Computer Science and Application 计算机科学与应用, 2015, 5, 83-91
Published Online April 2015 in Hans. http://www.hanspub.org/journal/csa
http://dx.doi.org/10.12677/csa.2015.54011

Hans汉斯

Study on Security Inspection and Evaluation Service System Orienting Telecom Operators' Cloud Computing Platform

Jin Cheng[1], Jia Liu[2], Luzhong Fang[1]

[1]China Electronics Cyberspace Great Wall Co., Ltd., Beijing
[2]China Transport Telecommunications & Information Center, Beijing
Email: boonbreath@126.com

Received: Apr. 15th, 2015; accepted: May 3rd, 2015; published: May 8th, 2015

Abstract

With the continuous development of cloud computing technology, information security has become increasingly prominent, which has become the bottleneck restricting the cloud computing technology's application development. Through the analysis of telecom operators' cloud computing platform architecture, this paper analyzes the security threats to cloud computing, and elaborates security detection indicators from multiple angles in cloud computing based on security system architecture and application security requirements. Finally, we propose the security inspection and evaluation service system of telecom operators from perspectives of cloud security, cloud management, cloud consulting and planning, etc.

Keywords

Cloud Computing, Cloud Security, Virtualization, Security Inspection Evaluation, Classified Protection

面向电信运营商云计算平台的安全检测评估服务体系研究

成　瑾[1]，刘　佳[2]，方禄忠[1]

[1]中电长城网际系统应用有限公司，北京
[2]中国交通通信信息中心，北京
Email: boonbreath@126.com

收稿日期：2015年4月15日；录用日期：2015年5月3日；发布日期：2015年5月8日

摘　要

随着云计算技术的不断发展，信息安全问题日益凸显，已经成为制约云计算技术应用发展的瓶颈。文章通过分析电信运营商云计算平台的架构，分析云计算平台面临的安全威胁，并在安全系统架构和应用安全需求基础上，从多个角度阐述云计算领域的安全检测评估指标。最后，从云安全、云管理、云咨询规划等多个层面提出了构建电信运营商级云计算平台的安全检测评估服务体系。

关键词

云计算，云安全，虚拟化，安全检测评估，等级保护

1. 引言

随着云计算技术的不断发展，以及相关技术标准和法律法规的不断健全完善，云计算已经走下“云端”，给工作、生活、生产方式和商业模式带来了根本性改变。从 Google、IBM、Microsoft、Amazon 等国际 IT 和商业巨头以不同领域和角度开始在“云计算”领域扎根，到国内的“移动大云”、“联通悦云”、“电信天翼云”、“阿里云”、“智慧城市”等云计算服务平台的运营，高效便捷的“云”IT 专业化服务也促使政府、行业、企业组织等大力开展“造云计划”。

云计算源于网络运营商的商业运作，是网格计算(Grid Computing)、并行计算(Parallel Computing)、分布式计算(Distributed Computing)、效用计算(Utility Computing)、虚拟化(Virtualization)、网络存储(Network Storage Technologies)、负载均衡(Load Balance)以及 IaaS (基础设施即服务)、PaaS (平台即服务)、SaaS (软件即服务)等技术融合演进并跃升的结果。云计算将大量计算资源、存储资源与软件资源链接在一起，形成巨大规模的、动态的、易扩展的共享虚拟 IT 资源池，通过高速互联网将数据处理过程传送给虚拟机的计算机集群资源的计算方式。云计算实质上是一种基础架构设计的方法论创新，由大量的计算机资源组成共享的 IT 资源池，云计算模式在信息处理、信息存储和信息共享等方面具有显著优势，将动态创建高度虚拟化的应用服务和数据资源提供给用户。未来的网络将向融合(Single)、扁平(Flat)、软通信(Softcom)方向演进，而云计算技术将是处理、控制的重要技术。网络层的“IP + 光”，业务的可编程、承载和控制解耦，应用和内容集中化管理等，都将通过云计算平台实现。因此，云计算的关键能力体现在架构、软件、算法、面向应用的系统定制和集成，电信运营商承载的以数据中心为特征的云计算平台也随之成为应用、运营、管理的核心。

