国家标准GB/T 31167—2014《信息安全技术 云计算服务安全指南》解读与实施

陈兴蜀 罗永刚 罗锋盈 编著

科学出版社

信息安全标准培训教材

国家标准 GB/T 31167—2014 《信息安全技术 云计算服务安全指南》 解读与实施

陈兴蜀　罗永刚　罗锋盈　编著

科学出版社

北京

内 容 简 介

GB/T 31167—2014《信息安全技术 云计算服务安全指南》是我国第一批正式发布的云计算服务安全相关的国家标准之一，本书对其进行解读，介绍标准各项条款的内容、含义及实施途径等，使标准的使用者能理解各项条款的要求，并正确应用标准来保障云计算服务中数据和业务的安全。

本书可供政府部门和重点行业的信息技术管理者、云服务商的管理和技术人员、第三方测评机构以及关注云计算安全标准的研究者和技术管理人员查阅参考。

图书在版编目(CIP)数据

国家标准 GB/T 31167-2014《信息安全技术 云计算服务安全指南》解读与实施 / 陈兴蜀, 罗永刚, 罗锋盈编著. —北京：科学出版社，2014.9
信息安全标准培训教材
ISBN 978-7-03-041969-9

Ⅰ.①国… Ⅱ.①陈… ②罗… ③罗… Ⅲ.①信息安全-安全规程-中国-教材 Ⅳ.①TP309-65

中国版本图书馆 CIP 数据核字（2014）第 217257 号

责任编辑：杨 岭 王 玮 / 责任校对：杨悦蕾 王 玮
责任印制：余少力 / 封面设计：墨创文化

科学出版社出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com

成都创新包装印刷厂印刷
科学出版社发行 各地新华书店经销
*
2014 年 10 月第 一 版 开本：B5 (720×1000)
2014 年 10 月第一次印刷 印张：7 3/4
字数：160 千字
定价：39.00 元
（如有印装质量问题，我社负责调换）

前　言

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*，以下简称标准)于 2014 年 9 月 3 日正式发布。2012 年，国家标准化管理委员会下达了信息安全国家标准制定计划，这意味着该标准的研究与制定正式开始，国标计划号为 20130344-T-469。2011 年年底，牵头单位四川大学先期组织其他编制单位，开始了前期的资料收集与研究；2012 年 3 月，标准编制组在成都正式组建。2014 年 1 月，经全国信息安全标准化技术委员会主任办公会审议通过，形成最终的标准报批稿。该标准的编制组成员在两年多时间的共同努力下，跟踪、研究了大量国内外信息安全技术的最新进展。在制定标准过程中，编制组紧跟学术界、产业界及各国政府发布的最新研究成果，广泛听取来自各方的意见，通过专题会议听取政府部门信息中心负责人、专家、云服务商等的意见。编制组对标准不断地进行修改与完善，先后起草了 4 个版本，征集、处理了近 500 条修改意见。

在此，特向为 GB/T 31167—2014 编制付出辛勤汗水的编制组成员表示衷心的感谢！该标准是编制组成员共同努力的结果，是他们智慧的结晶。他们是四川大学陈兴蜀、罗永刚，中国信息安全研究院有限公司左晓栋、周亚超，中国电子科技集团公司第三十研究所张建军、邬敏华、王强，工业和信息化部电子工业标准化研究院罗锋盈、杨建军、王惠莅，中电长城网际系统应用有限公司闵京华，工业和信息化部电子科学技术情报研究所尹丽波、伍扬，中国电子信息产业发展研究院冯伟，北京信息安全测评中心刘海峰、赵章界，中国科学院信息工程研究所信息安全国家重点实验室卿斯汉，中国移动通信有限公司研究院刘斐、柏洪涛，中金数据系统有限公司黎江、崔玲，华为技术有限公司蒋建平。

特别向为该标准的立项、编制及应用试点给予全程指导与关心，并付出大量精力的全国信息安全标准化技术委员会常务副主任委员赵泽良，以及付出巨大努力的副秘书长胡啸致以衷心的感谢与敬意！向为该标准提出意见、给予帮助与支持的学术界、企业界的专家和领导表示衷心的感谢！

