·云计算实践指南丛书·

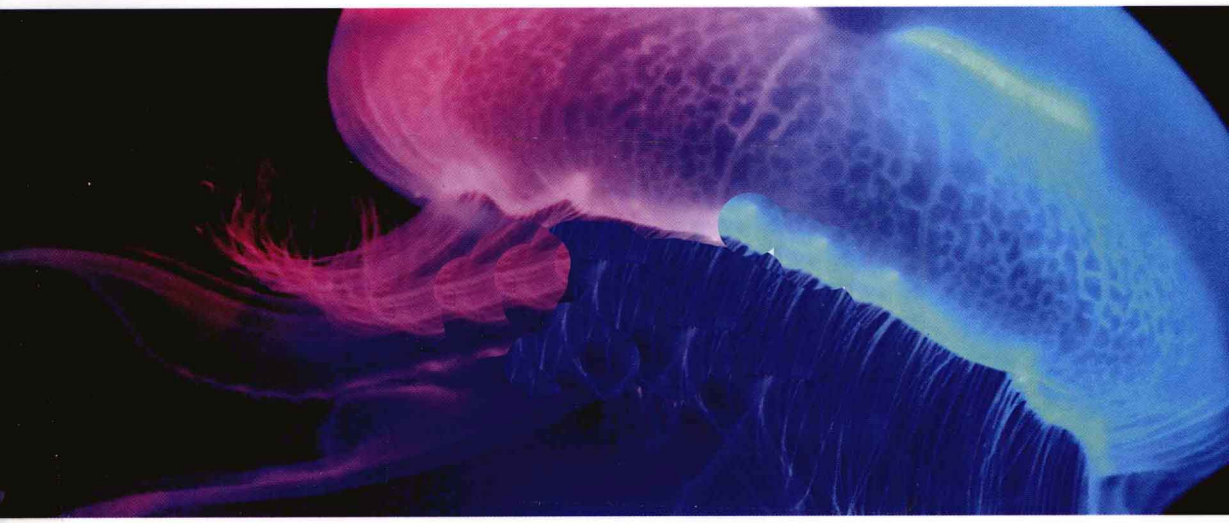
Broadview
www.broadview.com.cn

首次推出国内云计算安全原创著作！

# 云计算安全

## 技术与应用

中国电信网络安全实验室 编著



简单 透明 灵敏 强悍

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

·云计算实践指南丛书·

# 云计算安全

## 技术与应用

**编委** 胡乐明 冯 明 唐 宏

**著者** 中国电信网络安全实验室
金华敏 沈 军 汪来富 何 明 王 帅
刘国荣 罗志强 余晓光 刘东鑫 樊 宁

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

## 内 容 简 介

国内第一本云计算安全原创著作，全面了解云计算安全风险、安全防护手段的佳作。

在享受云计算便利服务的同时，如何保障隐私不被侵犯？信息不被窃取？云计算是否给技术安全领域带来了福音？

本书集合中国电信网络安全实验室多年的业内研究和实践经验，深入浅出地探讨了云计算应用安全体系及关键技术，勾画出云计算应用安全防护架构，提出安全防护建设最佳实践；同时，本书创新性地诠释了安全云服务的定义和特征，引入了面向业务应用模式的安全云服务层次模型全新理念，并分析了安全云服务的技术实现、实施、部署和应用实践。



**图书在版编目（CIP）数据**

云计算安全：技术与应用 / 中国电信网络安全实验室编著. —北京：电子工业出版社，2012.2
（云计算实践指南丛书）
ISBN 978-7-121-14409-7

Ⅰ. ①云… Ⅱ. ①中… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 169264 号

责任编辑：刘 皎
印 刷：北京市顺义兴华印刷厂
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：720×1000 1/16 印张：14.75 字数：236.5 千字 彩插：1
印 次：2012 年 2 月第 1 次印刷
印 数：4000 册 定价：59.00 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。

# 序 言

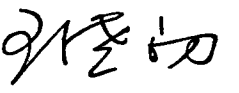
云计算是继个人计算机、互联网之后的第三次信息化革命，越来越多的国家把云计算产业的发展提升到了国家战略高度，我国十二五规划也将云计算列入重点扶植的战略新兴产业。云计算作为计算机技术和互联网技术融合发展的产物，不仅仅实现了IT技术的革新，更是IT商业模式和服务模式的一次重大革命。云计算技术的应用，缩小了中小企业和大企业的IT应用差距，甚至能让每个人都能以极低的成本获得顶尖的信息技术和服务，这种创新的计算模式和商业模式将给信息产业带来前所未有的深刻变革。

随着云计算技术应用的进一步深入，云安全也成为业界关注的焦点。云计算市场规模的迅速扩大，使得其将成为类似水电、煤气的公共基础设施，使用云计算服务的政府机构、企业和个人，其数据与信息安全将严重依赖于云计算服务提供系统的保密性和安全性，这给国家信息安全、企业安全和个人隐私保护带来了前所未有的挑战。云安全不仅是广大用户选择云计算服务的首要考虑因素，也是云计算实现健康可持续发展的基础。