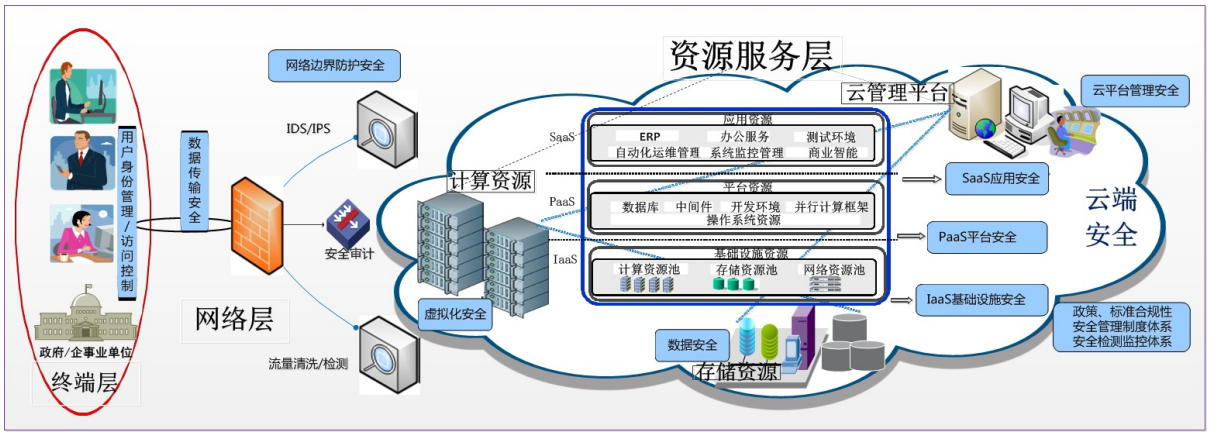
电信运营商的 IT 基础设施庞大，网络资源丰富，用户多，资金雄厚，在云计算发展中具有独到优势。随着云计算技术的不断成熟和 3G、HSPA+、LTE 等移动互联网技术的发展，以及无线和有线网络的深度覆盖，为云计算奠定了良好的承载基础。三大运营商对云计算的关注和重视程度相当，提出更符合自身发展的清晰的战略目标，中国移动着眼于业务支撑云服务；中国电信着眼于全面开花、重在 IaaS；中国联通着眼于眼前的业务模式延伸与升级。三大运营商也各自推出了云服务平台：移动大云，联通沃云，

电信天翼云。在多个专业领域从不同程度、不同方向上进行了云计算产业的实施工作，如大规模投资云计算基地的和云计算数据中心的建设；云主机、云存储、云应用等产品的推广；在深入结合行业应用的背景下，各种行业云如金融云、医疗云、交通云等已开始了服务[1]。虚拟主机托管和弹性计算资源出租等 IaaS 业务，成为多数运营商进入云服务领域的首要选择，AT&T、英国电信、德国电信等运营商都采取了类似的发展策略。未来，运营商将在逐步完善 IaaS 服务的基础上，发展 PaaS 能力和 SaaS 能力，将云服务演进成完整的生态系统。

由于云计算信息系统是在传统互联网信息系统的基础上发展起来的新的系统应用模式，涉及个人和企业运算模式的改变，涉及个人和企业的敏感信息，因此云计算面临的第一个重要问题就是云计算的安全。云计算平台不仅要面对传统信息系统的安全威胁，还将面临新的安全问题。云计算安全问题日益突出，已经成为制约云计算技术应用全面推广的主要因素。亚马逊“云震”等云安全事件也促使了对云计算应用安全风险的正视和反思。因此，鉴于电信运营商在云计算应用和发展过程中的重要地位，有必要将电信运营商级的云计算平台建设、检测、监管纳入到国家信息系统安全监管体系范围中来，建立和落实全面的安全检测评估服务体系，将更加有利于云计算平台应用的发展[2]。

本文将通过分析电信运营商云计算平台的架构，分析云计算平台面临的安全威胁，并在安全系统架构和应用安全需求基础上，从多个角度阐述云计算领域的安全检测评估指标。最后，从云安全、云管理、云咨询规划等多个层面提出了构建电信运营商级云计算平台的安全检测评估服务体系。

2. 电信运营商云计算平台安全体系层级结构



采用云计算技术的信息系统体系结构可分为三部分：终端层、网络层、资源服务层。

1) 终端层：主要包括电脑、手机、pos 机等各类智能终端设备上运行的应用程序。在通过用户身份验证和访问控制后，应用程序能够访问资源服务层提供的各类服务和共享数据，无需在本地工作站或服务器上进行数据的计算和存储。