四川大学网络与可信计算研究所的曾雪梅、金鑫、叶晓鸣、王毅桐、陈林等博士为本书的编写付出了辛勤劳动。在本书编写过程中，也得到了工业和信息化部电子工业标准化研究院罗锋盈、王惠莅等的大力支持。正是大家的共同努力，

使得本书能顺利完成，并用丰富的素材、分析对标准 GB/T 31167—2014 进行解读。

GB/T 31167—2014 关注云计算服务的安全管理，是云计算服务安全审查的系列标准之一。为了帮助读者学习和理解 GB/T 31167—2014 标准文本，推进 GB/T 31167—2014 的贯彻与实施，特编写本教材——《国家标准 GB/T 31167—2014〈信息安全技术 云计算服务安全指南〉解读与实施》。

本教材按照 GB/T 31167—2014 的章节顺序进行解读，并给出实施建议，其组成结构如下。

第一章：概述，包括编制背景、适用范围、规范性引用文件、术语和定义，共四节，分别对 GB/T 31167—2014 的引言和第 1～3 章进行解读。

第二章：云计算概述，包括云计算的主要特征、服务模式、部署模式、云计算的优势，共四节，分别对 GB/T 31167—2014 的 4.1～4.4 节进行解读。

第三章：云计算的风险管理，包括概述、云计算安全风险、云计算服务安全管理的主要角色及责任、云计算服务的信息安全管理基本要求、云计算服务生命周期，共五节，分别对 GB/T 31167—2014 的 5.1～5.5 节进行解读。

第四章：规划准备，包括概述、评估效益、分类政府信息、分类政府业务、确定优先级、安全保护要求、需求分析、形成决策报告，共八节，分别对 GB/T 31167—2014 的 6.1～6.8 节进行解读。

第五章：选择服务商与部署，包括云服务商安全能力要求、确定云服务商、合同中的安全考虑、部署，共四节，分别对 GB/T 31167—2014 的 7.1～7.4 节进行解读。

第六章：运行监管，包括概述、运行监管的角色与责任、客户自身的运行监管、对云服务商的运行监管，共四节，分别对 GB/T 31167—2014 的 8.1～8.4 节进行解读。

第七章：退出服务，包括退出要求、确定数据移交范围、验证数据的完整性、安全删除数据，共四节，分别对 GB/T 31167—2014 的 9.1～9.4 节进行解读。

目　录

第一章 概 述

第一节 编制背景

【标准条款】

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。

【条款解读 1】

一、目的和意图

GB/T 31167—2014 的引言简单地说明了本标准的编制背景，简要阐述了云计算的主要优势、对信息安全带来的挑战，以及云计算服务安全管理的必要性、实施步骤与主要目的。

二、解释和示例

2007 年，云计算这一新兴名词风靡 IT 界，国内外掀起云计算研究热潮。国内外研究机构、IT 界商业巨头纷纷迅速投入云计算研究，对云计算发展起到了推波助澜的作用。业界对云计算的定义众说纷纭，各家企业竞相推出各具特色的云计算平台。目前，云计算研究热潮仍在持续，运用机构和企业日益增多。

业界对云计算说法各异，但是有一点是相同的，云计算应该为用户提供方便的、可随时获取的、动态的计算资源。这也正是云计算掀起热潮的根本原因，它为广大用户描绘了一幅极具吸引力的美好蓝图：云计算提供无处不在的计算资源，为用户提供动态的、按需分配的计算资源，用户可以方便地从云计算服务中获取任何需要的 IT 资源。这正是目前广大企业和个人用户急切寻求的简单高效的 IT 解决方案，这种解决方案能够根据需要提供弹性的计算资源，满足用户多样化的需求。