中国电信在聚焦信息化服务、大力发展云计算的同时，对云安全问题也高度重视，在云安全核心技术研究、云安全商用试验方面积极探索、稳步实践，积累了宝贵的研究成果和安全运营经验。

《云计算安全：技术与应用》正是中国电信网络安全实验室多位安全专家近几年来在云安全技术研究和实践经验的基础上，结合国内外云安全最新发展动态写作而成。该书对云安全的基本概念、云计算面临的安全威胁、云计算应用安全防护技术、安全云技术进行了深入的剖析，并对业界最新云计算安全实践和应用案例进行了系统介绍和客观分析，具备很强的实践性。书中深入的技术剖析和丰富的实践成果对于广大云计算研发人员和云计算使用者都极具参考价值。

希望本书的出版，能够让广大读者对云安全有更为深入的理解和认识，并将相关技术及理念积极应用到相关的云计算实践中去，共同推动和提高我国云计算应用的整体安全水平，为我国云计算产业的发展做出应有的贡献。



**中国电信集团公司总经理**

# 专家推荐 1

Securing cloud computing is a global issue, and a shared responsibility between providers, customers, governments and innovators alike. This book is an important contribution to the best practices of cloud security and should be read carefully by anyone with a cloud in their future.

Jim Reavis

Executive Director, Cloud Security Alliance

# 专家推荐 2

当前云计算业务和技术迅猛发展，获得了从政府、产业界到学术界的广泛关注和投入，云计算应用中的安全问题也日益成为人们关注的重点。国内外很多专业技术机构和组织都开展了云计算安全学术和标准方面的研究和教育工作，例如云安全联盟 CSA 于 2010 年发布了云安全指南，为业界提供了一份重要参考。但是，尚缺乏能够从产业和工程角度对云计算安全进行深入研究并提供指导的著作资料。《云计算安全：技术与应用》是中国电信网络安全实验室多位安全专家在近几年的技术研究和应用实践的基础上写作而成，向业界分享了中国电信在云计算安全领域的丰硕研究成果和实践经验。

该书系统而又深入地阐述了云计算发展面临的各方面安全问题及相应的安全技术、方案和最佳实践，可为云计算的从业人员深入了解云计算安全理念、安全技术手段，以及提高云计算安全等级等提供技术指导和实践指南；同时，该书中介绍了很多云计算安全应用案例，对于广大非专业的云计算服务用户及潜在用户而言，也极具参考价值。

该书紧扣云计算安全技术与应用前沿，观点鲜明，内容详实，实践性强，是一部指导行业内云计算安全发展和应用的力作。我相信这本书会使很多读者受益，也希望本书的创作团队能在云计算安全技术的发展中不断分享新的研究成果和心得体会。

赵粮

CSA 中国分会理事

# 前 言

全球信息化进程不断加快，新一代信息技术日新月异，社会发展对信息服务的需求持续增长，已成为促进新一代信息技术产业发展的根本动力。继个人计算机、互联网变革之后，云计算作为第三次信息化浪潮的代表正在向我们走来，给人类生活、生产方式和商业模式带来根本性改变。云计算作为一种基于互联网，动态、可伸缩且以按需服务方式提供计算资源的全新计算和商业模式，不仅是技术革新驱动商业模式变革的产物，也是用户需求驱动的结果，这种创新的计算模式和商业模式将给整个信息产业带来前所未有的深远变革。

伴随着云计算市场规模快速扩大，成熟产业链正在形成之中，而安全仍然是云计算无法回避的重要话题。由于云计算系统规模巨大，承载了诸多用户隐私数据，以及前所未有的开放性和复杂性，使其安全性面临比传统信息系统更为严峻的挑战。从某种意义上讲，如何解决好其中的安全问题，是关系到云计算产业发展的关键。云计算的便利性和安全性随行相伴，云计算的发展使得网络计算超越了原有的物理界限，在促进诸多商业服务模式发展的同时也带来了严峻的安全挑战，安全性和隐私保护是当前用户评估采用云计算时最重要的考量因素。

当前我国一些地区发展云计算产业的热情高涨，出台了产业发展规划、行动计划，力图服务于本地区经济的发展。但也存在着需求不明确、盲目发展的问题，从而带来了严重的信息安全、信息监管方面的隐患，亟待加强规范和引导。因此，需要未雨绸缪，通过加强技术研发，健全法律法规等手段，不断完善云计算自身安全，以及云计算信息安全及隐私保护等问题，为云计算发展营造良好环境。

鉴于目前在国内云计算的概念及应用理念已被广泛接受，但人们对于云计算面临的安全风险、云计算安全体系架构、云计算应用安全防护关键技术，以及云计算安全运营要求等方面的内容了解较少，国内目前也鲜有系统性的资料可供参考。因

此，我们编写了这本《云计算安全：技术与应用》，本书作为国内一本系统性介绍云安全的图书，阐述了云计算发展面临的安全问题及相应的安全技术、方案和最佳实践，为云计算的从业人员、使用者、潜在客户全面了解云计算安全风险、安全防护手段提供指南。

