ICS 35.040
L 80

中华人民共和国国家标准

GB/T 31167—2014

信息安全技术　云计算服务安全指南

Information security technology—Security guide of cloud computing services

2014-09-03 发布　　2015-04-01 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

中 华 人 民 共 和 国
国 家 标 准
信息安全技术　云计算服务安全指南
GB/T 31167—2014
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.gb168.cn
服务热线:400-168-0010
010-68522006
2014 年 10 月第一版
*
书号:155066·1-50121

版权专有　侵权必究

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:四川大学、中国信息安全研究院有限公司、中国电子科技集团公司第三十研究所、工业和信息化部电子工业标准化研究院、工业和信息化部电子科学技术情报研究所、中国电子信息产业发展研究院、北京信息安全测评中心、中电长城网际系统应用有限公司、中金数据系统有限公司、中国科学院信息工程研究所信息安全国家重点实验室、中国移动通信有限公司研究院、华为技术有限公司、西安未来国际信息股份有限公司、浙江省电子信息产品检验所。

本标准主要起草人:陈兴蜀、左晓栋、闵京华、张建军、罗锋盈、杨建军、罗永刚、刘海峰、黎江、卿斯汉、邬敏华、刘斐、尹丽波、伍扬、冯伟、王惠莅、赵章界、周亚超、刘晓莉。

引　言

云计算是一种计算资源的新型利用模式，客户以购买服务的方式，通过网络获得计算、存储、软件等不同类型的资源。在云计算模式下，使用者不需要自己建设数据中心、购买软硬件资源，避免了前期基础设施的大量投入，仅需较少的使用成本即可获得优质的信息技术(IT)资源和服务。

云计算还处于不断发展阶段，技术架构复杂，采用社会化的云计算服务，使用者的数据和业务从自己的数据中心转移到云服务商的平台中，大量数据集中，使云计算面临新的安全风险。当政府部门采用云计算服务，尤其是社会化的云计算服务时，应特别关注安全问题。

本标准指导政府部门做好采用云计算服务的前期分析和规划，选择合适的云服务商，对云计算服务进行运行监管，考虑退出云计算服务和更换云服务商的安全风险。本标准指导政府部门在云计算服务的生命周期采取相应的安全技术和管理措施，保障数据和业务的安全，安全使用云计算服务。

本标准与GB/T 31168—2014《信息安全技术　云计算服务安全能力要求》构成了云计算服务安全管理的基础标准。本标准面向政府部门，提出了使用云计算服务时的信息安全管理和技术要求；GB/T 31168—2014面向云服务商，提出了为政府部门提供服务时应该具备的信息安全能力要求。

信息安全技术　云计算服务安全指南

1　范围

本标准描述了云计算可能面临的主要安全风险，提出了政府部门采用云计算服务的安全管理基本要求及云计算服务的生命周期各阶段的安全管理和技术要求。

本标准为政府部门采用云计算服务，特别是采用社会化的云计算服务提供全生命周期的安全指导，适用于政府部门采购和使用云计算服务，也可供重点行业和其他企事业单位参考。

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。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/T 25069—2010　信息安全技术　术语

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/T 25069—2010 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

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

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。

3.2

云计算服务　cloud computing service

使用定义的接口，借助云计算提供一种或多种资源的能力。

3.3

云服务商　cloud service provider

云计算服务的供应方。

注：云服务商管理、运营、支撑云计算的基础设施及软件，通过网络交付云计算的资源。

3.4

云服务客户　cloud service customer

为使用云计算服务同云服务商建立业务关系的参与方。

注：本标准中云服务客户简称客户。

3.5

第三方评估机构　Third Party Assessment Organizations；3PAO

独立于云计算服务相关方的专业评估机构。

3.6

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：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、网络链路和接口等）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。

3.7

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。

3.8

云计算环境　cloud computing environment

云服务商提供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。

4　云计算概述

4.1　云计算的主要特征

云计算具有以下主要特征：

a）　按需自助服务。在不需或较少云服务商的人员参与情况下，客户能根据需要获得所需计算资源，如自主确定资源占用时间和数量等。

b）　泛在接入。客户通过标准接入机制，利用计算机、移动电话、平板等各种终端通过网络随时随地使用服务。

c）　资源池化。云服务商将资源（如：计算资源、存储资源、网络资源等）提供给多个客户使用，这些物理的、虚拟的资源根据客户的需求进行动态分配或重新分配。

d）　快速伸缩性。客户可以根据需要快速、灵活、方便地获取和释放计算资源。对于客户来讲，这种资源是“无限”的，能在任何时候获得所需资源量。

e）　服务可计量。云计算可按照多种计量方式（如按次付费或充值使用等）自动控制或量化资源，计量的对象可以是存储空间、计算能力、网络带宽或账户数等。

4.2　服务模式

根据云服务商提供的资源类型的不同，云计算的服务模式主要可分为三类：

a）　软件即服务（SaaS）：在 SaaS 模式下，云服务商向客户提供的是运行在云计算基础设施之上的应用软件。客户不需要购买、开发软件，可利用不同设备上的客户端（如 Web 浏览器）或程序接口通过网络访问和使用云服务商提供的应用软件，如电子邮件系统、协同办公系统等。客户通常不能管理或控制支撑应用软件运行的低层资源，如网络、服务器、操作系统、存储等，但可对应用软件进行有限的配置管理。

b）　平台即服务（PaaS）：在 PaaS 模式下，云服务商向客户提供的是运行在云计算基础设施之上的软件开发和运行平台，如：标准语言与工具、数据访问、通用接口等。客户可利用该平台开发和部署自己的软件。客户通常不能管理或控制支撑平台运行所需的低层资源，如网络、服务器、操作系统、存储等，但可对应用的运行环境进行配置，控制自己部署的应用。

c）　基础设施即服务（IaaS）：在 IaaS 模式下，云服务商向客户提供虚拟计算机、存储、网络等计算资源，提供访问云计算基础设施的服务接口。客户可在这些资源上部署或运行操作系统、中间件、数据库和应用软件等。客户通常不能管理或控制云计算基础设施，但能控制自己部署的操作系统、存储和应用，也能部分控制使用的网络组件，如主机防火墙。

4.3 部署模式

根据使用云计算平台的客户范围的不同，将云计算分成私有云、公有云、社区云和混合云等四种部署模式：

a) 私有云：云计算平台仅提供给某个特定的客户使用。私有云的云计算基础设施可由云服务商拥有、管理和运营，这种私有云称为场外私有云（或外包私有云）；也可由客户自己建设、管理和运营，这种私有云称为场内私有云（或自有私有云）。

b) 公有云：云计算平台的客户范围没有限制。公有云的云计算基础设施由云服务商拥有、管理和运营。

c) 社区云：云计算平台限定为特定的客户群体使用，群体中的客户具有共同的属性（如职能、安全需求、策略等）。社区云的云计算基础设施可由云服务商拥有、管理和运营，这种社区云称为场外社区云；也可以由群体中的部分客户自己建设、管理和运营，这种社区云称为场内社区云。

d) 混合云：上述两种或两种以上部署模式的组合称为混合云。

4.4 云计算的优势

在云计算模式下，客户不需要投入大量资金去建设、运维和管理自己专有的数据中心等基础设施，只需要为动态占用的资源付费，即按需购买服务。客户采用云计算服务可获得如下益处：

