C S A 云 安 全 联 盟 标 准

CSA 0001.1—2016

云计算安全技术要求
第 1 部分：总则

Cloud Computing Security Technology Requirements(CSTR)

Part 1: General

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1部分。

本部分标准按照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、云安全（深圳）测评技术有限公司、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、深圳安布斯网络科技有限公司、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。

鸣谢：

感谢中金国际亦庄互联网研究院、腾讯云计算（北京）有限责任公司、华为技术有限公司、北京百度网讯科技有限公司、金蝶国际软件集团有限公司、阿里云计算有限公司、中国科学院信息工程研究所（信息安全国家重点实验室）在标准制定过程中提供的会议场所和会务组织。

感谢CSA大中华区 李雨航、叶思海、杨炳年、段学忠、于小丽在标准制定过程中的组织协调工作。

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

第1部分：总则

1 范围

本标准适用于云服务开发者在设计开发云计算产品和解决方案时使用，也可供云服务商选择云计算产品与解决方案时参考，还可为云服务客户选择云服务时判断云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。

本部分描述了云计算安全技术要求总则。

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。

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

以下术语和定义适用于本文件。

3.1 其他标准中定义的术语

3.1.1

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的模式，资源可按需自助获取和管理。

注：资源实例包括服务器、操作系统、网络、软件、应用和存储设备等。

[GB/T 32400-2015 ISO/IEC 17788:2014]

3.1.2

云服务 cloud service

通过云计算已定义的接口，提供一种或多种资源的能力。

[GB/T 32400-2015 ISO/IEC 17788:2014]

3.1.3

参与方 party

一个或一组自然人或法人，无论该法人是否注册。

[GB/T 32400-2015 ISO 27729:2012]

3.1.4

云服务提供者 cloud service provider

提供云服务的参与方。

[GB/T 32400-2015 ISO/IEC 17788:2014]

3.1.5

云服务客户 cloud service consumer

为使用云服务而处于一定业务关系中的参与方。

注 1：业务关系不一定包含经济条款。

注 2：本标准中云服务客户简称客户。

[GB/T 32400-2015 ISO/IEC 17788:2014]

3.1.6

云服务用户 cloud service user

云服务客户中使用云服务的自然人或实体代表。

注 1：上述实体包括设备和应用等。

注 2：本标准中云服务用户简称用户。

[GB/T 32400-2015 ISO/IEC 17788:2014]

3.1.7

租户 tenant

对一组物理和虚拟资源进行共享访问的一个或多个云服务用户。

[GB/T 32400-2015 ISO/IEC 17788:2014]

3.1.8

云能力类型 cloud capabilities type

根据资源使用情况对提供给云服务客户的云服务功能进行的分类。

注：云能力类型包括应用能力类型、基础设施能力类型和平台能力类型。

[GB/T 32400-2015 ISO/IEC 17788:2014]

3.1.9

基础设施能力类型 infrastructure capabilities type

云服务客户能配置和使用计算、存储或网络资源的一类云能力类型。

[GB/T 32400-2015 ISO/IEC 17788:2014]

3.1.10

平台能力类型 platform capabilities type

云服务客户能使用云服务提供者支持的编程语言和执行环境来部署、管理和运行客户创建或获取的应用的一类云能力类型。

[GB/T 32400-2015 ISO/IEC 17788:2014]

3.1.11

应用能力类型 application capabilities type

云服务客户能使用云服务提供者应用的一类云能力类型。

[GB/T 32400-2015 ISO/IEC 17788:2014]

3.1.12

云服务类别 cloud service category

拥有某些相同质量集合的一组云服务。

注：一种云服务类别能包含一种或多种云能力类型的能力。

[GB/T 32400-2015 ISO/IEC 17788:2014]

3.1.13

基础设施即服务 Infrastructure as a Service; IaaS

为云服务客户提供云能力类型中的基础设施能力类型的一种云服务类别。

注：云服务客户并不管理或控制底层的物理和虚拟资源，但是控制使用物理和虚拟资源的操作系统、

存储，以及部署的应用。云服务客户也可拥有对某些网络组件（如防火墙）的部分控制能力。

[GB/T 32400-2015 ISO/IEC 17788:2014]

3.1.14

平台即服务 Platform as a Service；PaaS

为云服务客户提供云能力类型中的平台能力类型的一种云服务类别。

[GB/T 32400-2015 ISO/IEC 17788:2014]