2) 网络层：主要包括各种终端设备传输使用的有线和无线网络所组成的数据传输体系，以及各个网络传输节点上部署的网络通信设备和边界安全防护设备。网络层是云计算信息系统提供服务的基础设施，也是信息系统安全体系建设的重要环节。

3) 资源服务层：是由虚拟化、分布式计算、海量数据存储和管理、负载均衡等多种信息技术融合应用的资源服务集群。云计算信息系统通过资源服务层实现用户的统一认证、海量信息数据的并行处理、海量数据的存储及共享、统一监控和安全审计等应用服务。通过云计算的三种服务模式——SaaS (软件即服务)、PaaS (平台即服务)和 IaaS (基础设施即服务)为终端用户提供各类应用服务。电信运营商也将会把

安全资源像计算、存储等一样实现资源池化，按客户需求将安全作为一种资源提供给用户[3]。

从云计算信息系统体系结构分析，电信运营商云计算平台也将面临着终端安全、网络安全、应用安全、虚拟化安全和数据安全等层面的安全威胁和挑战[4]。

3. 电信运营商云计算平台面临的安全威胁和挑战分析

从电信运营商云计算平台安全体系的层级结构分析，云计算信息系统与传统互联网信息系统在安全方面最大的差别是：应用环境和数据脱离了用户可控范围，数据和应用环境分离，终端的安全防护能力严重削弱，导致云计算平台主机系统、网络、Web 应用服务等层面存在安全威胁，为云计算平台的安全检测和防护带来了严峻的挑战。云计算安全问题包括云计算安全技术的挑战，服务供应商及用户如何进行相互协作的管理方面的挑战，以及其跨地域性、多租户、虚拟化等特性带来的数据安全、内容安全、隐私保护、风险评估、安全监管和司法取证等方面的挑战[5]。主要表现在以下方面：

1) 网络边界消失带来的安全威胁。由于在云计算环境下，存储和计算资源高度整合，基础网络架构统一化，安全设备的部署边界已经消失，这也意味着安全设备的部署方式将不再类似于传统的基于边界的安全隔离和访问控制，以及针对不同的安全区域设置有差异化的安全防护策略的安全建设模型，导致传统的网络 IP 攻击、操作系统和软件漏洞、病毒木马、拒绝服务攻击、僵尸网络、Web 攻击等安全威胁依旧会存在，并且将伴生新的攻击方式威胁。

2) 动态虚拟化技术应用带来的安全威胁。在云计算环境下，基于虚拟化技术的存储资源和服务器计算资源的高度整合和集中，存储计算资源的按需分配、数据之间的安全隔离成为必须，基础架构设施的性能和扩展能力将直接影响到云计算平台的持续、稳定运行。在虚拟化应用中还存在利用漏洞和隐蔽信道实现虚拟机和应用的穿透逃逸威胁，通常由于虚拟机之间共享硬件资源而引发，目前尚不具备有效的检测和防护手段。

因此，服务器计算和存储资源虚拟化技术的应用导致虚拟机的隔离、虚拟化软件的漏洞攻击、虚拟机自身的安全、虚拟机的访问控制、虚拟机的权限管理、虚拟机之间的通信安全、虚拟机迁移安全、虚拟机监视器(Hypervisor)安全、API 接口安全等安全威胁。

3) 混合技术的应用导致的安全威胁：由于云计算是多种计算机技术和网络技术融合发展的技术架构，从实践走向实践，所以云计算缺乏严谨的理论基础，多种混合技术和应用模式的将引发新的云安全应用漏洞存在，不同云计算平台间不能很好的移植和兼容，以客户端为主体的威胁检测方式也随之变化，直接影响云服务的安全性，也给漏洞的发现能力，安全检测效率等方面提出新的挑战。

4) 云计算安全模式存在的安全威胁：在云计算环境下，由于内部人员非法操作、黑客攻击及系统故障导致安全机制失效，引发数据隔离失效、数据和隐私泄露、删除后剩余数据的非法恢复等数据安全问题。这些安全问题的存在直接导致用户对云服务商是否正确使用数据产生信任危机。