a) 减少开销和能耗。采用云计算服务可以将硬件和基础设施建设资金投入转变为按需支付服务费用，客户只对使用的资源付费，无需承担建设和维护基础设施的费用，避免了自建数据中心的资金投入。云服务商使用虚拟化、动态迁移和工作负载整合等技术提升运行资源的利用效率，通过关闭空闲资源组件等降低能耗；多租户共享机制、资源的集中共享可以满足多个客户不同时间段对资源的峰值要求，避免按峰值需求设计容量和性能而造成的资源浪费。资源利用效率的提高有效降低云计算服务的运营成本，减少能耗，实现绿色 IT。

b) 增加业务的灵活性。客户采用云计算服务不需要建设专门的信息系统，缩短业务系统建设周期，使客户能专注于业务的功能和创新，提升业务响应速度和服务质量，实现业务系统的快速部署。

c) 提高业务系统的可用性。云计算的资源池化和快速伸缩性特征，使部署在云计算平台上的客户业务系统可动态扩展，满足业务需求资源的迅速扩充与释放，能避免因需求突增而导致客户业务系统的异常或中断。云计算的备份和多副本机制可提高业务系统的健壮性，避免数据丢失和业务中断。

d) 提升专业性。云服务商具有专业技术团队，能够及时更新或采用先进技术和设备，可以提供更加专业的技术、管理和人员支撑，使客户能获得更加专业和先进的技术服务。

5 云计算的风险管理

5.1 概述

云计算作为一种新兴的计算资源利用方式，还在不断发展之中，传统信息系统的安全问题在云计算环境中大多依然存在，与此同时还出现了一些新的信息安全问题和风险。

本章通过描述云计算带来的信息安全风险，提出了客户采用云计算服务应遵守的基本要求，从规划准备、选择云服务商及部署、运行监管、退出服务等四个阶段简要描述了客户采购和使用云计算服务的生命周期安全管理。

5.2 云计算安全风险

5.2.1 客户对数据和业务系统的控制能力减弱

传统模式下，客户的数据和业务系统都位于客户的数据中心，在客户的直接管理和控制下。在云计算环境里，客户将自己的数据和业务系统迁移到云计算平台上，失去了对这些数据和业务的直接控制能力。客户数据以及在后续运行过程中生成、获取的数据都处于云服务商的直接控制下，云服务商具有访问、利用或操控客户数据的能力。

将数据和业务系统迁移到云计算平台后，安全性主要依赖于云服务商及其所采取的安全措施。云服务商通常把云计算平台的安全措施及其状态视为知识产权和商业秘密，客户在缺乏必要的知情权的情况下，难以了解和掌握云服务商安全措施的实施情况和运行状态，难以对这些安全措施进行有效监督和管理，不能有效监管云服务商的内部人员对客户数据的非授权访问和使用，增加了客户数据和业务的风险。

5.2.2 客户与云服务商之间的责任难以界定

传统模式下，按照谁主管谁负责、谁运行谁负责的原则，信息安全责任相对清楚。在云计算模式下，云计算平台的管理和运行主体与数据安全的责任主体不同，相互之间的责任如何界定，缺乏明确的规定。不同的服务模式和部署模式、云计算环境的复杂性也增加了界定云服务商与客户之间责任的难度。

云服务商可能还会采购、使用其他云服务商的服务，如提供 SaaS 服务的云服务商可能将其服务建立在其他云服务商的 PaaS 或 IaaS 之上，这种情况导致了责任更加难以界定。

5.2.3 可能产生司法管辖权问题

在云计算环境里，数据的实际存储位置往往不受客户控制，客户的数据可能存储在境外数据中心，改变了数据和业务的司法管辖关系。

注：一些国家的政府可能依据本国法律要求云服务商提供可以访问这些数据中心的途径，甚至要求云服务商提供位于他国数据中心的数据。

5.2.4 数据所有权保障面临风险

客户将数据存放在云计算平台上，没有云服务商的配合很难独自将数据安全迁出。在服务终止或发生纠纷时，云服务商还可能以删除或不归还客户数据为要挟，损害客户对数据的所有权和支配权。云服务商通过对客户的资源消耗、通讯流量、缴费等数据的收集统计，可以获取客户的大量相关信息，对这些信息的归属往往没有明确规定，容易引起纠纷。

5.2.5 数据保护更加困难

云计算平台采用虚拟化等技术实现多客户共享计算资源，虚拟机之间的隔离和防护容易受到攻击，跨虚拟机的非授权数据访问风险突出。云服务商可能会使用其他云服务商的服务，使用第三方的功能、性能组件，使云计算平台结构复杂且动态变化。随着复杂性的增加，云计算平台实施有效的数据保护措施更加困难，客户数据被未授权访问、篡改、泄露和丢失的风险增大。

5.2.6 数据残留

存储客户数据的存储介质由云服务商拥有，客户不能直接管理和控制存储介质。当客户退出云计算服务时，云服务商应该完全删除客户的数据，包括备份数据和运行过程中产生的客户相关数据。目

前，还缺乏有效的机制、标准或工具来验证云服务商是否实施了完全删除操作，客户退出云计算服务后其数据仍然可能完整保存或残留在云计算平台上。

5.2.7 容易产生对云服务商的过度依赖

由于缺乏统一的标准和接口，不同云计算平台上的客户数据和业务难以相互迁移，同样也难以从云计算平台迁移回客户的数据中心。另外云服务商出于自身利益考虑，往往不愿意为客户的数据和业务提供可迁移能力。这种对特定云服务商的潜在依赖可能导致客户的业务随云服务商的干扰或停止服务而停止运转，也可能导致数据和业务迁移到其他云服务商的代价过高。由于云计算服务市场还未成熟，供客户选择的候选云服务商有限，也可能导致客户对云服务商的过度依赖。

5.3 云计算服务安全管理的主要角色及责任

云计算服务安全管理的主要角色及责任如下：

a) 云服务商。为确保客户数据和业务系统安全，云服务商应先通过安全审查，才能向客户提供云计算服务；积极配合客户的运行监管工作，对所提供的云计算服务进行运行监视，确保持续满足客户安全需求；合同关系结束时应满足客户数据和业务的迁移需求，确保数据安全。

b) 客户。从已通过安全审查的云服务商中选择适合的云服务商。客户需承担部署或迁移到云计算平台上的数据和业务的最终安全责任；客户应开展云计算服务的运行监管活动，根据相关规定开展信息安全检查。

c) 第三方评估机构。对云服务商及其提供的云计算服务开展独立的安全评估。

5.4 云计算服务安全管理基本要求

采用云计算服务期间，客户和云服务商应遵守以下要求：

a) 安全管理责任不变。信息安全管理责任不应随服务外包而转移，无论客户数据和业务是位于内部信息系统还是云服务商的云计算平台上，客户都是信息安全的最终责任人。

b) 资源的所有权不变。客户提供给云服务商的数据、设备等资源，以及云计算平台上客户业务系统运行过程中收集、产生、存储的数据和文档等都应属客户所有，客户对这些资源的访问、利用、支配等权利不受限制。

c) 司法管辖关系不变。客户数据和业务的司法管辖权不应因采用云计算服务而改变。除非中国法律法规有明确规定，云服务商不得依据其他国家的法律和司法要求将客户数据及相关信息提供给他国政府及组织。

d) 安全管理水平不变。承载客户数据和业务的云计算平台应按照政府信息系统安全管理要求进行管理，为客户提供云计算服务的云服务商应遵守政府信息系统安全管理政策及标准。

e) 坚持先审后用原则。云服务商应具备保障客户数据和业务系统安全的能力，并通过安全审查。客户应选择通过审查的云服务商，并监督云服务商切实履行安全责任，落实安全管理和防护措施。

