

美国联邦政府推行云计算的新进展

王佳存

(山东省科学技术厅, 济南 250101)

摘要: 云计算是IT领域的新兴技术,是互联网、移动电话、网络工具和虚拟技术的集成。云计算的发展不仅会创造新的就业岗位,提高劳动生产率,而且将对改变IT产业格局和整个国家间财富分配产生深远影响。近年来,云计算不仅得到美国企业、科技界的大力倡导和运用,而且也受到美国政府的高度关注和推动。目前,美国政府机构积极推行云迁移,在降低政府运行成本、提高政府工作效率、形成标准规范等方面取得了新的进展。

关键词: 美国; IT产业; 云计算; 云迁移

中图分类号: F49(712)-01; D771.231-39 **文献标识码:** A **DOI:** 10.3772/j.issn.1009-8623.2012.06.002

云计算(Cloud Computing)是近几年的一个热门词汇,也是IT领域的新兴技术,不仅得到美国企业、科技界的大力倡导和运用,而且也受到美国政府的高度关注和推动。目前,云计算正在美国联邦机构中云卷云舒,在降低政府运行成本、提高政府工作效率、推动政府公开透明、形成技术标准规范等方面取得了新的进展。

一、两次听证: 机遇、挑战或安全

2011年9月下旬和10月上旬,美国众议院的两个分委员会分别围绕云计算召开了两次听证会,邀请政府和企业的有关人员参加,就云计算的发展态势、政府在云计算中作用和实践以及面临的问题进行发言并回答议员的提问。

(一) 机遇与挑战并存, 机遇大于挑战

2011年9月21日,美国国会众议院科学、空间和技术委员会的技术和创新分委员会召开了题为“下一次IT革命? 云计算的机遇和挑战”的听证会,参加听证会的有虚拟计算环境公司主席兼CEO卡佩拉斯(Michael Capellas)、微软公司副总裁里德(Dan Reed)、EMC公司首席技术官库姆斯(Nick

Combs)以及联邦总务管理局(GSA)助理局长迈克(David McClure)。技术和创新分委员会主席奎勒(Ben Quayle)^[1]在开场白中说,过去几十年来,IT的发展促进了经济发展,云计算具有成为下一次IT浪潮的潜力,这一技术的广泛推广为新的创新带来了机遇,同时,也带来了很多的挑战,比如:网络安全、宽带接入、隐私保护、技术标准等。参加听证会的证人在发言中充分肯定云计算所带来的机遇。

1. 云计算是提高美国竞争力的重要因素

虚拟计算环境公司主席兼CEO卡佩拉斯^[2]也是美国技术基金云计算应用委员会的共同主席,他说,上世纪中期以来,信息技术的兴起催生了美国经济的繁荣。云计算是互联网、移动电话、网络工具和虚拟技术的集成,不仅会创造新的就业岗位,提高劳动生产率,而且将对改变IT产业格局和整合国家间财富分配产生深远影响。在他看来,谁的云迁移速度快,谁将具有更强的竞争力。

他表示,商业领域的云计算有着很大的市场,今后3年云计算的收入将达到500亿美元。云计算对于提高美国竞争力,增加就业岗位和提高生产率

作者简介: 王佳存(1965-),男,博士,副处长,主要研究方向为金融、信息处理、科技经济政策。

收稿日期: 2011年11月18日

非常重要。美国IT的领先地位依赖于云计算的领先地位。卡佩拉斯曾建议政府部门制定评估和授权云计算服务和产品的标准。

科技创新能力的提升需要云计算。里德^[3]认为,面对海量数据,科学家需要在短时间内进行分析和计算。比如,Sloan Digital Sky Survey 2011年1月发布的最大的数字彩色天空图,需要50万个高清电视才能观看。微软和NSF合作为科研工作者提供可扩展的云工具和服务,有13个科学研究团队利用Windows Azure云进行为其两年的研究。

2. 云计算已具备发展的条件

里德^[3]在发言中坦陈,云计算不是突然到来的,人们共享数字图片、网上购物、电子邮件、下载和应用程序、搜索引擎等都是云的使用,这些技术整合的条件已经成熟。支撑云计算的基础设施不断扩展而且越来越高效,一个云数据中心包括的数字资料相当于国会图书馆的收藏量,像微软那样的云提供商正在建立遍布全世界的数据中心网络;人们普遍使用的电子设备功能更加强大,能够实现远程医疗诊断、智能交通以及大规模数据传输和储存等;随着无线和有线宽带的发展,网络通讯越来越便捷、高效和低廉。