5) 云计算服务模式存在的安全威胁：由于云计算服务模式的转变，导致 SaaS 层面存在内容安全(垃圾信息防护、网络行为安全)、云服务安全(云病毒查杀、流量清洗)、用户数据安全(财务数据、敏感信息、用户隐私信息)等方面的安全威胁；PaaS 层面存在管理安全(身份认证等)、监管安全(态势实时监测、内容实时监控)、运营管理安全(配置管理、性能管理、故障管理、安全管理)等方面的安全威胁；IaaS 层面存在着物理安全(主机和存储硬件和操作系统安全)、虚拟化安全(虚拟机安全隔离、运行安全)、数据存储安全(数据备份、加密存储)、云计算网络安全(访问控制、入侵检测和防御)等方面的安全威胁。

6) 云计算平台监管和运营风险：由于电信运营商云计算平台建设和运营缺少标准化、体系化的技术规范要求和监管制度体系约束，导致在存在大量技术风险的同时，也存在着如宕机对用户的信誉打击；数据资源泄露和滥用影响；云计算运营商的服务能力和质量考核；用户操作行为鉴别和审计；持续稳定

运行、故障隔离、规避风险、降低最小影响；运行安全管理，职责划分与权限管控、安全资质、用户评级、安全公告等方面的运营监管能力缺失。另外，云计算应用模式打破了国与国的地域界限，各国不尽相同的法律法规要求，也给数据隐私、数据安全隔离等方面涉及的各种法律法规的遵守问题提出挑战。

4. 电信运营商云计算平台的安全需求

通过对云计算信息系统的安全体系层级结构和与面临的安全威胁分析，基于传统互联网的安全特征，分析电信运营商云计算平台的安全特性和特殊要求[6]。

1) 数据保护需求。在电信运营商云计算平台体系的数据资源共享环境中，将对严格的身份验证机制、符合数据安全级别和国家要求的加密机制、合理的数据隔离措施、完备的容灾备份机制提出了更高要求，以实现数据的传输安全、存储安全和审计安全。

2) 安全审计需求。电信运营商云计算平台需要具备统一的安全审计能力，实现对云计算平台系统和数据访问服务的全面安全审计，并能利用海量数据存储和挖掘分析能力实现审计事件日志的精确定位、溯源取证、长期存储的安全审计目标。鉴于审计数据的重要性，审计数据被篡改或恶意删除的风险加大，直接影响到用户权益保障问题，这将对审计数据保护措施以及云计算平台的运维管理和监督检查机制的力度提出更高要求。

3) 身份鉴别需求。采用集中的身份认证机制，有利于用户身份鉴别机制的增强，减少用户因自身身份鉴别机制的设置不当而引发安全事件的可能性。但用户终端自身的安全防护功能的缺失和终端物理防护的脆弱性，促使电信运营商云计算平台必须寻求新的身份鉴别机制来满足特定环境下的安全需求。

4) 安全监管需求。在电信运营商云计算平台中，如何建立云计算服务商的用户信任机制，使用户认可信息系统的安全防护能力和对数据隐私性的保护能力；如何建立云计算服务提供商的监管体制，规范云计算服务商的服务行为，都将成为电信运营商云计算平台亟需解决的问题。

因此，在云计算环境下，网络安全防御模式由被动式向主动式转变，云检测模式的变迁，也促使电信运营商云计算平台亟需采用新的安全技术手段和管理模式实现安全有效的检测和监管，也必将促进电信运营商云计算平台的安全检测和防御技术的发展。

5. 电信运营商云计算平台安全检测评估服务体系

5.1. 云安全检测评估服务体系模型

云计算是 IT 服务方式的改变，并未颠覆传统互联网安全模式。由于云计算应用架构的特点，导致云环境下安全设备和安全措施的部署和防护重点有所不同，也促使安全责任的主体发生了变化，由用户自我保护转变为由云计算服务提供商来保证服务提供的安全性。因此，电信运营商云计算平台的安全检测评估服务体系依旧需要遵循和借鉴国家信息安全等级保护等相关传统安全标准和最佳实践方法，契合电信运营商云计算平台的应用特点，从云安全整体考虑，突出云计算特点，实现电信运营商云计算平台重点部位的检测评估和安全防护。依据策略、技术和人的三个要素组合思想，提出以咨询服务为指导，以云安全技术和云安全管理为支撑的云计算平台安全检测评估体系模型。