5.5 云计算服务生命周期

5.5.1 概述

客户采购和使用云计算服务的过程可分为四个阶段：规划准备、选择服务商与部署、运行监管、退出服务，如图 1 所示。

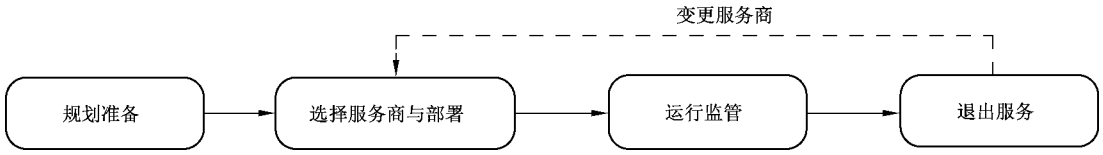

图 1　云计算服务的生命周期

5.5.2　规划准备

在规划准备阶段，客户应分析采用云计算服务的效益，确定自身的数据和业务类型，判定是否适合采用云计算服务；根据数据和业务的类型确定云计算服务的安全能力要求；根据云计算服务的特点进行需求分析，形成决策报告。

5.5.3　选择服务商与部署

在选择服务商与部署阶段，客户应根据安全需求和云计算服务的安全能力选择云服务商，与云服务商协商合同（包括服务水平协议、安全需求、保密要求等内容），完成数据和业务向云计算平台的部署或迁移。

5.5.4　运行监管

在运行监管阶段，客户应指导监督云服务商履行合同规定的责任义务，指导督促业务系统使用者遵守政府信息系统安全管理政策及标准，共同维护数据、业务及云计算环境的安全。

5.5.5　退出服务

在退出云计算服务时，客户应要求云服务商履行相关责任和义务，确保退出云计算服务阶段数据和业务安全，如安全返还客户数据、彻底清除云计算平台上的客户数据等。

需变更云服务商时，客户应按要求选择新的云服务商，重点关注云计算服务迁移过程的数据和业务安全；也应要求原云服务商履行相关责任和义务。

6　规划准备

6.1　概述

5.2 对云计算面临的安全风险及新问题进行了阐述，云计算服务并非适合所有的客户，更不是所有应用都适合部署到云计算环境。是否采用云计算服务，特别是采用社会化的云计算服务，应该综合平衡采用云计算服务后获得的效益、可能面临的信息安全风险、可以采取的安全措施后做出决策。只有当安全风险在客户可以承受、容忍的范围内，或安全风险引起的信息安全事件有适当的控制或补救措施时方可采用云计算服务。

6.2　效益评估

效益是采用云计算服务的最主要动因，只有在可能获得明显的经济和社会效益，或初期效益不一定十分明显，但从发展的角度看潜在效益很大，并且信息安全风险可控时，才宜采用云计算服务。

云计算服务的效益主要从以下几个方面进行分析比较：

a) 建设成本。传统的自建信息系统，需要建设运行环境、采购服务器等硬件设施、定制开发或采购软件等；采用云计算服务，初期资金投入可能包括租用网络带宽、客户采用的安全控制措施等。

b) 运维成本。传统的自建信息系统，日常运行需要考虑设备运行能耗、设备维护、升级改造、增加硬件设备、扩建机房等成本；采用云计算服务，仅需为使用的服务和资源付费。

c) 人力成本。传统的自建信息系统，需要维持相应数量的专业技术人员，包括信息中心等专业机构；采用云计算服务，仅需适当数量的专业技术和管理人员。

d) 性能和质量。云计算服务由具备相当专业技术水准的云服务商提供，云计算平台具有冗余措施、先进的技术和管理、完整的解决方案等特点，应分析采用云计算服务后对业务的性能和质量带来的优势。

e) 创新性。通过采用云计算服务，客户可以将更多的精力放在如何提升核心业务能力、创新公众服务上，而不是业务的技术实现和实施；可以快速部署满足新需求的业务，并按需随时调整。

6.3 政府信息分类

6.3.1 信息分类原则

客户将信息部署或迁移到云计算平台之前，应先明确信息的类型。

本标准中的政府信息是指政府机关，包括受政府委托代行政府机关职能的机构，在履行职责过程中，以及政府合同单位在完成政府委托任务过程中产生、获取的，通过计算机等电子装置处理、保存、传输的数据，相关的程序、文档等。

涉密信息的处理、保存、传输、利用按国家保密法规执行。

本标准将非涉密政府信息分为敏感信息、公开信息两种类型。

6.3.2 敏感信息

6.3.2.1 敏感信息的概念

敏感信息指不涉及国家秘密，但与国家安全、经济发展、社会稳定，以及企业和公众利益密切相关的信息，这些信息一旦未经授权披露、丢失、滥用、篡改或销毁可能造成以下后果：

a) 损害国防、国际关系；

b) 损害国家财产和公共利益，以及个人财产或人身安全；

c) 影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等；

d) 影响行政机关依法调查处理违法、渎职行为，或涉嫌违法、渎职行为；

e) 干扰政府部门依法公正地开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责；

f) 危害国家关键基础设施、政府信息系统安全；

g) 影响市场秩序，造成不公平竞争，破坏市场规律；

h) 可推论出国家秘密事项；

i) 侵犯个人隐私、企业商业秘密和知识产权；

j) 损害国家、企业、个人的其他利益和声誉。

6.3.2.2 敏感信息的范围

敏感信息包括但不限于：

a) 应该公开但正式发布前不宜泄露的信息，如规划、统计、预算、招投标等的过程信息；

b) 执法过程中生成的不宜公开的记录文档；
c) 一定精度和范围的国家地理、资源等基础数据；
d) 个人信息，或通过分析、统计等方法可以获得个人隐私的相关信息；
e) 企业的商业秘密和知识产权中不宜公开的信息；
f) 关键基础设施、政府信息系统安全防护计划、策略、实施等相关信息；
g) 行政机构内部的人事规章和工作制度；
h) 政府部门内部的人员晋升、奖励、处分、能力评价等人事管理信息；
i) 根据国际条约、协议不宜公开的信息；
j) 法律法规确定的不宜公开信息；
k) 单位根据国家要求或本单位要求认定的敏感信息。

6.3.3 公开信息

公开信息指不涉及国家秘密且不是敏感信息的政府信息，包括但不限于：
a) 行政法规、规章和规范性文件，发展规划及相关政策；
b) 统计信息，财政预算决算报告，行政事业性收费的项目、依据、标准；
c) 政府集中采购项目的目录、标准及实施情况；
d) 行政许可的事项、依据、条件、数量、程序、期限以及申请行政许可需要提交的全部材料目录及办理流程；
e) 重大建设项目的批准和实施情况；
f) 扶贫、教育、医疗、社会保障、促进就业等方面的政策、措施及其实施情况；
g) 突发公共事件的应急预案、预警信息及应对情况；
h) 环境保护、公共卫生、安全生产、食品药品、产品质量的监督检查情况等；
i) 其他根据相关法律法规应该公开的信息。

6.4 政府业务分类

6.4.1 业务分类原则

确定了信息类型后，还需要对承载相关信息的业务进行分类。根据业务不能正常开展时可能造成的影响范围和程度，本标准将政府业务划分为一般业务、重要业务、关键业务等三种类型。