本书创新性地将云安全划分为云计算应用安全和安全云，即云计算应用自身的安全和云计算在安全领域的应用。在云计算应用安全方面，本书从技术、管理、法律、用户等多维度系统分析了云计算面临的安全挑战，深入浅出地探讨了云计算应用安全体系及关键技术，全面勾画了云计算应用安全防护架构，并针对目前热点的云计算应用实例提出了安全防护建设最佳实践。在安全云方面，本书从全新的视角诠释了安全云服务的定义和特征，引入面向业务应用模式的安全云服务层次模型的全新理念，深入探讨了安全云服务的技术实现、实施、部署和应用实践。

第 1 章在概要介绍云计算技术及理念的基础上，结合云计算的安全案例，对云计算带来的安全问题进行剖析，给出云计算安全的内涵，让读者对云安全有一个初步的整体认识。

第 2 章从技术、管理和法律等角度全面分析了云计算面临的安全挑战，并分别从个人用户、企业用户和云服务提供商的角度分析其所面临的安全风险，最后，从国家安全的战略高度，阐述了云计算对我国信息化进程带来的安全挑战。

第 3 章主要从云计算的应用模式、支撑性安全基础设施建设的角度，提出云计算应用安全体系，并对其中的身份认证与访问控制、数据加密与密钥管理等关键技术进行介绍。

第 4 章从云计算核心架构安全、云计算网络与系统安全防护、数据与信息安全，以及身份管理和安全审计四个层面系统阐述云计算应用的安全防护方案；并针对公共基础设施云和私有云分别提出安全防护策略应用建议。

第 5 章主要对云计算迁移过程中的相关应用流程和关键问题进行了系统梳理，包括迁移前的风险评估、迁移的主要步骤，以及迁移后的安全管理，并对典型的迁移场景进行了介绍。

第 6 章以业界当前应用较为广泛的云主机、云存储为例，从网络安全、虚拟机

安全、数据安全、运营管理安全等方面探讨了如何进行云计算应用的安全防护建设。

第 7 章从全新的视角诠释了安全云服务的定义和特征，引入面向业务应用模式的安全云服务层次模型的理念，深入探讨了安全云服务的技术实现、实施、部署方式和应用策略。

第 8 章介绍安全云应用实践，阐述了安全云服务提供商和设备提供商在安全云应用中使用的各种技术解决方案，让读者能够更深入了解云计算技术在网络安全领域的具体应用。

第 9 章介绍云安全的业界动态，主要涉及当前研究云安全的国内外标准组织，业界知名的云安全厂商及其主要安全产品，使读者能够对当前的研究热点、技术发展动态有较为全面的了解。

本书大部分内容和应用案例来自于作者的实践经验和研究成果，并参考了大量的业界研究成果和相关技术资料；同时，本书的写作得到了中国电信集团公司和中国电信广州研究院的鼎力支持，在此一并表示感谢。

本书由中国电信网络安全实验室的金华敏、沈军、汪来富、何明、王帅、刘国荣、罗志强、余晓光、刘东鑫、樊宁等多位作者联合编写。由于作者水平有限，书中难免存在谬误之处，欢迎各位读者批评、指正。

# 目 录

# 第1章

# 云计算安全概述

云计算是当前发展十分迅猛的新兴产业，被认为是继微型计算机、互联网后的第三次 IT 革命，是互联网发展的大趋势。它不仅是互联网技术发展、优化和组合的结果，也为整个社会信息化带来了全新的服务模式，为形成信息化经济时代基于访问权的商业模式提供了可能，将对人类社会生活带来重大变革。现在，越来越多的国家把云计算发展提升到了国家战略层面，我国也将云计算作为新一代信息技术列为十二五规划重点扶植的战略新兴产业，各级政府和社会各界对此均高度重视并开始积极探索。

鉴于云计算在信息化进程中的战略地位，云计算安全的重要性也不言而喻，它不仅是广大用户选择云计算应用时的首要考虑因素，是云计算实现健康可持续发展的基础，也是网络安全领域新的探索。充分考虑并加强云计算安全不仅能增强用户对云计算服务的信心，促进云计算市场的成熟和发展，也能极大推动网络安全领域技术和应用的发展。本章将首先对云计算概念、架构及应用发展进行简略介绍，然后通过近期业界云计算应用典型安全案例分析云计算安全所带来的影响及面临的安全威胁，最后引申并总结出云计算安全的内涵。

## 1.1 云计算基础

### 1.1.1 云计算的定义和特征

从并行计算、分布式计算、网格计算、普适计算到云计算，整体计算技术的不断发展推动了整个互联网技术和应用模式的演变，互联网已进入一个全新的云计算时代。但在全世界“云计算热”的今天，对于“云计算究竟是什么”业界并没有达成共识，不同机构赋予云计算不同的定义和内涵，造成目前众说纷“云”的局面。以下给出几个较典型的云计算定义：

美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）认为，云计算是一个模型，这个模型可以方便地按需访问一个可配置的计算资源（例如，网络、服务器、存储设备、应用程序，以及服务）的公共集。这些资源可以在实现管理成本或服务提供商干预最小化的同时被快速提供和发布。