3. 云计算可以更有效地防范安全风险

库姆斯^[4]提出,在看到云迁移提高效率、降低成本、增加收入的同时,相信,在建立云信任的前提下,从长远看,云计算的采用将有助于改进网络安全,因为未来的云计算服务提供者会采取集中监测、管理的解决方案,而且,将安全手段内置于信息基础设施中,以更为专业的技术应对安全威胁;同时,强化《联邦信息安全和管理法》(FISMA)的实施,对于解决当前面临的安全风险问题以及建立今后有效的运行风险管理框架至关重要。

4. 联邦机构要积极实施云计算

迈克^[5]介绍了政府机构推行云计算的做法。近年来,联邦总务管理局在改革IT管理、实施云计算方面发挥中心作用,会同白宫管理和预算办公室出台了联邦数据中心精简计划,制定了联邦机构电子邮件云迁移的方案。他认为,在日益数据中心化、环境网络化的时代,云迁移是提高政府效率的关键措施。

(二) 云计算有风险,控制风险有措施

2011年10月6日,美国国会众议院国土安全委员会虚拟安全、基础设施保护和安全技术分委员会同样召开了一个关于云计算的听证会,题目是“云计算:有什么安全问题”,由分委员会主席鲁格林(Dan Lungren)主持。参加听证会的有国土安全部首席技术官斯皮雷斯(Richard Spires)、联邦总务管理局助理局长迈克、审计署信息安全事务主任威尔束森(Greg Wilshusen)、计算机科学公司北美公共事务总裁歇尔弗(James W. Sheaffer)、CA技术公司高级副总裁布朗(Timothy Brown)、克莱姆森大学分管计算和信息技术的副校长波特姆(James R. Bottum)、美国互联网注册公司CEO库兰(John Curran)。

鲁格林在开场白中说,政府实行“云优先政策”,国土安全部宣布向云计算迁移,分委员会要考察了解政府信息在云环境下的管理和安全情况,同时听取私营部门是如何采用这一共享技术、如何降低成本和风险的。他提出,有人怀疑云计算是否比现有计算机系统更容易受到攻击,政府有责任解除他们的疑问。与会听证人员分别围绕安全问题发表了见解。

1. 传统IT环境和云计算都有安全问题

迈克^[6]说,安全问题并不是云计算系统所独有的,联邦政府部门正在对云计算加强新的安全控制,制定新的标准。他还说,云计算提高了政府效率,避免了建设和维护昂贵的IT基础设施的费用,同时,由于采用了更为有效的安全风险管控措施,云计算更加安全并持续地保护政府的IT设施、数据 and 应用程序。

2. 联邦政府机构需要云

斯皮雷斯^[7]说,目前,政府机构的IT设施和系统各自为政,运行分散,不断出现潜在的安全漏洞,在预算紧张的情况下很难满足执政以及提高执政效率的需要,必须利用云技术进行IT资源的升级换代。同时,不论是传统IT环境还是云环境都可能受到网络攻击,比如APT等,但是,由于云环境具有更为先进的监测能力和更为专业的信息安全人员,因此更有可能抵御和化解网络攻击,从而更好地维护信息安全。

斯皮雷斯认为,随着信息技术服务的商品

化，云计算将推动IT的变革。即便所采取的安全措施不能完全说服质疑者，但是对于联邦政府实现降低运行成本、适应当前的技术发展趋势来说，云计算是不可或缺的。

3. 云计算安全要重视

威尔束森^[8]依旧强调了云计算存在的安全问题，他的态度远没有其他联邦官员乐观，认为在已经开始推行云计算的情况下，联邦应对安全的措施还不完备，还需要做更多的工作。波特姆^[9]说，云计算是有效的、经济的，收益大于风险，但是，为了使用这一兴起的技术，要同时制定安全工具、安全措施和安全政策。

4. 云计算挑战之一是建立信任

歇尔弗^[10]认为，云计算面临的挑战之一是信任，包括云用户对云提供商的信任以及云技术的信任。实现云迁移后，云用户会特别关心云的安全、可用、可信、对用户透明以及提取数据的能力。比如说，政府重要的数据能够信赖云吗？

两次听证会，联邦总务管理局助理局长迈克都参加了。他在谈及安全的同时还介绍说，通过实现云计算，联邦总务管理局实现了从购买和管理IT物理资产向购买IT服务的转变，政府机构仅仅支付所使用的IT资源，不再需要支付建设和维持IT基础设施的高昂开支，促进了2000多个联邦数据中心的整合和精简，实现了政府IT投入效益的最大化；同时，今后将在整个政府部门中间实施联邦风险和授权管理计划，以更为统一和综合的手段应对云环境下的安全威胁^[6]。