5.2. 电信运营商云计算平台安全检测评估技术

针对电信运营商云计算平台面临的安全威胁和安全需求，结合云计算平台安全检测评估体系模型，遵循国家信息安全等级保护建设和测评的标准和规范，参考风险评估的理论思想，将对电信运营商云计算平台从云安全、云管理、咨询服务等层面进行检测评估技术的内容介绍[7]。

1) 云安全

① 基础设施安全合规性检查

物理安全：重点检测评估机房安全措施、出入监控管理、物理安全管理制度等，参照等级保护 3 级的机房建设和管理要求。

网络安全：重点检测评估安全域的划分方法、网络访问控制技术、入侵检测防御技术、传输数据加密技术、流量分析管理技术、综合审计技术、安全事件日志分析技术、通信线路安全保障、骨干线路冗余防护、核心设备防雷击等网络安全防护措施和策略，并通过渗透测试等评估技术，验证配置策略和防护措施的有效性。检测网络安全产品端到端的扩充和收敛的虚拟化应用方式，评估端到端网络虚拟通道的安全性。

宿主机安全：从安全配置与加固、服务器安全防护措施、恶意代码防护、补丁管理、访问控制、系统加固、强认证、安全事件日志、基于主机的入侵检测系统/入侵防御系统等方面进行安全检测和评估分析。

VM 安全：重点对虚拟机间的隔离、虚拟机配置与加固、虚拟机镜像安全管理、虚拟化环境下的通信安全、虚拟化和物理安全设备的统一管理和可视化、虚拟层安全防护措施等方面进行检测评估，通过漏洞挖掘分析和漏洞利用穿透技术，验证评估虚拟机的安全性。

容灾备份：从 PaaS 层(数据容灾、应用容灾、运营管理、资源调度)和 SaaS 层(数据容灾、应用容灾、服务软件管理、运营管理)的容灾备份管理机制和措施进行检测评估。

管理平台系统：检测评估云管理平台的访问控制、管理客户端安全、通信安全、数据库安全、日志安全、补丁管理等功能措施。

② 云计算应用与运营管理

检测评估双方的职责划分：PaaS：云服务提供商除了负责底层基础设施安全外，还需解决应用接口安全、计算可用性等；而云用户则需负责应用环境之上的应用服务安全等。SaaS：云服务提供商需保障其所提供的 SaaS 服务从基础设施到应用层的整体安全；云用户则需维护与自身相关的数据安全，如身份认证账号、密码的防泄漏等。

检测评估 SLA 安全条款要求：从性能保障、可用性保障、据及隐私安全保障、应急响应机制、审计机制等方面进行。

身份管理与访问控制要求：检测云计算服务提供商应支持对内部管理用户和外部租户进行集中的身份维护管理，是否具备统一、集中的认证和授权体系。评估集中访问控制、集中授权、集中审计、访问认证、维护管理能力。重点对用户帐号生命周期的身份供应/取消供应、认证、联盟、授权和用户配置策略文件管理以及为满足各种用户和访问流程自动化需求的开放式应用程序接口、授权审计、信息同步等检测评估；对集中用户认证、集中用户授权、日志管理、加密机制、用户和访问生命周期管理流程、以及审计和合规功能进行检测评估。

数据安全及隐私保护要求：对数据安全、隐私保护、加密及密钥管理、数据隔离、数据加密解密、身份认证和权限管理，保障用户信息的可用性、保密性和完整性等方面进行检测评估。

安全管理要求：检测评估涉及安全策略管理、虚拟化资源安全管理、基础设施安全管理的策略和措施。

安全审计要求：检测评估审计数据采集、分析、呈现、预警响应能力。

安全检测能力：检测评估客户端和云端的关联耦合云检测能力、对未知安全威胁或是可疑安全威胁的传感检测能力。

安全组织和管理制度体系：新的 IT 架构和服务模式需要新的组织和流程来保障服务的开展。需要检

测评估组织机构、人员管理、制度体系落实情况。

③ 应用安全测试

在云服务的模式下，面向业务的流程和架构的持续优化非常重要，需要不断契合业务发展需求，提高系统效率。应用安全架构的评估和业务模块的应用安全检测包括自动化 Web 漏洞扫描工具测试、服务器信息收集、服务器信息收集、认证测试、会话管理测试、权限管理测试、文件上传下载测试、信息泄漏测试、输入数据测试、跨站脚本攻击测试、API 接口安全测试、“最小特权”配置测试、逻辑测试、搜索引擎信息收集、Web Service 测试以及云计算系统功能和标准符合性测试、云计算系统性能测试、云计算系统安全可靠性测试等检测评估内容。