6.4.2 一般业务

一般业务出现短期服务中断或无响应不会影响政府部门的核心任务，对公众的日常工作与生活造成的影响范围、程度有限。

通常政府部门、社会公众对一般业务中断的容忍度以天为单位衡量。

6.4.3 重要业务

重要业务一旦受到干扰或停顿，会对政府决策和运转、对公服务产生较大影响，在一定范围内影响公众的工作生活，造成财产损失，引发少数人对政府的不满情绪。此类业务出现问题，造成的影响范围、程度较大。

满足以下条件之一的业务可被认为是重要业务：
——政府部门对业务中断的容忍程度小于 24 h；
——业务系统的服务对象超过 10 万用户；

——信息发布网站的访问量超过每天 500 万人次；

——出现安全事件造成 100 万元以上经济损失；

——出现问题后可能造成其他较大危害。

6.4.4 关键业务

关键业务一旦受到干扰或停顿，将对政府决策和运转、对公服务产生严重影响，威胁国家安全和人民生命财产安全，严重影响政府声誉，在一定程度上动摇公众对政府的信心。

满足以下条件之一的业务可被认为是关键业务：

——政府部门对业务中断的容忍程度小于 1 h；

——业务系统的服务对象超过 100 万用户；

——出现安全事件造成 5 000 万元以上经济损失，或危害人身安全；

——出现问题后可能造成其他严重危害。

6.5 优先级确定

在分类信息和业务的基础上，综合平衡采用云计算服务后的效益和风险，确定优先部署到云计算平台的数据和业务，如图 2 所示。

a) 承载公开信息的一般业务可优先采用包括公有云在内的云计算服务，尤其是那些利用率较低、维护和升级成本较高、与其他系统关联度低的业务应优先考虑采用社会化的云计算服务。

b) 承载敏感信息的一般业务和重要业务，以及承载公开信息的重要业务也可采用云计算服务，但宜采用安全特性较好的私有云或社区云。

c) 关键业务系统暂不宜采用社会化的云计算服务，但可采用场内私有云(自有私有云)。

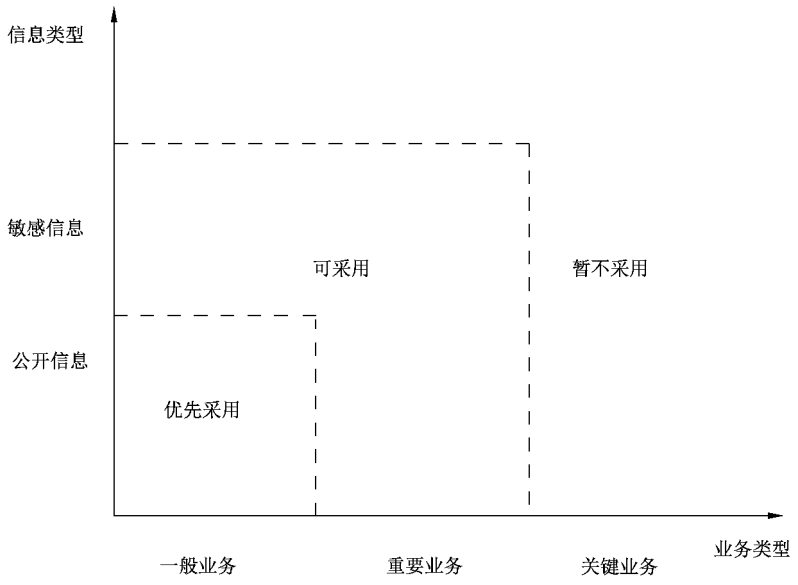

图 2 采用云计算服务的优先级

6.6 安全保护要求

所有的客户信息都应该得到适当的保护。对于公开信息主要是防篡改、防丢失，对于敏感信息还要防止未经授权披露、丢失、滥用、篡改和销毁。

所有的客户业务都应得到适当保护，保证业务的安全性和持续性。

不同类型的信息和业务对安全保护有着不同的要求，客户应要求云服务商提供相应强度的安全保护，如图 3 所示。

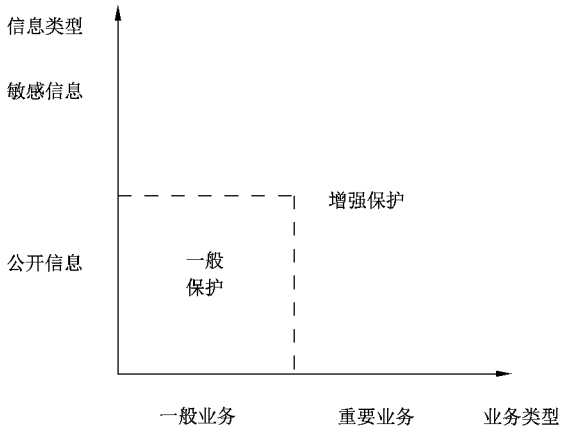

图 3　安全保护要求

对云计算服务的安全能力要求如下：

a）　承载公开信息的一般业务需要一般安全保护；

b）　承载敏感信息的一般业务和重要业务，以及承载公开信息的重要业务需要增强安全保护。

关于一般安全保护和增强安全保护的具体指标要求，见 GB/T 31168—2014。

6.7　需求分析

6.7.1　概述

客户应从以下方面对云计算服务的需求进行分析，提出各项功能、性能及安全要求。

6.7.2　服务模式

云计算有 SaaS、PaaS 和 IaaS 三种主要服务模式。不同服务模式下云服务商与客户的控制范围不同，如图 4 所示，图中两侧的箭头示意了云服务商和客户的控制范围，具体为：

a）　在 SaaS 模式下，应用软件层的安全措施由客户和云服务商分担，其他安全措施由云服务商实施。

b）　在 PaaS 模式下，软件平台层的安全措施由客户和云服务商分担。客户负责自己开发和部署的应用及其运行环境的安全，其他安全措施由云服务商实施。

c）　在 IaaS 模式下，虚拟化计算资源层的安全措施由客户和云服务商分担。客户负责自己部署的操作系统、运行环境和应用的安全。云服务商负责虚拟机监视器及底层资源的安全。

图 4 中的下三层由设施层、硬件层和资源抽象控制层构成。设施层和硬件层是云计算环境的物理元素，设施层主要包括采暖、通风、空调、电力和通信等，硬件层包括了所有的物理计算资源，例如：服务器、网络（路由器、防火墙、交换机、网络连接和接口）、存储部件（硬盘）和其他物理计算元件。资源抽象控制层通过虚拟化或其他软件技术实现对物理计算资源的软件抽象，基于资源分配、访问控制、使用监视等软件组件实现资源的访问控制。在所有服务模式下，这三层均处于云服务商的完全控制下，所有安全措施由云服务商实施。

图 4 中的上三层由应用软件层、软件平台层、虚拟化计算资源层构成云计算环境的逻辑元素。虚拟化计算资源层通过服务接口，使客户可以访问虚拟机、虚拟存储、虚拟网络等计算资源。软件平台层向客户提供编译器、函数库、工具、中间件以及其他用于应用开发和部署的软件工具与组件。应用软件层

