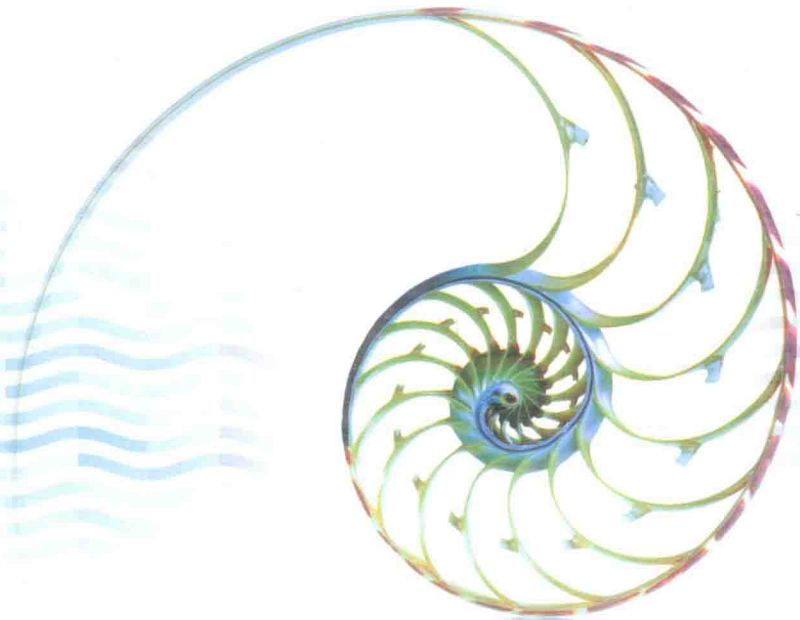
工业和信息化部电子第五研究所　组编



# 云计算信息安全管理
## ——CSA C-STAR 实施指南

◎ 赵国祥　刘小茵　李　尧　编著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

# 云计算信息安全管理

## ——CSA C-STAR 实施指南

工业和信息化部电子第五研究所　组编
赵国祥　刘小茵　李　尧　编著
编写组成员：朱志军　谢灵群　高智伟
张寒坤　朱楠楠　周明轩

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

## 内 容 简 介

本书包括理论篇和实践篇两部分，详细介绍了云计算环境下的信息安全管理指南。理论篇从梳理 Gartner、云计算安全联盟（CSA）、欧洲网络与信息安全局（ENISA）等知名研究组织提出的云计算环境下所面临的安全问题着手，分析总结了现阶段常见的云计算环境下的信息安全风险；同时，对现有的国内外成熟的云计算信息安全管理标准及常见的云计算信息安全管理方法和模型进行了分析，有针对性地提出了 C-STAR 分级模型及评估方法。实践篇从应用和接口安全，审计保证与合规性，业务连续性管理和操作弹性，变更控制和配置管理，数据安全和信息生命周期管理，数据中心安全，加密和密钥管理，治理和风险管理，人力资源，身份识别和访问管理，基础设施和虚拟化安全，互操作性和可移植性，移动安全，安全事件管理、电子证据及云端调查取证，供应链管理、透明性及责任，威胁和脆弱性管理等 16 个方面详细解读了 C-STAR 体系规范中各项条款的内容和含义，同时给出了企业实施落地的实践参考，使 C-STAR 管理体系的建立者能深入理解各项条款的要求，并正确应用相关参考内容建设云计算环境的信息安全管理体系，有针对性地开展云计算安全管理。

本书融通俗性、完整性、实用性于一体，为打算/正在建立云计算信息安全管理体系的企业提供参考，为准备接受 C-STAR 评估的企业提供自我检查的依据，为开展 C-STAR 的评估人员提供技术指导，也可作为云计算工程技术人员、云安全应用研究人员、信息安全从业人员的参考工具书。



**图书在版编目（CIP）数据**

云计算信息安全管理：CSA C-STAR 实施指南/赵国祥，刘小茵，李尧编著；工业和信息化部电子第五研究所组编. —北京：电子工业出版社，2015.10

ISBN 978-7-121-27267-7

Ⅰ. ①云… Ⅱ. ①赵… ②刘… ③李… ④工… Ⅲ. ①计算机网络－信息安全－安全管理
Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2015）第 227493 号