美国政府于 2010 年 12 月 9 日发布了云计算战略，颁布了《改革联邦信息技术管理的 25 点实施规划》，主要内容如下：①从本文颁布之日起的 18 个月内，调整或终止至少 1/3 正在进行的 IT 项目；②确定“云计算优先”战略，每个部门必须在 3 个月之内确定 3 个迁移到云计算平台的 IT 服务，在 12 个月之内完成 1 个服务的迁移，在 18 个月之内保证迁移服务数量达到 2 个；③到 2015 年，至少减少 800 个联邦数据中心(截至 2010 年，美国联邦数据中心已有 1100 个以上)；④对新的 IT 项目进行严格审批，加强项目管理。2011 年 2 月 8 日，美国发布了联邦云计算战略，期望通过云计算来提高联邦信息资源的利用效率，主要内容有：①清楚阐述云计算带来的利益以及需要考虑和权衡的问题；②提供决策框架与案例，以支持政府部门业务向云计算平台迁移；③进一步加强云计算设施的部署力度；④制定联邦政府的行动计划，明确相关部门在加速采用云计算的过程中应采取的行动、应承担的角色和职责。

云计算会带来一些新的信息安全风险。云计算需要采用虚拟化技术、分布式计算、负载均衡等大量技术实现资源的按需供给，只有云计算规模达到“足够”的水平，才能获得规模经济所带来的低成本效益。而庞大且复杂的系统会给信息安全带来不利影响。为了提高资源利用效率、降低资源使用成本，云计算会让不同的客户共享相同的软硬件资源，如在同一台服务器上虚拟化出多个虚拟机供若干客户使用，多个客户共享一台物理服务器的资源(CPU、内存、硬盘、网卡等)，尽管不同的虚拟化软件采用不同的隔离机制，对不同客户的资源采用软件隔离机制，但是软件隔离是否能做到安全隔离目前还没有明确的结论。

云计算为数据保护带来一些特殊困难。客户在采用云计算服务，尤其是社会化的云计算服务时，所需的软硬件资源由云服务商拥有、管理和维护。将数据存放在云计算平台后，客户很难准确得知数据及副本的存储情况、数据及副本(可

能有多个副本)保存在什么位置(包括哪个数据中心、数据中心的地理位置)等信息。客户也很难准确得知客户数据在处理和传输过程中经过哪些链路，例如数据在传输过程中是否经过其他国家等。云服务商可能会采用一些专有的技术或接口保存和处理客户数据，当客户不打算继续采用云计算服务时，如果不能以较低的代价获得数据，则客户可能会面临云服务商提出的各种不平等的条件，甚至被云服务商以数据相要挟。

云计算会给客户业务持续性带来新的问题。与客户自建信息系统不同，客户业务的正常运行需要云服务商持续提供云计算服务，当云服务中断时，客户的业务功能也不得不中断。如果云服务商由于各种原因不再提供客户所需的云计算服务，构建在该云计算服务之上的客户业务也必须中断。在客户自建信息系统的情况下，客户购买了提供商的各种软硬件产品，自己负责运营维护。即使提供商不再提供这些产品或技术支持，客户的信息系统仍然可以正常运行，不会给客户的业务持续性带来重大影响。云计算市场还处于不断发展之中，在此过程中必然会出现云服务商倒闭等情况，因此，客户应首先考虑市场相对成熟的云计算服务。

一个云计算服务将会为大量的客户提供相同的服务，若每个客户在采购该云计算服务时均执行一系列的安全评估，这种重复的评估工作不仅会导致不必要的资源浪费，也会给云服务商带来沉重的负担。因此对于政府部门的客户，应该采用一种统一的方法对云服务商所提供的云计算服务进行安全评估，并将评估结果共享给不同的客户，客户在采购云计算服务时只需要对自身特殊的安全要求进行评估，这样可以大大减少安全评估工作的工作量。