向客户提供业务系统需要的应用软件，客户通过客户端或程序接口访问这些应用软件。

客户可根据不同服务模式的特点和自身数据及业务系统的安全管理要求，结合自身的技术能力、市场及技术成熟度等因素选择服务模式。

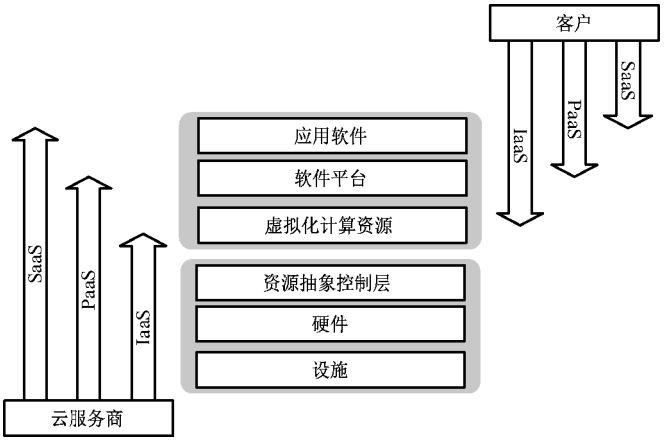

图 4　服务模式与控制范围的关系

6.7.3　部署模式

云计算有公有云、社区云和私有云三种典型部署模式，不同的部署模式下，云计算基础设施部署的场所、客户访问云计算服务的网络链路、是否与其他客户共享资源等属性有较大差异，客户需要综合分析部署模式对自身数据和业务的影响。不同部署模式下关注的主要问题包括：

a) 是否与其他客户共享云计算平台。公有云是云服务商面向社会提供的服务，客户需要与其他未知客户共享云计算平台，安全风险相对较大；社区云中的客户群体具有共同责任、相同安全需求、相同策略等属性，客户与这些有共同属性（如同一行业、同一业务需求等）的已知客户共享资源，安全风险相对较小；私有云的云计算平台为客户独享，由客户或专门委托的云服务商独立管理和控制云计算平台，安全性相对较高。

b) 对云计算平台管理技能的要求。若采用私有云、社区云，且云计算平台由客户承担管理任务，则需要客户具备专业的技术人才，对人员技能的要求远比公有云高。

c) 业务的可扩展性要求。公有云的资源由大量客户共享，资源规模较大，客户可以根据业务和资源使用情况随时调整资源需求，可以充分扩展；社区云和私有云的灵活程度会受到具体的部署场所和策略的影响。

客户应综合考虑以上问题，选择适合的部署模式，使安全风险可控。

6.7.4　功能需求的稳定性和通用性

当客户的业务功能需求不断变化时，云服务商需要不断开发、测试和部署新的组件。云计算的多客户共享资源特点使得云计算平台基于客户的功能定制或变更较为困难。因此，为了提高应用规模和效益，云服务商通常愿意提供通用性较好、功能相对稳定和成熟的服务。

通用的功能需求有助于客户参考成熟的应用案例，包括参考其部署、运行监管、评估等最佳实践，可提高效率并降低安全风险。另外，业务功能的通用性利于实现规模化所带来的低成本效益。

客户应优先将功能需求不经常发生变化的业务部署或迁移到云计算平台，还要考虑是否已有成功的应用案例。

6.7.5 资源的动态需求特点

有些业务具有临时、周期性特点，如公务员招考等业务系统，可能会出现访问和请求的突发高峰，要求可根据访问需求动态分配资源。此类业务采用云计算服务，可以满足动态、灵活的资源需求，且客户只需为业务系统所占用的资源支付使用费用。

客户应优先将对资源有动态、周期变化需求的业务部署或迁移到云计算平台，可在满足业务性能需求的前提下节省资金。

6.7.6 时延

时延是指云计算环境处理某个请求的时间延迟，包括客户请求消息传输到云计算环境和结果回传时间，以及云计算环境的处理时间。不同类型的应用对云计算服务的时延要求差异明显，例如，电子邮件通常容许出现短暂的服务中断和较大的网络时延，但自动化控制与实时应用一般都对时延要求较高。

客户应针对业务系统对响应速度方面的要求做详尽分析，确定业务本身对时延的容忍度，以及可能采取的补救措施等。在将数据和业务部署或迁移到云计算平台前，应考虑响应时间、海量数据传输性能等指标要求。

6.7.7 业务持续性

云计算服务是否会中断、是否能持续访问依赖于多方面因素，包括网络、云计算平台以及云服务商等。

网络依赖。云计算服务依赖于互联网等网络，客户通过持续可用的网络连接来获取服务。网络依赖意味着每个应用都是网络应用，从客户到云计算平台的网络复杂度通常高于客户内部局域网。

平台依赖。尽管专业的云计算平台具有较高的可靠性，但出于人为因素（如恶意攻击或管理员的失误）、自然灾害（如洪水、台风、地震等）的原因，云计算平台故障与服务中断不可能完全避免。

云服务商依赖。采用自有系统时，即使软硬件供应商暂停技术支持、售后服务或停业，客户可能不会立即受到影响，可以继续使用其产品。对于社会化云计算服务而言，客户高度依赖云服务商提供的服务，云服务商倒闭、市场变化等主观或客观原因所造成的中断或停止，会立即导致客户所需服务的中断或停止。

在采用云计算服务前，应对云计算服务的可靠性、持续性需求进行充分评估，应关注中断频率与预期恢复时间。可考虑如下措施：

a) 客户与云计算平台之间的网络链路采用多个网络运营商的优质链路，做到网络链接冗余。

b) 确定云服务商是否有异地数据中心实现数据与业务系统的异地备份，保障即使自然灾害发生，也能对数据进行有效保护和恢复。

c) 对云服务商的经营状态进行定期检查，发现异常及时处理。

6.7.8 可移植性与互操作性

可移植性。移植是指将数据和业务系统从一个云服务商迁移到另一个云服务商的云计算平台，或迁移回客户的数据中心。可移植性取决于标准化的接口与数据格式。可移植性的实现难度与采用的云计算服务模式有关，通常从 IaaS、PaaS 到 SaaS 可移植性的难度逐渐增加。

互操作性。部署在云计算平台上的业务系统可能需要与其他系统进行数据交互，不同云计算平台间及与自有信息系统之间的数据交换与访问目前还较为困难。同时，云服务商为了商业竞争的目的，对可移植性和互操作性支持一般不够积极。

客户应制定将数据和业务系统从某一云计算平台迁移到其他云计算平台或自有数据中心的计划，充分考虑云计算服务与其他已有或将来的业务系统集成需求。

6.7.9 数据的存储位置

云服务商在数据中心选址时，为了节省建造、能源、雇员等成本，可能会将数据中心分布在不同的地区，甚至不同的国家。云计算服务的运行管理对客户往往缺少透明性，客户难以掌握数据和副本在存储设备和数据中心的具体位置。

根据国家的有关规定，存储、处理客户数据的数据中心和云计算基础设施不得设在境外。客户在确定采用云计算服务时，应禁止云服务商在境外存储、处理客户数据，不得由于客户数据存储位置的改变而改变其司法管辖权。

6.7.10 监管能力

传统计算模式中，用户直接控制、管理自己的数据和业务系统。在云计算平台中，客户的数据及运行过程中生成、获取的数据都在云服务商的直接控制下，客户没有直接的控制权。客户需要通过监管了解和掌握自身数据和业务系统在云计算平台上的状态，了解云计算平台是否提供了足够的安全防护措施满足安全需求。

客户应通过合同明确云服务商的责任和义务，强调客户对数据和业务系统运行状态的知情权；要求云计算平台提供必要的监管接口和日志查询功能，建立有效的审查、检查机制，实现对云计算服务的有效监管。