策划编辑：张 榕
责任编辑：夏平飞
印 刷：三河市双峰印刷装订有限公司
装 订：三河市双峰印刷装订有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：720×1 000 1/16 印张：20.75 字数：428 千字
版 次：2015 年 10 月第 1 版
印 次：2015 年 10 月第 1 次印刷
印 数：3 500 册 定价：68.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

# 前言

## <<<<< PREFACE

信息安全是IT领域永恒的话题，在信息技术进入云计算时代后，信息安全仍然是专家、学者、CIO 们热议的话题。行业统计分析显示，传统信息安全领域中有超过 70%的问题是来自于管理不善或者需要管理手段解决的问题，因此，在云计算环境下，对于信息安全问题需要从管理和技术双重角度来分析和管控，一整套体系化的解决方案是必不可少的。

本书编写团队借助国家级科研项目的研究基础以及与 CSA（云安全联盟）合作开发 C-STAR 过程中的积累，希望能将国际上先进的云计算安全管理理念和方法进行深入浅出的解读，以帮助读者快速了解现阶段较成熟、认可度较高的国内外云安全管理方法论。同时，本书也基于 C-STAR 评估内容向云服务提供商提供了体系化云安全管理的指南性解读，在帮助云服务提供商快速建立云计算安全管理体系的前提下也作为工具书帮助企业 CIO、C-STAR 审核员、云服务厂商安全管理员等专业人员对 C-STAR 各控制域进行理解。另一方面，本书也可作为云服务用户在选择云服务供应商时进行安全性的评价之用，帮助云服务用户全面了解云服务环境下常见的安全问题以及需要关注的具体内容。

本书分为理论篇和实践篇，期望能从理论分析的角度帮助读者先进行云计算安全相关背景知识的梳理，再结合全球云计算安全管理相关领域的成熟理念及方法论来帮助读者建立云计算安全管理的基础知识的基础上为读者提供可落地的具体操作指导。

理论篇共分为 4 个章节，通过对比云计算和传统 IT 环境下的信息安全不同关注点，结合对国内外主流的信息安全管理方法和模型的研究分析，针对性地提出了云计算信息安全管理方法和评估模型，为实践篇的内容介绍铺垫了基础知识和背景资料，帮助读者更加深入地理解实践篇的内容。

第 1 章 云计算发展历程，简单回顾了信息技术的发展历程，从发展的角度解释了云计算的出现，并总结了云计算与现有 IT 技术的区别和联系，提炼出了云计算的主要特征，为后续章节做了铺垫。

第 2 章 云计算所面临的安全问题，从云计算领域的龙头企业发生过的信息安全事件分析入手，结合 Gartner、CSA、ENISA 等知名研究组织提出的云计算环境下所

面临的安全问题分析报告，对云计算环境与 IT 环境所面临的信息安全问题进行了梳理和分析，并提出了常见的云计算环境下的信息安全风险。

第 3 章 云计算信息安全管理标准介绍，对现有云计算安全管理相关的标准化进行梳理和介绍，根据云计算安全管理标准化初步呈现的发展趋势为第 4 章的云计算信息安全管理提出参考依据。

第 4 章 云计算信息安全管理方法和模型，本章结合对信息安全管理领域成熟的管理模型/标准（ISMS、CERT-RMM、等级保护、PCI-DSS 等）的研究分析，提出了云计算领域的信息安全管理方法和评估模型（C-STAR），在帮助云服务提供商开展体系化的信息安全管理的同时，为被评估方的云安全管理体系的改进提供方向和指引。评估的结果同样可供云服务使用者评价其云服务提供商的安全管理能力及情况。

实践篇分为 16 章，作为本书的重点部分，根据 C-STAR 的评估内容，针对每一个条款进行深入的分析和解读，力求帮助读者快速理解云计算信息安全管理体系的要求，为打算/正在建立云计算信息安全管理体系的企业提供参考，为准备接受 C-STAR 评估的企业提供自我检查的依据。