④ 云客户端安全

检测评估主要涉及客户端安全设计、软件的审核、校验机制和控制和管理机制、用户的安全识别和认证机制、密码策略、数据传输、数据存储、防篡改能力、客户端保护以及数字证书的数字签名终端可信的授权与能力的控制等方面。

2) 云管理

① 分布式管理

主要检测评估资源分配、负载均衡、路由管理功能。比如安全域划分和策略配置、资源访问控制措施、负载均衡设备的最大虚服务(实服务)个数、实现每个虚拟设备具备独立的管理权限、配置变更管理等。

② 云平台管理

主要检测云平台的统一智能部署和统一智能升级以及统一智能检测能力。以及对云平台设备的性能、容量、处理能力，扩展性、系统性能的便捷提升进行评估，并对安全厂商的响应和服务能力进行评估。

③ 虚拟资源管理

主要检测虚拟资源监控的能力和监控有效性。

④ 云平台资源管理

主要检测云平台对主机资源、存储资源、网络资源的管理能力。

3) 咨询服务能力

从虚拟化平台建设咨询、安全监管制度规范、安全监督体系建设咨询、运营 SAL 体系建设咨询、CISP 培训和人才队伍建设等方面整体进行云平台服务能力的评估。

5.3. 云安全检测评估流程

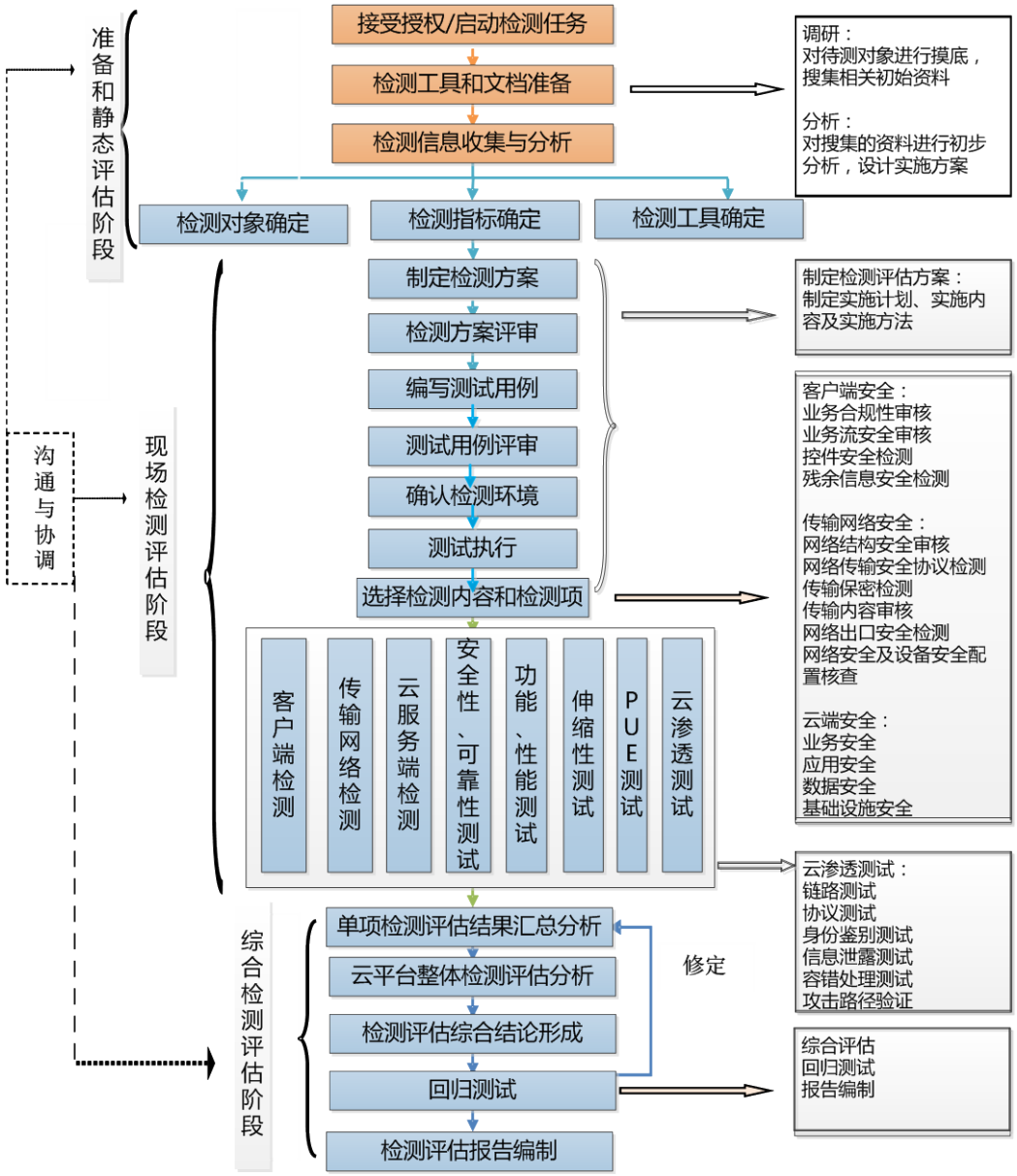
云安全检测评估流程主要包括三个阶段：

1) 准备和静态评估阶段

本阶段需与被检测单位就检测对象、检测目标、检测范围等进行全面的沟通，并根据保密原则和不侵害原则签订检测授权协议，根据云计算平台的特点，准备相应的检测表单、检测工具，并根据初步搜集的材料进行检测方案的编制。

2) 现场检测评估阶段

本阶段根据检测评估方案，细化具体的检测实施计划、内容及方法，编制相配套的测试用例，并根据静态评估阶段获得的信息，选择相匹配的检测内容和检测项，从客户端、传输网络、云服务端等三大层面开展相关内容的检测，综合采用云渗透测试、链路测试、协议测试、身份鉴别测试、信息泄露测试、容错处理测试、攻击路径验证等检测方法，全面评估云计算平台的安全性、可靠性、伸缩性、PUE、防渗透性等方面的现状。