3.1.15

软件即服务 Software as a Service；SaaS

为云服务客户提供云能力类型中的应用能力类型的一种云服务类别。

[GB/T 32400-2015 ISO/IEC 17788:2014]

3.2 本标准中定义的术语

3.2.1

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。硬件资源指由计算组件、存储组件、网络组件组成的所有的物理计算资源及其他物理计算基础元素；资源抽象控制组件指对物理计算资源进行软件抽象，云服务提供者通过这些组件提供和管理对物理计算资源的访问。

3.2.2

云计算平台 cloud computing platform

云服务提供者的云计算基础设施及其上的服务软件的集合。

3.2.3

计算资源管理平台 computing resource management platform

云服务提供者对物理计算资源进行软件抽象和管理的控制组件的集合。

3.2.4

存储资源管理平台 storage resource management platform

云服务提供者对物理存储资源进行软件抽象和管理的控制组件的集合。

3.2.5

云计算环境 cloud computing environment

云服务提供者的云计算平台及客户在云计算平台之上部署的软件及相关组件的集合。

3.2.6

PaaS系统PaaS system

PaaS 云服务提供者的云计算平台及其客户在云计算平台之上部署的软件及相关组件的集合。

3.2.7

SaaS系统SaaS system

SaaS 云服务提供者的云计算平台及相关组件的集合。

3.2.8

云计算平台管理网络cloud computing platform management network

承载云计算平台管理指令流量的网络。

3.2.9

云计算平台业务网络cloud computing platform work load network

承载云计算平台自身业务信息流量的网络。

3.2.10

租户私有网络tenant private network

分配给租户的虚拟空间内的网络。

3.2.11

租户业务承载网络tenant's work load carrier network

承载租户私有网络到其他网络流量的网络。

3.2.12

PaaS系统管理网络PaaS system management network

承载 PaaS 系统网络、主机、Paas 资源管理平台管理指令流量的网络。

3.2.13

PaaS系统业务网络PaaS system work load network

承载 PaaS 系统自身业务信息流量的网络。

3.2.14

PaaS租户业务网络PaaS tenant's work load network

承载 PaaS 租户业务流量的网络。

3.2.15

PaaS 资源管理平台 PaaS resource management platform

云服务提供者对 PaaS 资源进行软件抽象和管理的控制组件的集合。

3.2.16

SaaS系统管理网络SaaS system management network

承载 SaaS 系统网络、主机、Saas 资源管理平台、应用软件管理指令流量的网络。

3.2.17

SaaS系统业务网络SaaS system work load network

承载 SaaS 系统自身业务信息流量的网络。

3.2.18

SaaS租户业务网络SaaS tenant's work load network

承载 SaaS 租户业务流量的网络。

3.2.19

内部通信通道internal communication channel

提供虚拟化平台和虚拟机之间的消息通信功能的通道。

注：内部通讯通道不包括为虚拟机提供基本IO能力的通道，例如，网络通讯、磁盘IO。

3.2.20

防护间隙instant-on Gap

虚拟机或系统从没有安全措施或安全措施不完整到实施完整防护措施之间的时间间隔。

4 缩略语

下列缩略语适用于本文件。

API	应用编程接口（Application Programming Interface）
IaaS	基础设施即服务（Infrastructure as a Service）
PaaS	平台即服务（Platform as a Service）
SaaS	软件即服务（Software as a Service）
VLAN	虚拟局域网（Virtual Local Area Network）
VXLAN	可扩张的虚拟局域网（Virtual eXtensible LAN）
CPU	中央处理单元（Central Processing Unit）
VPC	虚拟私有云（Virtual Private Cloud）
ACL	访问控制列表（Access Control List）

NAT	网络地址转换（Network Address Translation）
IP	网络协议（Internet Protocol）
MAC	硬件地址（Media Access Control）
VPN	虚拟专用网络（Virtual Private Network）
CLI	命令行界面（Command Line Interface）
DDoS	分布式拒绝服务（Distributed Denial of Service）

5 概述

5.1 云计算安全责任模型

云计算环境的安全性由云服务提供者和客户共同保障，在不同的云服务类别中，云服务提供者和客户承担的安全责任不同。

云服务主要包括基础设施即服务（IaaS）、平台即服务（PaaS）、软件即服务（SaaS）等三种服务类别。不同服务类别下云服务提供者和客户对资源的控制范围不同，控制范围则决定了安全责任的边界，如下面图1和图2所示，图中两侧的箭头示意了云服务提供者和客户的控制范围。云服务提供者和客户承担各自控制范围内的安全责任。