第 5 章 应用和接口安全，从数据的完整性、抗抵赖性、应用安全等方面提出应满足的管理的要求。

第 6 章 审计保证与合规性，从审计计划、独立审计、信息系统合规性评价、密码产品的使用、安全产品的使用、选择安全服务商、个人信息安全管理、个人信息保护的评审、个人信息的收集、个人信息的加工、个人信息的转移、个人信息的删除、个人信息安全培训、个人信息投诉与质询、个人信息安全事件处置等方面提出云服务安全管理的审计与合规应满足的要求。

第 7 章 业务连续性管理和操作弹性，从业务连续性计划、业务连续性测试、数据中心条件、信息系统文件、环境风险、设备位置、电力和通信保障、中断影响分析、安全策略和保存策略、数据备份等方面提出了云环境下应满足的 12 条控制要求。

第 8 章 变更控制和配置管理，从系统的开发、变更、测试、交付等方面针对组织内外的变更配置管理等方面提出了云环境下应满足的 7 条控制要求。

第 9 章 数据安全和信息生命周期管理，从数据的分类、标记、管理等方面针对组织的数据安全保护提出了云环境下应满足的 15 条控制要求。

第 10 章 数据中心安全，从物理、技术等方面针对组织的数据中心安全保护提出了云环境下应满足的 10 条控制要求。

第 11 章 加密和密钥管理，本控制域提出了在云环境下使用加密和密钥管理的要求，从授权、密钥生成、敏感数据保护、保存与访问控制等方面提出了具体要求。

第 12 章 治理和风险管理，提出了对云计算安全管理体系的管理框架，包括基准安全要求、数据安全评估、管理监督、管理程序、管理支持/参与、信息安全策略、罚则、风险评估对安全策略的影响、安全策略的评审、风险评估、风险管理框架等要求。

第 13 章 人力资源，对于人员聘用前、中、后环节的关注点提出了管理要求，并结合设备设施的授权使用管理以及重要岗位配备多人并签署专门的保密协议等方面提出了具体要求。

第 14 章 身份识别和访问管理，从“身份识别信息的生命周期管理”和“系统、工具和数据的访问控制管理”两大方面（包含审计工具、验证证书、诊断和配置端口、源码、第三方、身份验证信息、身份凭证、特权程序等方面的访问控制管理以及访问控制策略、访问控制程序、访问权限分离、访问授权管理、访问权限评审、访问权限变更、多因素认证等方面的控制措施）提出了云环境下应满足的 14 条控制要求。

第 15 章 基础设施和虚拟化安全，本章从云计算基础设施环境安全管理的角度提出了需要满足的要求，内容涵盖了审计日志、变更检测、时钟同步、系统文档、脆弱性管理、网络安全、操作系统加固、生产环境隔离、系统隔离、虚拟机安全、Hypervisor 加固、无线安全、恶意代码、审计进程保护、资源控制等方面的内容。

第 16 章 互操作性和可移植性，对于开放式接口、数据和虚拟机的互操作性和可移植性提出具体管理要求。

第 17 章 移动安全，重点针对 BYOD 设备的接入和使用提出了要求。

第 18 章 安全事件管理、电子证据及云端调查取证，提出了在提供云服务的过程中为及时应对信息安全事件，保障云服务的持续提供，需要关注的内容。

第 19 章 供应链管理、透明性及责任，提出对于供应链上下游的管理要求，内容涵盖数据安全、事件通报、供应链协议、第三方评审等环节。

第 20 章 威胁和脆弱性管理，提出了云服务环境下的恶意代码、漏洞/补丁以及移动代码的管理要求。

本书力求全面、深入浅出地阐述云计算安全所面临的问题和风险，通过分析和介绍信息安全管理的成熟标准和模型，提出了云计算环境下的信息安全管理理念和方法，期望能给本书的读者以有用的参考。由于本书编写人员的能力有限，书中难免会有错误和不太合适的地方，请读者不吝赐教，以便我们不断改进。

编　者

2015 年 6 月

# 目录

CONTENTS

## 理论篇

# 理 论 篇

# 第1章

# 云计算发展历程

## 1.1 云计算的出现和发展

自2007年10月8日谷歌和IBM宣布联合加入云计算研究工作以来，云计算对整个IT行业产生了巨大的影响。全球范围内关于云计算的讨论如火如荼，IBM、谷歌、亚马逊等IT巨头纷纷加入云计算的研究和产品生产。各国政府也斥巨资发展云计算，争先恐后地以更快的速度和更强的力度抢占这一先进生产力。