美国为了方便联邦政府部门安全地采用云计算服务，于 2012 年 6 月启动了“联邦风险和授权管理项目”(federal risk and authorization management program，FedRAMP)。FedRAMP 的核心思想是联邦政府统一对计划为联邦政府部门提供云计算服务的云服务商进行安全评估，将评估结果保存到统一的信息库中，联邦政府部门在需要采购云计算服务时，从该信息库中获取评估结果，并根据本部门自身情况添加或删除一些安全需求，再针对自身的特殊安全需求开展安全评估，从而大大减少了联邦政府部门对云计算服务安全评估的重复工作。按照 FedRAMP 的要求①，截至 2014 年 6 月，已有 12 个云计算服务通过了联合授权委员会(Joint Authorizaiton Board，JAB)的认可，5 个云计算服务获得了联邦政府部门的认可。

综上所述，云计算服务可以使客户快速获得所需资源，不需要提前对资源需求作详细规划，让客户将注意力集中到提高业务功能和创新能力上。正是由于云计算能给客户带来巨大的成本效益，因此各国政府、企业等均在积极实施、推进云计算使用计划。但同时还需要看到云计算也带来一些新的安全挑战，比如数据

①FedRAMP 的运行过程可以参考 FedRAMP 发布的相关文档，其官方网络站点为 http：//cloud. cio. gov/fedramp。

保护变得更加困难，客户的业务持续性更依赖于云服务商等。因此，采用云计算服务时需要认真规划、合理安排、加强管理，才能确保客户数据和业务在云计算平台上的安全。

本标准根据采用云计算服务的生命周期，将客户采用云计算服务划分为规划与准备、选择服务商与部署、运行监管、退出服务 4 个阶段。在规划与准备阶段，客户应该首先确定哪些数据与业务已具有使用云计算服务的条件，哪些数据与业务使用云计算服务的条件还不成熟。对于可以使用云计算服务的数据与业务，客户应该首先确定其安全需求。客户制定安全需求时应根据本标准中 6.3 节和 6.4 节的要求确定数据和业务的类型，随后根据本标准 6.6 节的要求确定云计算平台的安全保护要求，不同安全保护强度的云计算平台的安全要求参考标准 GB/T 31168—2014。客户还需要根据自身业务的特点考虑特殊安全要求。当客户确定采用云计算服务后，应该考虑采用通过了安全审查的云计算服务，并与云服务商协商合同细节。选择服务商与部署阶段的主要工作是协商云计算服务采购合同和将数据及业务部署到云计算平台中。客户数据和业务部署到云计算平台后，要通过测试才能正式使用云计算服务。为确保云计算服务在整个服务过程中的安全态势能持续满足客户要求，需要对云计算服务进行运行监管。当客户不再使用云计算服务或需要将数据和业务迁移到其他云服务商的云计算平台时，特别需要注意明确云服务商归还客户的数据范围、数据格式等，为了避免数据泄漏，客户应要求云服务商对保存客户数据的介质进行适当的处理，保证数据安全。

第二节 适用范围

【标准条款】

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，特别是为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。

【条款解读 2】

一、目的和意图

界定 GB/T 31167—2014 的适用范围。

二、解释和示例

GB/T 31167—2014 从涵盖内容和目标对象两个方面界定了其适用范围：

(1)标准将客户采用云计算服务的生命周期划分为 4 个关键阶段，阐述了各阶段需要注意的安全问题以及应采取的技术和管理措施，标准有助于客户明确各个阶段的关键环节，使客户有计划、有步骤地完成云计算服务的采用过程，确保客户数据和业务在云计算环境中的安全。

(2)拟采用云计算服务的政府部门的信息安全人员、管理人员是 GB/T 31167—2014 的主要目标对象，其他目标对象还包括重点行业或企事业单位的云计算服务采购决策人员及信息安全人员、云服务商、第三方测评机构人员、希望了解云计算服务安全和管理的人员等。

社会化的云计算服务的解释参考 P38【条款解读 26】。

第三节 规范性引用文件

【标准条款】

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。凡是标注日期的引用文件，仅所注日期的版本适用于本文件。凡是未标注日期的引用文件，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

