最小化安装，仅安装必要的组件和应用程序的能力；

i) 应支持资源集中监控的能力；

j) 应支持过载保护，保障业务公平性和系统资源利用最大化的能力；

k) 应支持租户故障的安全隔离，单个PaaS租户应用故障，不影响其他租户的能力；

l) 应支持可用性，部分系统故障不影响提供PaaS服务的能力；

m) 应支持禁止系统管理员直接访问查看租户数据的能力；

n) 应支持用户权限控制，支持限制用户功能权限和数据访问权限的能力；

o) 应支持设置用户权限最小化的能力；

p) 应支持控制PaaS用户使用资源，限制用户不超范围使用资源的能力；

q) 应支持PaaS用户的资源使用监控，支持资源异常提醒的能力；

r) 应支持记录PaaS系统的登录日志的能力；
登录日志包括记录用户成功、失败的认证、登录、用户注销、超时退出等活动。

s) 应支持记录对用户信息管理日志的能力，管理日志包括记录用户和用户权限的增删改以及密码的修改和重置等活动；

t) 应支持记录数据操作日志的能力，数据操作日志包括应记录应用系统中存放的业务数据进行操作(查询、修改、删除等)的活动等；

u) 应支持向PaaS租户提供审计日志的能力。

7.3.2 增强要求

PaaS 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) 应支持安全启动的能力；
注：安全启动指启动时的版本和预期是一致的，完整性没有受到破坏。

c) 应支持对重要配置文件完整性检测的能力；

d) 应支持对重要程序运行状态下完整性保护的能力；

e) 应支持软件白名单的能力；

f) 应支持组件间通信采用安全传输的能力；

g) 应支持补丁升级不影响业务正常运行的能力；

h) 应支持PaaS租户自定义网络访问控制，自定义允许访问PaaS服务的IP 地址列表的能力；

i) 应支持向PaaS租户提供统一获取日志的接口能力；

j) 应支持网络高可用性部署，在系统出现部分故障时，自动将业务转离受影响系统的能力。

7.4 租户虚拟资源空间安全

7.4.1 基础要求

PaaS 系统应符合的基础要求如下：

a) 应支持租户间PaaS服务的安全隔离，PaaS租户只能访问和操作自己PaaS服务资源的能力；
b) 应支持限制PaaS系统管理员未授权访问PaaS租户应用资源的能力；
c) 应支持租户间的数据安全隔离，PaaS租户只能访问和操作自己PaaS服务数据的能力；
d) 应支持限制PaaS系统管理员未授权访问PaaS租户数据的能力；
e) 应支持由PaaS租户自行定义和设置数据备份和数据导出权限的能力；
f) 应支持由PaaS租户自行定义和设置数据重置权限的能力；
g) 应支持PaaS租户的应用和数据存储资源回收时应删除租户相关数据的能力；
h) 应支持PaaS租户退租后删除租户相关数据，包括删除备份和归档数据的能力。

7.4.2 增强要求

PaaS 系统应符合的增强要求如下：

a) 应支持PaaS租户间采用不同实例或主机隔离的能力。

8 安全管理

8.1 身份鉴别和访问管理

8.1.1 基础要求

PaaS 系统应符合的基础要求如下：

a) 应支持租户身份和访问管理，集中管理租户账户的能力；
b) 应支持租户密码策略管理的能力，密码策略管理能力应满足如下要求：
   1) 支持密码复杂度策略；
   2) 支持设置密码有效期，到期强制租户修改密码
   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。
c) 应支持集中管理租户鉴别凭证，保护租户鉴别凭证的机密性和完整性的能力；
d) 应支持在租户修改任何租户鉴别凭证前强制进行租户身份验证的能力；
e) 应支持租户账户异常检测并通知租户的能力；
f) 应支持多种租户身份鉴别方式的能力；
g) 应支持租户自主选择两种或两种以上的组合机制进行身份鉴别的能力。
h) 应支持依据系统管理员的角色建立不同的账号并分配权限的能力；
i) 应支持系统管理员用户首次登录时强制用户修改默认口令的能力；
j) 应支持系统管理员权限分离的能力；
k) 应支持系统管理员权限最小化的能力；
l) 应支持多种系统管理员身份鉴别方式的能力；
m) 应支持系统管理员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