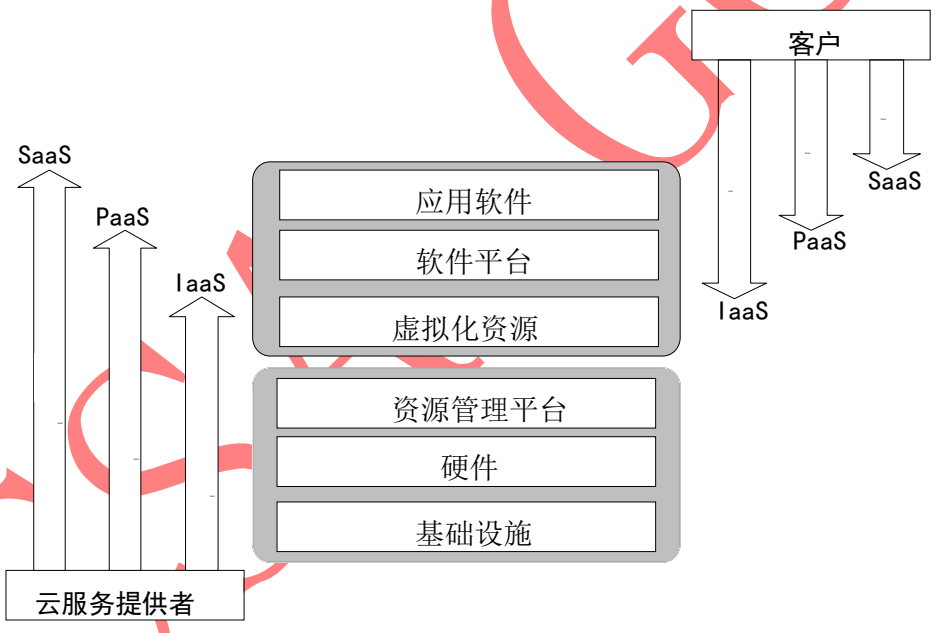

图1 云服务类别与资源控制范围的关系 1

图1表示：

— 在 IaaS 服务类别，IaaS 服务提供者控制了底层的物理和虚拟资源；客户控制了访问和使用 IaaS 服务的用户凭据（如：用户证书、账号口令等）、工具（如：Web 浏览器、客户端软件等）或系统(如：运行客户业务处理、应用、中间件和相关基础设施的企业系统)，客户同时控制了使用物理和虚拟资源的操作系统、存储，以及部署的应用。

— 在 PaaS 服务类别，PaaS 服务提供者控制了底层的物理、虚拟资源和 PaaS 服务的软件平台；客户控制了访问和使用 PaaS 服务的用户凭据、工具或系统，客户同时控制了部署在 PaaS 软件平台的应用。

— 在 SaaS 服务类别，SaaS 服务提供者控制了底层的物理、虚拟资源和 SaaS 服务的软件平台及应用；客户控制了使用 SaaS 应用服务的用户凭据、工具或系统。