【条款解读 3】

一、目的和意图

提供 GB/T 31167—2014 正文中所引用的相关标准或规范性文件的信息。

二、解释和示例

GB/T 31167—2014 列出了三项引用的国家标准，其中：

(1)国家标准 GB/T 25069—2010《信息安全技术 术语》是我国自主制定的信息安全标准，于 2010 年 9 月 2 日正式发布，并于 2011 年 2 月 1 日正式实施。GB/T 25069—2010 界定了信息安全技术领域相关的概念、术语和定义，并明确了各术语词条之间的关系。

(2)国家标准 GB/T 29245—2012《信息安全技术 政府部门信息安全管理基

本要求》是我国自主制定的信息安全标准，于 2012 年 12 月 31 日正式发布，并于 2013 年 6 月 1 日正式实施。GB/T 29245—2012 从适用范围、信息安全组织管理、日常信息安全管理、信息安全防护管理、信息安全应急管理、信息安全教育培训、信息安全检查 7 个方面规定了政府部门信息安全管理基本要求，用于指导各级政府部门的信息安全管理工作以及信息安全检查工作，保障政府机关各部门、各单位信息和信息系统的安全。

(3)国标 GB/T 31168—2014《信息安全技术 云计算服务安全能力要求》在 P1【条款解读 1】中已说明。

第四节 术语和定义

【标准条款】

3 术语和定义

GB/T 25069—2010 中确立的以及下列术语和定义适用于本指导性技术文件。

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。

【条款解读 4】

一、目的和意图

定义术语“云计算”和“云计算服务”。

二、解释和示例

现实生活中，人们打开水龙头就有自来水流出，只需要为消耗了多少水付费，而不用考虑如何建设水厂和管网；需要电时打开电源开关就会有源源不断的电力供应，只需为用了多少电买单，而不用投资建设电力基础设施；将钱交给银行管理，可以避免遗失造成的意外损失和携带大量现金旅行造成的不便。

同供水管网、电力网络、金融系统一样，云计算出现以后，人们需要处理、

保存大量数据时，不需要自购服务器、存储设备，不用再建设自己的数据中心，转而通过互联网等信息网络去利用云服务商的资源，作为消费者，只需要为使用这些资源支付费用；当一个单位需要网站、邮件系统、业务系统时，自己动手完成硬件、软件采购或开发已不是唯一途径，可以通过购买云计算服务等方式将这些工作外包给云服务商。

以上描述以非正式的语言阐述了云计算服务给客户带来的好处，本标准中给出的云计算定义参考了 NIST SP 800－145 *The NIST Definition of Cloud Computing* 和 ISO/IEC 17788 的云计算定义。

云计算定义分几个部分来理解。首先，“定义”强调云计算是一种模式，不是一种技术，也不是一种具体的产品。其次，“定义”对模式进行阐述，即这种模式支持通过网络访问可配置的共享资源池，并且是一种非常方便的、任何地方或任何设备均可通过网络访问资源的方式，访问的资源不是预先静态配置好的，而是根据需要进行“按需”访问。云计算中的资源可以快速供给客户，客户也可以快速释放不再需要的资源，资源供给和释放过程只需要极少的管理工作，客户几乎不需要与云服务商进行人与人的交互，同时可以对不同的资源(如选择 CPU 数量、内存数量、磁盘大小、使用时间等)进行自由组合，体现了云计算的灵活性和自主性。从“定义”中不难看出，方便和动态性是云计算的两个重要特点。也正因如此，很多人将云计算与水电进行对比，此种对比主要体现了云计算的方便之处。但云计算中资源的种类多、形式灵活，云计算服务是云服务商与客户等不同角色在所构成的生态环境中共同相互作用的结果，从这个角度来看，云计算服务比供水系统、银行系统等复杂得多。