事实上，美国不论是过去还是现在从来没有放松过对信息安全的重视。2011年10月7日奥巴马发布“关于改进机密网络安全、更加负责任地共享和保护机密信息的体制改革”总统令，一是要求各相关部门主要负责人对本部门机密计算机网络和机密信息共享以及保护负总责，指定一名高级官员具体监督，实施内部威胁检查和防范项目，根据总统令的政策和标准进行自我检查；二是成立高级别信息共享和保护指导委员会，由管理和预算办公室和国家安全局的高级代表共同主持，国务院、国防部、司法部、能源部、国土安全部、国家情报局、中央情报局、国家档案管理局信息安全监督办公室以及相关部门为成员；三是在信息共享环境项目管

理办公室（PM-ISE）内部成立机密信息共享和保护办公室（CISSO），负责计算机网络上的机密信息共享和保护；四是国防部部长和国家安全局局长共同负责总统令的实施，制定更为有效的技术保护政策和标准，对政府各部门机密信息保护情况进行独立评估并将结果报高级别信息共享和保护指导委员会；五是成立跨部门的内部威胁防范小组，由司法部长和国家情报局长共同负责，对政府各部门进行内部威胁的检查、监测和化解，同时负责制定防范政策、目标和优先重点。

二、一个战略：释放云能量

奥巴马重视IT技术的应用，2009年3月在白宫管理和预算办公室首次设立并任命昆德拉（Vivek Kundra）为第一任联邦政府首席信息官，主要负责联邦机构的IT技术应用。2009年12月昆德拉提出针对联邦政府工厂管理改革的“25点计划”^[11]，完全肯定了云计算的发展战略；2011年2月，昆德拉签署发布《联邦云计算战略》（*Federal Cloud Computing Strategy*）^[12]，对云计算的定义、作用进行了明确阐述，提出了推行云计算的措施。

（一）云计算内涵

云计算概念提出以来，人们对其内涵是见仁见智。《联邦云计算战略》中采用的是美国国家标准与技术研究院（NIST）的定义，认为云计算是一种可以实现对共享的可配置计算资源池（如网络、服务器、应用软件和服务）进行便捷、按需网络接入的模式，且这些资源可以在最低程度的管理和服务提供商干预的情况下，得以迅速地提供和交付。云计算的特点有5个，分别是：按需服务（on-demand service）、广泛网络接入（broad network access）、资源池化（resource pooling）、快速扩展（rapid elasticity）以及可计量服务（measured service）。

根据使用性质，云可分为私有云、社区云、公共云和混合云。私有云是指某个机构独立操作管理云基础设施，并自己或委托第三方管理；社区云是指一组具备相同任务、相同安全需求、相同政策或相同IT遵循策略的机构共同管理云基础设施，共同使用；公有云是指某个机构拥有和管理云基础设施，向社会提供云服务；混合云是指云计算基础

设施是由两种云(私有或公共)组成,每种云保持独立,但用标准的或专有的技术将他们组合起来,具有数据和应用程序的可移植性,这种云既可自己使用,也可向其他机构提供服务。

根据服务类别,云计算有几种不同的服务模式,分别是:

1. 软件即服务(SaaS)。客户使用云服务商提供的运行在云基础设施上的应用程序。这些应用程序可以被各种各样的客户端设备通过客户端接口,如WEB浏览器(基于WEB的电子邮件)访问。客户无法管理或控制底层的云基础设施,包括网络、服务器、操作系统、存储设备,甚至独立的应用程序,但有一些受限的、用户专用的应用配置设置权限。

2. 平台即服务(PaaS)。客户使用云服务提供商支持的开发语言和工具,开发出应用程序,部署到云基础设施上。客户无法管理和控制底层云基础设施,包括网络、服务器、操作系统、存储,但可以控制其部署的应用程序和应用配置环境。

3. 基础设施即服务(IaaS)。向客户提供处理能力、存储能力、网络以及其他基本计算资源,客户可以使用这些资源部署或运行他们自己的软件,包括操作系统或应用程序。客户无法管理和控制底层云基础设施,但是可以控制操作系统、存储、发布应用程序,或拥有有限的网络组件控制权(如防火墙)。

(二) 云计算的作用

从技术上来说,云计算实现了信息处理、传输、接入等各种IT技术的整合;从模式上来说,云计算实现了政府部门从建设和管理IT基础设施为主向使用IT服务为主的转变。这一转变将推动政府IT环境发生根本性的变革,为联邦政府机构带来降低运行成本、提高工作效率、实现技术更新等方面的巨大收益。