云计算提供的计算资源服务模式可总结为“基于基础设施的安全、共享、可扩展性特点，根据在 Internet 上的计算机环境、应用程序和业务流程的需求来付费[1]的一种形式”。采用这些技术最重要的目的是使得企业能够将资源切换到需要的应用上，根据需求访问计算机和存储系统。好比是从古老的单台发电机模式转向了电厂集中供电的模式。它意味着计算能力也可以作为一种商品进行流通，就像煤气、水电一样，取用方便，费用低廉。

云计算不是突然出现的，是以往技术和计算模式发展和演变的一种结果[2]。从技术架构演进的视角看，云计算为IT领域自1946年2月14日，世界上第一台计算机 ENIAC 在美国宾夕法尼亚大学诞生之后的第三次里程碑式的变革，是对传统计算架构与计算机模式的颠覆与创新。图1-1展示了IT基础设施架构的发展历程。

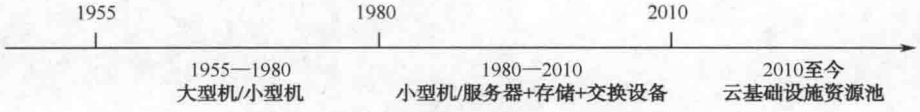



图1-1 IT基础设施架构的发展历程

回顾企业IT基础设施架构演进的整个历史，我们不难看到，第一台计算机诞生后，计算机高度集中化、支持多用户多任务的大型机和小型机是企业 IT 的主流形态，但是构成IT系统的软硬件堆栈各层之间缺少统一的工业标准，呈现出内聚与耦

合的特征，仅少数厂家拥有提供端到端高度复杂化的 IT 系统软硬件的能力[3]。那个时代的 IT 系统造价高昂，往往是少数高端企业才能拥有的“奢侈品”。

1980 年，以 x86 服务器和 PC 系统的诞生为标志，IT 产业迎来了第二次里程碑式的变革，主要表现为从大型机、全封闭的软硬件栈走向了多层次水平分布架构，并且使各层之间的接口标准化、规范化，IT 系统终于走向千家万户。

随着企业信息化进程的不断推进，企业 IT 系统使用者和维护者发现分层架构的弊端逐步显现，企业信息化重心向软件转移，但计算、存储、网络硬件弹性供给的能力及其相互协同的不足，越来越成为软件价值提升的制约性因素。这是因为第二代 IT 系统分层过多，尤其是当今企业软件应用由单一的应用迅速发展成为大规模分布式应用，各层之间集成交付的难度越来越大。现有的服务器、网络、存储等各方面的基础设施资源的协同合作，成为影响企业 IT 快速响应业务需求的制约因素。另外，大部分的资源不能合理地利用，扎堆使用及高峰效应现象等问题导致越来越无法有效地利用资源。

云计算作为 IT 产业第三次里程碑式的变革，它的出现使提供计算能力的方式发生了巨大变化。云计算通过分析已有技术的发展，尤其是虚拟化技术、分布式技术的发展，把所有 IT 基础设施资源都集中到一个数据中心，通过云系统建立一台超级计算机，然后再通过虚拟化和分布式计算技术，把资源按照用户的需求动态地分给每个用户。使得建成的超大规模“云计算机”像发电厂一样，多用户可以从这座“电厂”中随时地获取所需要的计算资源。云计算通过按需计费的方式付费，就像生活中用电一样，用户无须考虑是如何“发电”的，也不用担心“电力”调配、维护、更新问题。集中管理的方式不但节省了资源，提高了资源利用率，而且大大地提高运算能力，带来更好的用户体验。

## 1.2 云计算与传统 IT 的联系

通过观察一些技术的发展，尤其是在互联网技术（Web 2.0、Web 服务）、分布式计算技术（效用计算、网格计算）和大规模资源管理技术（资源虚拟化、数据中心管理技术）方面，可以有助于我们了解云计算的发展[4]。图 1-2 显示了上述技术领域的融合，极大地推动了云计算的发展。