PaaS 系统应符合的增强要求如下：

a) 应支持系统管理员特权账号管理的能力，特权账号管理应满足如下要求：
   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；
c) 应支持与租户自建身份认证中心对接的能力。

8.2 安全审计

8.2.1 基础要求

PaaS 系统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应满足如下要求：
   1) 记录 PaaS 系统管理员和租户登录信息和身份鉴别信息；
   2) 记录 PaaS 系统管理员对 PaaS 系统资源的管理操作信息；
   3) PaaS 系统管理员对租户资源的操作信息。
   4) 租户通过 PaaS 系统对租户资源的操作信息；
   5) 记录 PaaS 系统运行过程的系统日志信息；
   6) 记录其他与 PaaS 系统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 PaaS 系统唯一确定的时钟产生的能力；
d) 应支持系统管理员对审计记录进行查询、分类和分析，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的相互隔离的能力；
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、覆盖或丢失的能力；
h) 应支持审计信息满足法律法规及云服务商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

PaaS 系统应符合的增强要求如下：

a) 应支持 PaaS 系统审计信息的集中审计能力；
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 PaaS 系统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 PaaS 系统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 PaaS 系统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系统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系统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

PaaS 系统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

PaaS 系统应符合的增强要求如下：

a) 应支持租户查询数据和备份数据存储位置的能力；
b) 应支持对 PaaS 系统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。

8.4 安全运维

8.4.1 基础要求

PaaS 系统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化下发的能力；

b) 应支持统一的运维入口的能力，同时，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

PaaS 系统应符合的基础要求如下：

a) 应支持定期对 PaaS 系统运行的硬件和软件系统进行安全性检测，识别与鉴别、授权、访问控制和系统完整性设置相关的特定的安全脆弱性的能力；

b) 应支持统一的补丁管理机制，支持识别 PaaS 系统软件、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) 应支持实时监控 PaaS 系统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

PaaS 系统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 PaaS 系统的基础信息、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 PaaS 系统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

PaaS 系统应符合的基础要求如下：

a) 应支持 PaaS 系统所使用数字证书，以及租户与 PaaS 系统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 PaaS 系统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

PaaS 系统应符合的增强要求如下：

a) 应支持租户与 PaaS 系统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 应用安全服务

9.1.1 基础要求

无。

9.1.2 增强要求

PaaS 系统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。

9.2 数据安全服务

9.2.1 增强要求

无。

9.2.2 增强要求

PaaS 系统应符合的增强要求如下：

a) 应支持为租户提供数据加密服务的能力；

b) 应支持为租户提供密钥管理服务的能力；

c) 应支持租户密钥由租户自管理或第三方管理服务的能力；

d) 应支持为租户提供备份和恢复服务的能力；

e) 应支持为租户提供系统账号安全服务的能力；

f) 应支持为租户提供数据库安全服务的能力；

g) 应支持为租户提供数据完整性验证服务的能力；

h) 应支持为租户提供数据访问控制服务的能力。

9.3 审计与合规安全服务

9.3.1 基础要求

PaaS 系统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。

注：安全日志服务向租户提供租户在PaaS系统的日志信息，如登录日志、资源请求日志、API调用日志等。

9.3.2 增强要求

PaaS 系统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，包括对反动、赌博、色情、枪支、毒品等敏感内容的实时监控和检测；

b) 应支持为租户系统提供运维审计服务的能力；

c) 应支持为租户提供安全监控服务的能力。

注：安全监控服务指为租户提供租户内部网络安全监控。

9.4 安全情报服务

9.4.1 基础要求

无。

9.4.2 增强要求

PaaS 系统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 主机安全

PaaS 系统应符合的要求如下：

a) 应支持基于硬件保护的主机安全启动能力；
b) 应支持基于硬件保护的主机运行状态完整性保护的能力。

A.2 PaaS 资源管理平台

PaaS 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安全保护的安全启动的能力；
b) 应支持对重要程序运行状态下基于硬件安全保护的完整性保护的能力；
c) 应支持对重要配置文件基于硬件安全保护的完整性保护的能力。

A.3 安全审计

PaaS系统应符合的要求如下：

a) 应支持第三方审计系统或接口获取的系统关键软件启动过程中版本信息采用了基于 PaaS 系统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 PaaS 系统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 PaaS 系统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 PaaS 系统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 PaaS 系统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)