6.8 形成决策报告

完成对信息和业务的综合分析后，需要形成采用云计算服务的决策报告，经本单位最高领导批准后成为指导采用云计算服务的重要依据。报告应包括但不限于以下内容：

a) 背景描述。描述拟采用云计算服务的信息和业务；
b) 效益分析。从场地、人员、设备、软件、运行管理、维护升级、能耗等方面，对采用本地应用与云计算服务所需费用进行综合分析；
c) 云计算服务模式、部署模式选择。分析客户与云服务商的安全措施实施边界和管理边界；
d) 风险分析。分析数据和业务部署到云计算环境后可能遇到的安全威胁，提出应对措施；
e) 功能需求分析。分析不同模式下的资源需求，数据的备份与恢复能力，备份数据的存储位置，数据的传输方式和网络带宽要求，拟部署到云计算平台上的业务与其他系统之间的数据交互需求等；
f) 性能需求分析。主要分析可用性、可靠性、恢复能力、事务响应时间、吞吐率等指标；
g) 安全要求。基于对准备部署到云计算平台的信息和业务的分类结果，确定云计算服务的安全能力要求；
h) 业务持续性要求。将业务系统迁移到云计算平台后，原有系统可与迁移到云计算平台的业务系统并行运行一段时间；
i) 退出云计算服务或变更云服务商的初步方案；
j) 对客户相关人员进行安全意识、技术和管理培训的方案；
k) 本单位负责采用云计算服务的领导、工作机构及其责任；
l) 采购和使用云计算服务过程中应该考虑的其他重要事项。

7 选择服务商与部署

7.1 云服务商安全能力要求

为客户提供云计算服务的云服务商应具备以下10个方面的安全能力。

7.1.1 系统开发与供应链安全

云服务商应在开发云计算平台时对其提供充分保护，对信息系统、组件和服务的开发商提出相应要求，为云计算平台配置足够的资源，并充分考虑安全需求。云服务商应确保其下级供应商采取了必要的安全措施。云服务商还应为客户提供有关安全措施的文档和信息，配合客户完成对数据和业务系统的管理。

7.1.2 系统与通信保护

云服务商应在云计算平台的外部边界和内部关键边界上监视、控制和保护网络通信，并采用结构化设计、软件开发技术和软件工程方法有效保护云计算平台的安全性。

7.1.3 访问控制

云服务商应严格保护云计算平台的客户数据，在允许人员、进程、设备访问云计算平台之前，应对其进行身份标识及鉴别，并限制其可执行的操作和使用的功能。

7.1.4 配置管理

云服务商应对云计算平台进行配置管理，在系统生命周期内建立和维护云计算平台（包括硬件、软件、文档等）的基线配置和详细清单，并设置和实现云计算平台中各类产品的安全配置参数。

7.1.5 维护

云服务商应维护好云计算平台设施和软件系统，并对维护所使用的工具、技术、机制以及维护人员进行有效的控制，且做好相关记录。

7.1.6 应急响应与灾备

云服务商应为云计算平台制定应急响应计划，并定期演练，确保在紧急情况下重要信息资源的可用性。云服务商应建立事件处理计划，包括对事件的预防、检测、分析和控制及系统恢复等，对事件进行跟踪、记录并向相关人员报告。云服务商应具备容灾恢复能力，建立必要的备份与恢复设施和机制，确保客户业务可持续。

7.1.7 审计

云服务商应根据安全需求和客户要求，制定可审计事件清单，明确审计记录内容，实施审计并妥善保存审计记录，对审计记录进行定期分析和审查，还应防范对审计记录的非授权访问、修改和删除行为。

7.1.8 风险评估与持续监控

云服务商应定期或在威胁环境发生变化时，对云计算平台进行风险评估，确保云计算平台的安全风险处于可接受水平。云服务商应制定监控目标清单，对目标进行持续安全监控，并在发生异常和非授权情况时发出警报。

7.1.9 安全组织与人员

云服务商应确保能够接触客户信息或业务的各类人员(包括供应商人员)上岗时具备履行其安全责任的素质和能力,还应在授予相关人员访问权限之前对其进行审查并定期复查,在人员调动或离职时履行安全程序,对于违反安全规定的人员进行处罚。

7.1.10 物理与环境保护

云服务商应确保机房位于中国境内,机房选址、设计、供电、消防、温湿度控制等符合相关标准的要求。云服务商应对机房进行监控,严格限制各类人员与运行中的云计算平台设备进行物理接触,确需接触的,需通过云服务商的明确授权。

7.2 确定云服务商

7.2.1 选择云服务商

为保证数据和业务安全,客户应选择通过安全审查的云服务商。选择云服务商应考虑但不限于以下方面的因素:

a) 服务模式能否满足需求;
b) 部署模式能否满足需求;
c) 云计算服务的安全能力(一般保护或增强保护)能否满足需求;
d) 定制开发能力能否满足需求;
e) 云服务商对运行监管的接受程度,能否提供运行监管接口;
f) 云计算平台的可扩展性、可用性、可移植性、互操作性、功能、容量、性能等能否满足需求;
g) 云服务商能否满足 5.4 c)的要求;
h) 数据的存储位置,包括数据传输的路径;
i) 灾难恢复能力能否满足需求;
j) 资源占用、带宽租用、监管、迁移或退出服务、培训等费用的计费方式和标准;
k) 出现安全事件并造成损失时,云服务商的补偿能力与责任;
l) 云服务商是否配合对其雇员进行背景调查。

7.2.2 人员背景调查

客户根据信息和业务的敏感程度,确定是否需要对访问数据和业务的云服务商雇员进行背景调查。

7.3 合同中的安全考虑

7.3.1 概述

合同是明确云服务商与客户间责任和义务的基本手段。有效的合同是安全、持续使用云计算服务的基础,应全面、明确地制定合同的各项条款,突出考虑信息安全问题。

7.3.2 云服务商的责任和义务

合同应明确云服务商需承担以下责任和义务:

a) 承载客户数据和业务的云计算平台应按照政府信息系统安全管理要求进行管理,为客户提供云计算服务的云服务商应遵守政府信息系统安全管理政策及标准。
b) 客户提供给云服务商的数据、设备等资源,以及云计算平台上客户业务运行过程中收集、产生、存储的数据和文档等都属客户所有,云服务商应保证客户对这些资源的访问、利用、支配等权利。

c) 云服务商不得依据其他国家的法律和司法要求将客户数据及相关信息提供给他国政府及组织。
d) 未经客户授权，不得访问、修改、披露、利用、转让、销毁客户数据；在服务合同终止时，应将数据、文档等归还给客户，并按要求彻底清除数据。如果客户有明确的留存要求，应按要求留存客户数据。
e) 采取有效管理和技术措施确保客户数据和业务系统的保密性、完整性和可用性。
f) 接受客户的安全监管。
g) 当发生安全事件并造成损失时，按照双方的约定进行赔偿。
h) 不以持有客户数据相要挟，配合做好客户数据和业务的迁移或退出。
i) 发生纠纷时，在双方约定期限内仍应保证客户数据安全。
j) 法律法规明确或双方约定的其他责任和义务。

7.3.3 服务水平协议

服务水平协议(简称 SLA)约定云服务商向客户提供的云计算服务的各项具体技术和管理指标，是合同的重要组成部分。客户应与云服务商协商服务水平协议，并作为合同附件。

服务水平协议应与服务需求对应，针对需求分析中给出的范围或指标，在服务水平协议中要给出明确参数。服务水平协议中需对涉及的术语、指标等明确定义，防止因二义性或理解差异造成违约纠纷或客户损失。