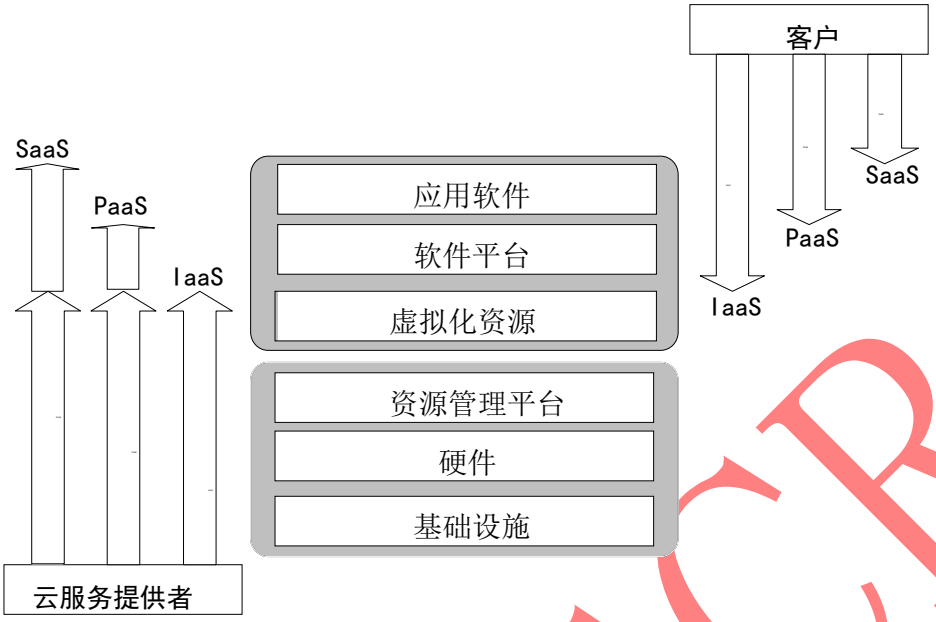

图 2 云服务类别与资源控制范围的关系 2

图2表示：

— 在 IaaS 服务类别，IaaS 服务提供者控制了底层的物理和虚拟资源；客户控制了访问和使用 IaaS 服务的用户凭据、工具或系统，客户同时控制了使用物理和虚拟资源的操作系统、存储，以及部署的应用。

— 在 PaaS 服务类别，PaaS 服务提供者使用了 IaaS 服务，IaaS 服务提供者控制了底层的物理和虚拟资源；PaaS 服务提供者控制了访问和使用 IaaS 服务的用户凭据、工具或系统，同时控制了提供 PaaS 服务的软件平台；客户控制了使用 PaaS 服务的用户凭据、工具或系统，以及部署的应用。

— 在 SaaS 服务类别，SaaS 服务提供者使用了 IaaS 服务，IaaS 服务提供者控制了底层的物理和虚拟资源；SaaS 服务提供者控制了访问和使用 IaaS 服务的用户凭据、工具或系统，同时控制了控制了提供 SaaS 服务的软件平台及应用；客户控制了使用应用服务的用户凭据、工具或系统。