### 1.2.1 云计算与网格计算的关系

网格计算是信息技术发展的一个重要标志，网格计算的目的是实现互联网上所有资源的全面共享，包括计算资源、存储资源、通信资源、软件资源、信息资源

等，任何人都可以作为请求者使用其他节点的资源，任何人都需要贡献一定的资源给其他节点。

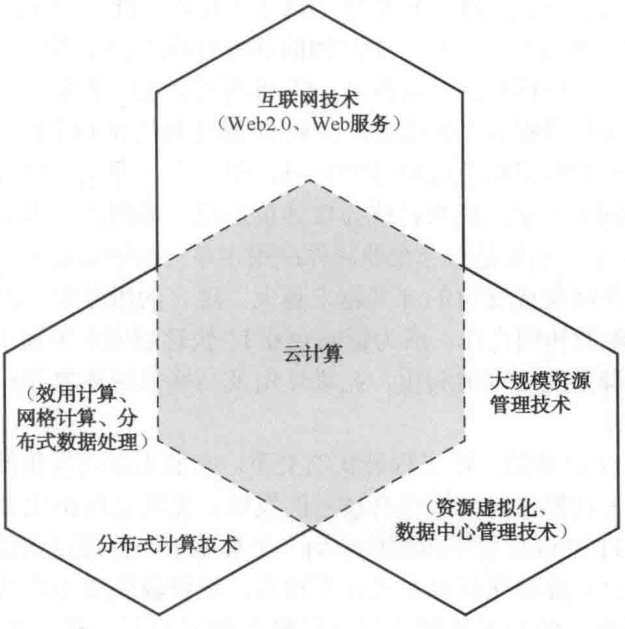



图 1-2　云计算与相关技术的关系

但是在网格计算使用过程中会遇到一些问题，如对资源的可用性与软件的不同配置，包括不同的操作系统、库、编译器、运行环境等。同时，用户的应用往往只能运行在特定的环境中。因此，网格基础设施上常常存在可移植性障碍，从而约束用户在效用计算环境中使用网格。然而，虚拟化技术可以完美地解决网格在效用计算环境中遇到的问题，又为云计算的发展推进了一步。

与云计算相比，网格计算强调将工作量转移到远程的可用计算资源上。云计算强调专有，任何人都可以获取自己的专有资源，并且这些资源是少数团体提供的，用户不需要贡献自己的资源。在云计算中，计算资源被转换形式去适应工作负载，它既支持网格类型应用，也支持非网格环境。网格计算侧重并行的计算集中性需求，并且难以自动扩展。云计算则侧重事务性应用，大量单独的请求，可实现自动、半自动的扩展。

网格计算的构建大多为完成某一特定的任务需要或者支持挑战性的应用。而云计算一般来说都是为了通用应用而设计的。云计算在初始阶段就支持广泛企业计算、Web 应用，普适性更强。网格计算的主要思路是聚合分布的松散资源，而云计算的 IT 资源相对集中，以 Internet 的形式提供底层资源的获得和使用。云计算与网格计算的比较如表 1-1 所示。

表 1-1 云计算与网格计算的比较

| 网格计算 | 云计算 | 网格计算 | 云计算 |
|---|---|---|---|
| 异构资源 | 同构资源 | 松耦合问题 | 紧耦合问题 |
| 不同机构 | 单一机构 | 免费（政府支付） | 按量计费 |
| 虚拟组织 | 虚拟机 | 标准化 | 尚无标准 |
| 科学计算为主 | 数据处理为主 | 科学界 | 商业社会 |
| 高性能计算机 | 服务器/PC | | |

## 1.2.2 云计算与对等计算的关系

对等计算（P2P）是一种分散的、非集中化和自组织的分布式系统，利用分布式资源进行关键性的应用。人们可以直接链接到其他用户的计算机以便交换文件，而不像过去那样链接到服务器去浏览与下载。在这种模式下，不存在服务器与客户端的差异，网上的所有节点都可以“平等”共享其他节点的计算资源。对等计算的核心思想是所有参与系统的节点（互联网上某个计算机）处于完全对等的地位，没有客户机和服务器之分，也就是说每个节点既是客户机，也是服务器。既向他人提供服务，也享受来自他人的服务。