7.3.4 保密协议

可访问客户信息或掌握客户业务运行信息的云服务商应与客户签订保密协议；能够接触客户信息或掌握客户业务运行信息的云服务商内部员工，应签订保密协议，并作为合同附件。

保密协议应包括：

a) 遵守相关法律法规、规章制度和协议，在客户授权的前提下合理使用客户信息，不得以任何手段获取、使用未经授权的客户信息；
b) 未经授权，不应在工作职责授权范围以外使用、分享客户信息；
c) 未经授权，不得泄露、披露、转让以下信息：
   1) 技术信息：同客户业务相关的程序、代码、流程、方法、文档、数据等内容；
   2) 业务信息：同客户业务相关的人员、财务、策略、计划、资源消耗数量、通信流量大小等业务信息；
   3) 安全信息：包括账号、口令、密钥、授权等用于对网络、系统、进程等进行访问的身份与权限数据，还包括对正当履行自身工作职责所需要的重要、适当和必要的信息；
d) 第三方要求披露 c)中信息或客户敏感信息时，不应响应，并立刻报告；
e) 对违反或可能导致违反协议、规定、规程、策略、法律的活动或实践，一经发现，应立即报告；
f) 合同结束后，云服务商应返还 c)中信息和客户数据，明确返还的具体要求、内容；
g) 明确保密协议的有效期。

7.3.5 合同的信息安全相关内容

客户在与云服务商签订合同时，应该全面考虑采用云计算服务可能面临的安全风险，并通过合同对管理、技术、人员等进行约定，要求云服务商为客户提供安全、可靠的服务。

合同至少应包括以下信息安全相关内容：

a) 云服务商的责任和义务，包括但不限于 7.3.2 的全部内容。若有其他方参与，应明确其他方的责任和义务；

b） 云服务商应遵从的技术和管理标准；
c） 服务水平协议，明确客户特殊的性能需求、安全需求等；
d） 保密条款，包括确定可接触客户信息特别是敏感信息的人员；
e） 客户保护云服务商知识产权的责任和义务；
f） 合同终止的条件及合同终止后云服务商应履行的责任和义务；
g） 若云计算平台中的业务系统与客户其他业务系统之间需要数据交互，约定交互方式和接口；
h） 云计算服务的计费方式、标准，客户的支付方式等；
i） 违约行为的补偿措施；
j） 云计算服务部署、运行、应急处理、退出等关键时期相关的计划，这些计划可作为合同附件，涉及的相关附件包括但不限于：
   1） 云计算服务部署方案，确定阶段性成果及时间要求；
   2） 运行监管计划，明确客户的运行监管要求；
   3） 应急响应计划、灾难恢复计划，明确处理安全事件、重大灾难事件等的流程、措施、人员等；
   4） 退出服务方案，明确退出云计算服务时客户数据和业务的迁移、退出方案；
   5） 培训计划，确定云服务商对客户的培训方式、培训内容、人员及时间；
k） 其他应包括的信息安全相关内容。

7.4 部署

7.4.1 概述

为确保云计算服务的部署工作顺利开展，客户应提前与云服务商协商制定云计算服务部署方案，该方案可作为合同附件。如果涉及将正在运行的业务系统迁移到云计算平台，客户还应考虑迁移过程中的数据安全及业务持续性要求。

7.4.2 部署方案

云计算服务部署方案至少应包括以下内容：
a） 客户和云服务商双方的部署负责人和联系人，参与部署的人员及其职责；
b） 部署的实施进度计划表；
c） 相关人员的培训计划；
d） 部署阶段的风险分析。部署阶段的风险可能包括：技术人员误操作导致的数据丢失；业务系统迁移失败无法回退到初始状态；业务系统迁移过程中的业务中断；云服务商在部署过程中获得了额外的访问客户数据和资源的权限等；
e） 部署和回退策略。为降低部署阶段的安全风险，客户应制定数据和业务系统的备份措施、业务系统迁移过程中的业务持续性措施等，制定部署失败的回退策略，避免由于部署失败导致客户数据的丢失和泄漏。

7.4.3 投入运行

客户组织技术力量或委托第三方评估机构对云计算服务的功能、性能和安全性进行测试，各项指标均满足要求后方可投入正式运行。

客户数据和业务系统迁移后，原有业务系统应与迁移到云计算平台上的业务系统并行运行一段时间，以确保业务的持续性。

云计算服务投入运行后，应按第8章的要求加强使用过程中的运行监管，确保客户能持续获得安全、可靠的云计算服务。

8 运行监管

8.1 概述

在采用云计算服务时，虽然客户将部分控制和管理任务转移给云服务商，但最终安全责任还是由客户自身承担。客户应加强对云服务商的运行监管，同时对自身的云计算服务使用、管理和技术措施进行监管。运行监管的主要目标是确保：

a) 合同规定的责任义务和相关政策规定得到落实，技术标准得到有效实施；
b) 服务质量达到合同要求；
c) 重大变更时客户数据和业务的安全；
d) 及时有效地响应安全事件。

8.2 运行监管的角色与责任

8.2.1 概述

客户要按照合同、规章制度和标准加强对云服务商和自身的运行监管，云服务商、第三方评估机构应积极参与和配合。客户、云服务商应明确负责运行监管的责任人和联系方式。

8.2.2 客户的监管责任

客户在运行监管活动中的责任如下：

a) 监督云服务商严格履行合同规定的各项责任和义务，自觉遵守有关政府信息安全的规章制度和标准；
b) 协助云服务商处理重大信息安全事件；
c) 按照政府信息系统安全检查要求，对云服务商的云计算平台开展年度安全检查；
d) 在云服务商的支持配合下，对以下方面进行监管：
   1) 服务运行状态；
   2) 性能指标，如资源使用情况；
   3) 特殊安全需求；
   4) 云计算平台提供的监视技术和接口；
   5) 其他必要的监管活动；
e) 加强对云计算服务和业务使用者的信息安全教育和监管；
f) 对自身负责的云计算环境及客户端的安全措施进行监管。

客户根据运行监管过程中获得的相关材料进行风险评估(客户可以根据自身情况确定是否委托第三方评估机构)，若发现问题则要求云服务商进行整改。若评估结果表明云服务商存在严重问题，不能满足客户需求，客户可以选择退出服务或变更云服务商。

8.2.3 云服务商的责任

云服务商在运行监管中的责任如下：

a) 严格履行合同规定的责任和义务，遵守政府信息系统安全管理政策及标准；
b) 开展周期性的风险评估和监测，保证安全能力持续符合 GB/T 31168—2014，包括：监视非授权的远程连接，持续监视账号管理、策略改变、特权功能、系统事件等活动，监视与其他信息系统的数据交互等；

c) 按照合同要求或双方的约定，向客户提供相关的接口和材料，配合客户的监管活动；
d) 云计算平台出现重大变更后，及时向客户报告情况，并委托第三方评估机构进行安全评估；
e) 出现重大信息安全事件时，及时向客户报告事件及处置情况；
f) 持续开展对雇员的信息安全教育，监督雇员遵守相关制度。

云服务商应按客户要求执行运行监视活动，提供运行监视材料和接口；应按要求提交年度运行报告、重大变更申请和安全事件报告等相关材料；应按客户要求接受第三方评估机构的测评，并及时开展整改工作。

8.3 客户自身的运行监管

8.3.1 概述

客户应将云计算服务纳入其信息安全管理工作内容，加强云计算服务使用过程中对自身的运行监管，主要涉及对云计算服务及业务系统使用者的违规及违约情况、自身负责的安全措施实施情况的监管。