3) 综合检测评估阶段

本阶段根据现场检测评估获得的各单项检测评估结果进行汇总分析，并结合云计算平台的总体特点形成总体性结论，完成回归测试后形成最终的检测评估报告。

6. 结束语

云计算的前景广阔，但是与之相符的却是规范与管控和检测能力的缺失，云计算作为一项全新的互联网应用商业模式，各类应用发展迅速，而安全性是用户选择云计算应用时的首要考虑因素，也是云计算实现健康可持续发展的基础。本文在总结、分析云计算应用面临的技术层面安全威胁和法律合规风险的基础上，对云计算安全服务检测评估技术进行了系统分析与研究，并提出云计算应用安全策略与检测评估建议，结合云计算的特征，创新性的提出了适用于云计算安全检测评估的流程，检测内容等，具有较强的推广和实践价值。

随着云计算环境安全建设模型和思路，以及检测评估技术的继续实践和探索，将使得云计算的服务交付更加安全可靠，从而实现对传统 IT 应用模式的转变。

参考文献 (References)

[1] 张敏, 陈云海, 林立宇 (2009) 电信运营商云计算数据中心的构建分析. *电信技术*, **6**, 100-104.

[2] 郭乐深, 张乃靖, 尚晋刚 (2009) 云计算环境安全框架. *信息网络安全*, **7**, 62-64.

[3] 杨新民 (2009) 关于云安全的分析. *信息安全与通信保密*, **9**, 45-47.

[4] 汪兆成 (2011) 基于云计算模式的信息安全风险评估研究. *信息网络安全*, **9**, 56-59.

[5] 蔡盈芳 (2010) 基于云计算的信息系统安全风险评估模型. *中国管理信息化*, **6**, 75-77.

[6] 高志新, 等 (2012) 关于云计算安全及检测要求的探讨. http://www.doc88.com/p-903965693213.html

[7] 成晓旭 (2012) 电信运营商云计算发展分析. http://blog.csdn.net/cxxsoft/article/details/7608547