云计算服务是云计算的一种资源服务实例。比如华为公司提供的弹性计算云，客户可以通过网页定制每个虚拟主机的 CPU 个数、内存容量、磁盘容量、网络带宽等，可以指定需要的虚拟主机数量、使用时间等。阿里云应用引擎是一款基于弹性扩展的网络应用托管平台，采用多层沙箱保护提供安全运行环境，并且整合多种软件开发常用的扩展服务，帮助开发者快速开发和部署应用程序，将开发者从系统运维、底层技术钻研等工作中解放出来，集中于核心业务的开发和运营。

【标准条款】

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。

【条款解读 5】

一、目的和意图

定义云计算服务中三个关键的角色。

二、解释和示例

在云计算服务过程中，任何提供云计算服务的组织或机构均称为云服务商。直接采购云服务商所提供的云计算服务的组织或机构为客户。客户可以采购多个云服务商提供的云计算服务，经过组合、开发后形成一种新的云计算服务。在此种情况下，与客户直接建立业务和合同关系的云服务商所提供云计算服务的安全不仅依赖于该云服务商，还依赖于该服务商所采购的其他云服务商的云计算服务。

有关云计算客户的角色还存在一些定义。在英文的不同文档中，可以用 customer、tenant、user 三个单词表示“客户”，将这三个单词翻译为中文分别为“客户”“租户”“用户”。在标准 GB/T 31167—2014 中，对“客户”的定义基于以下考虑。

customer 的英文解释为“a person or organization that buys goods or services from a shop or business”，即购买一种商品或服务的一方为客户。对于云计算服务来讲，某个组织或机构需要支付费用才能使用云服务商所提供的服务，因此该组织或机构在本次交易过程中的角色为客户。

在云计算的相关文档中(如 SP 800－144《公有云的安全与隐私指南》)，在介绍资源的共享结构时引入 tenant 这个单词，与 tenant 一同出现的其他词汇有 multi-tenant platform、multi-tenant applications、multi-tenant environment、multi-tenant software architecture 等。由此不难看出，tenant 常在描述技术架构时使用，表示某个应用申请短期占用某个软硬件资源，使用完成后释放这些资源。

user 与云服务商之间没有直接的商务关系。例如某个组织或机构采购了某云服务商的 IaaS 服务，在这些虚拟机之上部署了该组织或机构的门户网站，则访问这些网站的个人为用户。

【标准条款】

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。

【条款解读 6】

一、目的和意图

定义“云计算基础设施”“云计算平台”和“云计算环境”。

二、解释和示例

定义云计算的以上几个术语有两个目的：①方便客户和云服务商之间责任的界定；②方便客户知道能控制的软硬件组件范围。对于管理责任来讲，按照“谁实施，谁负责”的原则，客户和云服务商需要分别承担一定的管理责任。对于控制范围来讲，客户和云服务商均只能对自己拥有的软硬件组件进行控制。

云计算基础设施由云服务商拥有和管理，云服务商具有完全控制权限，云计算基础设施对于客户来讲是不可见的，它包括服务器、网络交换机、路由器、虚拟化软件(如 Xen、KVM 等)，以及这些物理设备和虚拟化软件的管理软件(如 OpenNebula、OpenStack 等)。

云计算平台包括云计算基础设施以及其上由云服务商部署的用于提供云计算服务的软件的集合，如 IaaS 平台、Hadoop 平台、数据库、Web 应用服务器等。云计算平台包括的软件由云计算服务的类型确定，一般来说，提供 SaaS 服务的云计算平台的软硬件集合比提供 IaaS 服务的云计算平台的软硬件集合更加复杂和庞大。

云计算环境包括云计算平台上支撑客户业务的所有软硬件的集合，其中包括客户在云计算平台上部署的特定业务系统的所有软硬件的集合。也就是说，云计算环境包括由云服务商和客户部署的所有软硬件，由云服务商和客户共同管理和负责。

第二章　云计算概述

第一节　云计算的主要特征

【标准条款】

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。

【条款解读 7】

一、目的和意图

阐述云计算具有的主要特征。

二、解释和示例

GB/T 31167—2014 阐述了云计算的 5 个主要特征：

(1)按需自助服务。这个特征表明客户可以通过 Web 或云计算的服务管理接