8.3.2 对违规及违约情况的监管

客户应对云计算服务及业务系统使用者进行监管，要求其遵守国家有关信息安全的法律法规、标准及合同要求：

a) 不得向云计算平台和相关系统传送恶意程序、垃圾数据，以及其他可能影响云计算平台正常运行的代码；
b) 不得利用云计算平台实施网络攻击；
c) 不得对云计算平台进行网络攻击，窃取或篡改数据资料；
d) 不得利用云计算平台可能存在的技术缺陷或漏洞破坏云服务商和客户的权益；
e) 不得利用云计算平台制作和传播淫秽、反动和危害国家安全的非法信息。

8.3.3 对安全措施的监管

客户应对其负责的云计算环境及客户端的安全措施进行监管，确保安全措施已实施并正常运行，应监管的安全措施包括但不限于：

a) 监管客户账号，包括管理员账号和一般用户账号，发现任何非法使用客户账号的情况，应在权限范围内处置，必要时通知云服务商；
b) 监管云客户端的安全防护措施，如恶意代码防护、浏览器版本及插件更新、智能移动终端安全加固等；
c) 监管客户在 PaaS 环境中开发、部署应用的安全措施；
d) 监管客户在 IaaS 环境中部署的操作系统、业务系统等安全措施；
e) 由客户或委托第三方评估机构对客户负责实施的安全措施进行安全测评和检查。

8.4 对云服务商的运行监管

8.4.1 运行状态监管

客户通过运行状态监管了解和掌握云服务商及其提供的云计算服务的状态，运行监管内容包括：

a) 安全事件响应；
b) 重大变更处理；
c) 整改记录；

d) 信息安全策略更新；
e) 应急响应计划更新；
f) 应急响应演练；
g) 云服务商委托第三方评估机构的测评。

8.4.2 重大变更监管

客户或委托第三方评估机构评估云计算平台中重大变更可能带来的风险，并根据评估结果确定需要进一步采取的措施，包括退出云计算服务。重大变更包括但不限于：

a) 鉴别(包括身份鉴别和数据源鉴别)和访问控制措施的变更；
b) 数据存储实现方法的变更；
c) 云计算平台中软件代码的更新；
d) 备份机制和流程的变更；
e) 与外部服务商网络连接的变更；
f) 安全措施的撤除；
g) 已部署商业软硬件产品的替换；
h) 云计算服务分包商的变更，例如 PaaS、SaaS 服务商更换 IaaS 服务商。

8.4.3 安全事件监管

在运行监管活动中，客户、云服务商的任何一方发现安全事件，都应及时通知对方，云服务商应及时对安全事件进行处置。安全事件包括但不限于：

a) 非授权访问事件，如对云计算环境下的业务系统、数据或其他计算资源进行非授权逻辑或物理访问等；
b) 拒绝服务攻击事件；
c) 恶意代码感染，如云计算环境被病毒、蠕虫、特洛伊木马等恶意代码感染；
d) 客户违反云计算服务的使用策略，例如发送垃圾邮件等。

9 退出服务

9.1 退出要求

合同到期或其他原因都可能导致客户退出云计算服务，或将数据和业务系统迁移到其他云计算平台上。退出云计算服务是一个复杂的过程，客户需要注意以下环节：

a) 在签订合同时提前约定退出条件，以及退出时客户、云服务商的责任和义务，应与云服务商协商数据和业务系统迁移出云计算平台的接口和方案；
b) 在退出服务过程中，应要求云服务商完整返还客户数据；
c) 在将数据和业务系统迁移回客户数据中心或其他云计算平台的过程中，应满足业务的可用性和持续性要求，如采取原业务系统与新部署业务系统并行运行一段时间等措施；
d) 及时取消云服务商对客户资源的物理和电子访问权限；
e) 提醒云服务商在客户退出云计算服务后仍应承担的责任和义务，如保密要求等；
f) 退出云计算服务后需要确保云服务商按要求保留数据或彻底清除数据；
g) 如需变更云服务商，应首先按照选择云服务商的要求，执行云服务商选择阶段的各项活动，确定新的云服务商并签署合同。完成云计算服务的迁移后再退出原云计算服务。

9.2 确定数据移交范围

从云计算平台迁移出的数据，不仅包括客户移交给云服务商的数据和资料，还应包括客户业务系统在云计算平台上运行期间产生、收集的数据以及相关文档资料，如数据文件、程序代码、说明书、技术资料、运行日志等。应制订详细的移交清单，清单内容包括：

a) 数据文件。每个数据文件都应标明：文件名称、数据文件内容的描述、存储格式、文件大小、校验值、类型(敏感或公开)等。应要求云服务商提供解密方法与密钥，实现加密文件的移交；提供技术资料或转换工具，实现非通用格式文件的移交；

b) 程序代码。针对客户定制的功能或业务系统，在合同或其他协议中明确是否移交可执行程序、源代码及技术资料，可能涉及的内容包括：可执行程序、源代码、功能描述、设计文档、开发及运行环境描述、维护手册、用户使用手册等；

c) 其他数据。根据事先的约定和双方协商，确定应移交的其他数据，包括客户业务运行期间收集、统计的相关数据，如云计算服务的客户行为习惯统计、网络流量特征等资料；

d) 文档资料。客户使用云计算服务过程中提供给云服务商的各种文档资料，及双方共同完成的涉及客户的相关资料。

9.3 验证数据的完整性

客户应对云服务商返还的数据完整性进行验证，为完整获得数据，客户应采取以下措施：

a) 要求云服务商根据移交数据清单完整返还客户数据，特别注意历史数据和归档数据；

b) 监督云服务商返还客户数据的过程，并验证返还数据的有效性。对加密数据进行解密并验证；利用工具恢复专有格式数据并验证；

c) 可通过业务系统验证数据的有效性和完整性，如将数据和业务系统部署在新的平台上运行验证。

9.4 安全删除数据

客户退出云计算服务后，仍应要求云服务商安全处理客户数据，承担相关的责任和义务。客户应采取以下措施：

a) 退出服务后，要求云服务商按合同要求安全存储客户数据一段时间；

b) 通过书面授权，要求云服务商删除客户数据及所有备份；

c) 要求云服务商安全处置存放客户数据的存储介质，涉及以下方面：

1) 重用前应进行介质清理[1)]，不可清理的介质应物理销毁；

2) 要求云服务商记录介质清理过程，并对过程进行监督；

3) 存放敏感信息的介质清理后不能用于存放公开信息。

---

1) 介质清理：指删除介质上数据的过程，该过程不会破坏介质。

GB/T 31167—2014

参 考 文 献

[1] GB/Z 28828—2012 信息安全技术 公共及商用服务信息系统个人信息保护指南

[2] GB/T 29245—2012 信息安全技术 政府部门信息安全管理基本要求

[3] NIST Special Publication 800-145, The NIST Definition of Cloud Computing, September 2011

[4] NIST Special Publication 800-146, Cloud Computing Synopsis and Recommendations, May 2012

[5] NIST Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing, December 2011

[6] AGIMO, Australia. A Guide to Implementing Cloud Services. September 2012

[7] BSI, German. Security Recommendations for Cloud Computing Providers. June 2011

[8] FedRAMP Office. Continuous Monitoring Strategy & Guide. Version1.1, July 27, 2012

[9] FedRAMP Office. Concept of Operations. Version 1.2, July, 27, 2012

GB/T 31167-2014

版权专有 侵权必究

*

书号:155066·1-50121