5.2 云计算安全技术要求框架

ISO/IEC 17789:2014 对云计算层次框架的定义如图 3 所示，定义为用户层、访问层、服务层、资源层、跨层功能五个层次。

图 3 云计算层次框架

本标准根据 ISO/IEC 17789:2014 定义的云计算层次框架，结合安全业务特点，定义云计算安全技术要求框架，如图 4 所示：

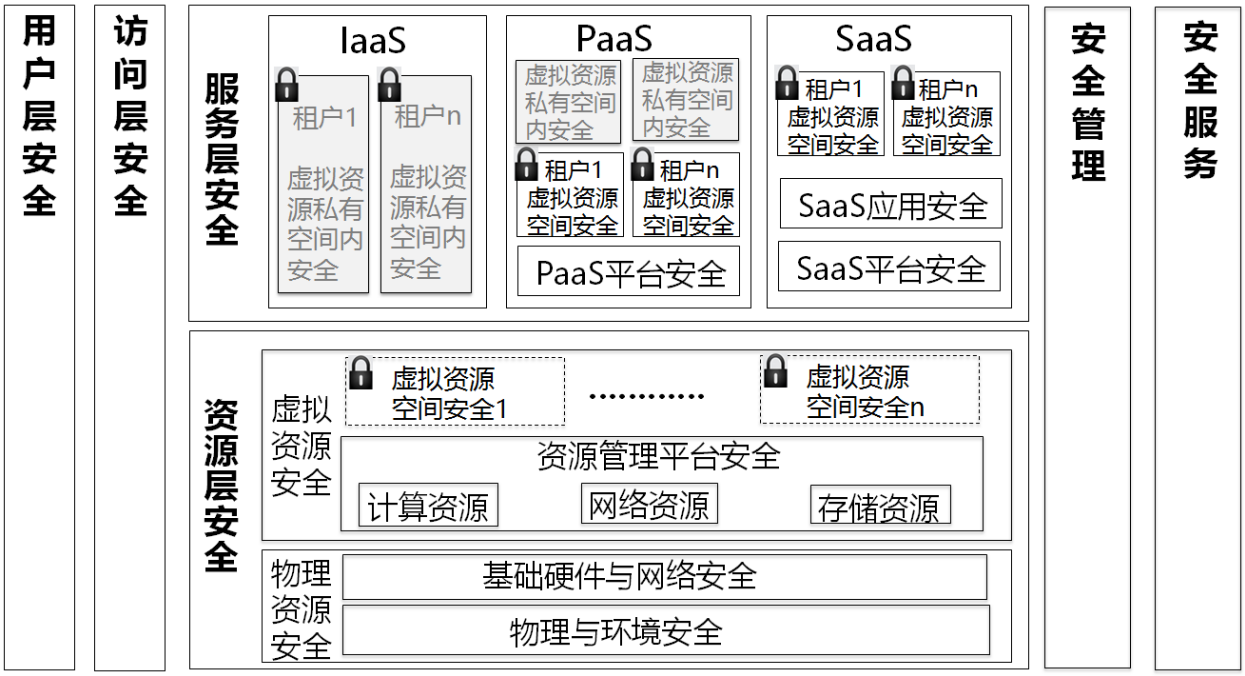

图 4 云计算安全技术要求框架

5.2.1 用户层安全

用户层是用户接口。通过该接口，云服务客户和云服务提供者及其云服务进行交互，执行与客户相关的管理活动，监控云服务。用户层功能包括用户功能、业务功能和管理功能。

用户功能支持云服务用户访问和使用云服务。根据云计算安全责任模型，用户访问和使用云服务的用户凭据、工具或系统等由客户控制，其安全责任由客户承担，对客户的安全技术要求不在本标准范围之内。如果用户访问云服务的工具或系统是由云服务提供者提供的，云服务提供者应提供符合业界最佳安全实践的工具或系统，其安全技术要求不在本标准范围之内。

业务功能支持云服务客户的业务管理活动，如云服务的选择和订购，使用云服务涉及的财务和财务管理，其安全责任由客户承担，对客户的安全技术要求不在本标准范围之内。如果业务功能自身是通过云服务来提供的，其安全技术要求在资源层安全、服务区安全和安全管理中定义。

管理功能支持云服务客户的服务管理活动，包括用户身份和配置文件管理、对服务活动和服务使用的监控、事件处理和问题报告，其安全责任由客户承担，对客户的安全技术要求不在本标准范围之内。

如果管理功能自身是通过云服务来提供的，其安全技术要求在资源层安全、服务区安全和安全管理中定义。

5.2.2 访问层安全

访问层提供对服务层能力进行手动和自动访问的通用接口。这些能力既包含服务能力，也包含管理能力和业务能力。

访问层负责将云服务能力通过一种或多种访问机制展现出来，例如，通过浏览器 Web 访问、通过 API 访问或通过网络直接访问。

访问层安全需要定义访问服务层能力通用接口的安全技术要求。

5.2.3 资源层安全

资源层分为物理资源和资源抽象与控制两部分。

物理资源指云服务提供者运行和管理其提供的云服务所需的各种元素，包括硬件资源，例如计算机（CPU、内存），网络（路由器、防火墙、交换机、网络链路和网络连接器），存储组件（硬盘）和其他物理计算基础设施元素；也包括对硬件资源管理的运营支撑系统，例如服务器上运行的非云特有的软件，以及其他设备，例如主机操作系统、虚拟机监控器、设备驱动程序、通用系统管理软件。

资源抽象与控制指通过对硬件资源的软件抽象，形成虚拟资源，通过对虚拟资源的控制，使云服务提供者能够实现例如快速弹性扩展、资源池化、按需自服务等云计算特征。虚拟资源分配给租户，需要实现不同租户的计算和数据彼此隔离和不可访问，图 4 以一把锁来形象的描述虚拟资源空间的隔离效果。当某个虚拟资源空间分配给某个具体的租户后，该虚拟资源空间的控制权就交给该租户，进入虚拟资源空间的钥匙就交到了租户的手上。

资源层安全需要定义物理资源和虚拟资源安全技术要求。

5.2.4 服务层安全

服务层是对云服务提供者所提供服务的实现，包含和控制实现服务所需的软件组件，并安排通过访问层为用户提供云服务。

不同的服务类别，云服务提供者和客户承担的安全责任不同。服务层安全需要定义云服务提供者控制的资源范围内的安全技术要求，客户控制的资源范围内的安全技术要求不在本标准范围之内。

5.2.5 安全管理

安全管理体系的要求不在本标准范围之内，本标准只定义支撑云计算安全管理体系所需要的安全技术要求。

5.2.6 安全服务

安全服务即以服务的方式提供的安全能力，云服务提供者可通过提供安全服务协助客户做好客户安全责任范围内的安全防护。安全服务属于客户要求才提供，客户不需要时可以随时停用。

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)