对等计算的优势是集合大量计算机，大大地提高了计算能力，同时，使用空闲计算时间，降低成本。对等计算的劣势：（1）用户注意力有限，不可能有大量类似的活动；（2）单元之间相互独立；（3）不稳定的计算能力，需要不断推动用户参与。

对等计算与云计算的比较如表 1-2 所示。

表 1-2 对等计算与云计算的比较

| 比较 | 对等计算 | 云计算 |
|---|---|---|
| 不同点 | 对等计算是 CPU 高度密集型的，相对于计算时间而言，其传输时间微不足道。因此，P2P 计算贡献的是 CPU 周期，而不是带宽 | 云计算是 CPU 和带宽高度密集型的。云计算的作业在一个聚集很高带宽的数据中心运行 |
| | 对等计算是在接入互联网的不可信的计算机上运行，这些计算机的网速不高，而且数据也不在本地 | 云计算是在高带宽的高性能数据中心的可信任的专用硬件设备上运行 |
| 相同点 | 将问题分为独立的块，然后进行并行计算 | |

## 1.2.3 云计算与集群计算的关系

集群的一个常用用途就是在一个高流量的网站中实现负载均衡。一个网页请求被送到“管理者”服务器，然后此服务器决定此请求由几个相同 Web 服务器中的哪

一个进行处理，从而能够提升通信量和处理速度。集群计算主要有以下几个特点。

（1）集群技术支持混合平台工作模式，体系结构上可以同时支持精简指令集计算机（Reduced Instruction Set Computer）和英特尔结构（Intel Architecture）节点，操作上可以同时支持 Windows Server、Linux 和 UNIX 操作系统。

（2）集群技术具有统一的系统监控和管理功能，可以简单直观地监控整个集群的软硬件运行状态，同时通过集群的主机入侵检测系统保障系统的安全性。

（3）集群技术的架构具有优异的动态扩展性，可以根据用户的需要随时增加新的节点，而不必改动整个系统。

（4）集群服务器节点可以根据不同需要，灵活地进行调整和配置，承担不同的应用服务、计算任务或通过软件管理协同处理某一特定的任务。

云计算与集群计算的区别与联系如表 1-3 所示。

表 1-3　云计算与集群计算的区别与联系

| 比　较 | 集群计算 | 云　计　算 |
| --- | --- | --- |
| 区别 | 集群计算局限于某个领域，是为了解决计算能力不足的问题而创建的，因为通常局限于 LAN 范围内，不适用于不同领域参与者之间的资源共享 | 云计算能提供更为广泛的、域内、域间的通信以及资源的共享 |
| | 集群中的节点是集中控制的，而且集群管理器知道每个节点的状态 | 云计算是分布式控制的 |
| 联系 | （1）集群计算是云计算的一个不可缺少的子集，集群计算可以构成私有云，它是规模更大的云计算的基础；<br>（2）集群问题能够减少更高一级云计算必须解决的问题的数目；<br>（3）集群计算使用资源和软件来实现组合单元的外部特性，这些特性影响它的使用或到更大的云计算中集成 | |

## 1.2.4　云计算与资源虚拟化的关系

虚拟化技术对云计算的发展起到了关键性的作用。虚拟化技术可以增大硬件空间，简化软件的重新配置过程。虚拟化的目的是实现高效的资源利用率，提高系统可扩展性和工作负载能力，同时通过将底层物理设备与顶层应用分离，实现计算资源的灵活性。虚拟化减弱了用户与资源之间的关联性，使用户不再依赖于资源的某种特定方式而实现。虚拟化技术的特点如图 1-3 所示。

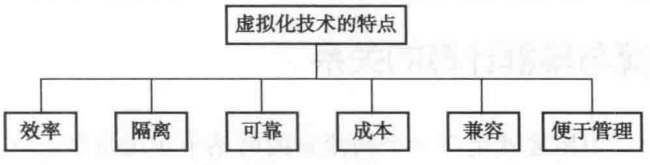



图 1-3　虚拟化技术的特点