1. 减少政府支出。2010财年,美国联邦政府IT投入的30%用于数据中心基础设施,很多政府部门服务器存储量的使用不到30%,而且各个部门都建设数据中心,造成了IT基础设施建设的极大重复和IT资源的巨大浪费。如果实行云计算,充分释放云的能量,将使政府节约大量的财政经费,使政府IT资源得到更加有效、科学的配置。

2. 提高工作效率。在传统IT环境下,政府部门的工作效率以及对社会的服务主要依赖本部门的IT能力,面临突发事件,常常很难利用自己的IT

能力满足工作需求,从而造成工作的被动和效率低下。比如,曾经用于汽车补贴和退税的IT系统(CARS,通常称为“旧车换现金”),因为工作负荷远远高于其系统处理能力而多次失败。作为“旧车换现金”的主办单位——美国国家公路交通安全管理局(NHTSA),曾预期25万次的交易量至少需要4个月的时间,但是在短短的90天,系统处理的交易量就达69万辆,导致系统不堪重负,引起政府对社会服务的中断。云计算由于将IT资源进行整合,因而具有强大的处理能力,满足政府部门不可预知的IT服务需求量,避免部门IT服务瓶颈问题,能够最大程度地减少类似服务中断的发生。

3. 实现技术更新。企业是技术创新的重要推动者,在采用前沿技术上常常领先于政府部门。比如,在日常生活中,人们可以在线随时随地查询一批海运货物的方位,可以订购一张比萨饼或一双鞋,可以进行旅游、酒店、餐厅的预定,可以与朋友和同事沟通。然而,当涉及到处理与联邦政府相关的事务时,人们却总是需要排队、电话等候或以书面表格的方式递交。在云环境下,由于政府将IT经费主要投入到购买IT服务上,因此,可以向企业那样能够利用最新的IT技术。

(三) 政府推行云计算的措施

对于政府部门来说,云计算是利用IT观念和方式的变革。为推行云计算,美国政府采取了以下措施:

1. 加强对云计算的指导。在首席信息官的组织领导下,开发了云计算使用案例库和云计算一站式服务平台Apps.gov,展示并提供得到政府认可的云计算应用方案,有关政府部门可以根据自身行政特点选择合适的案例以及云服务提供商,并以此为参考建立自己的云计算环境。同时,要求各相关部门参加NIST和GSA等组织的云计算工作组,在云计算标准、参考架构、分类、安全、隐私和商业应用等方面听取建议。

2. 确保营造安全可靠的云环境。联邦政府向云计算环境转型,确保政府信息的安全、公民隐私权与国家安全。2010年,出台了“联邦风险与授权管理项目”,对漏洞扫描、活动监控、日志、报告等提出了明确的要求,以提高对云计算环境的信赖度和信任度。国土安全局将每隔6个月或根据实际需要列出一份头号安全威胁黑名单,并与政府所

有安全专家组成的大型团队一起确保相应安全控制措施的实施,以消除这些安全威胁。国家标准技术研究院将发布技术安全指南,按照风险管理框架,集中持续地监测云计算解决方案。

3. 简化采购程序。联邦政府将为云服务提供商提供“一次审批,多次使用”的做法,简化审批手续。美国总务管理局(GSA)通过一次审批,与12家云服务提供商签署了IaaS合同,减少了不必要的成本和重复劳动。

4. 建立云计算标准。NIST将会同相关部门制定、评估和修订云计算路线图,确定云计算重点领域,建立云计算架构、交互性、安全、数据移植等方面的标准。

5. 充分认识云计算的国际因素。重点考虑今后10年内的数据主权、数据传输和访问数据问题,确定国家数据隐私、安全和知识产权之间的平衡点;考虑适用于云计算的国际法律、法规和管理框架,探索国内和国际环境下数据的互操作性和可移植性,建立全球统一的云计算标准等。

6. 实行职责明晰的管理体制。政府在推行云计算战略中发挥关键作用,NIST将领导并与联邦、州和地方政府的专门机构CIO及私营部门的专家和国际机构合作,共同制订云计算标准和指导意见;总务管理局将采用政府采购手段采购云计算应用解决方案;国土安全部将监测与云业务有关的安全问题;各相关部门负责评估其采购策略,充分考虑云计算解决方案;联邦首席信息官理事会将推动政府各部门审批通过云计算方案,确定下一代云技术;白宫管理和预算办公室协调并指导各部门确定云计算优先项目。

三、28家机构:加速云迁移

根据13011号总统令,美国成立了首席信息官委员会,由28家政府机构组成,主要是推动联邦信息资源的设计、采购、开发、使用、共享等,这些机构根据政府云计算战略,在联邦IT环境向云迁移方面进行了初步的实践。

这28家机构是国务院、财政部、国防部、司法部、内政部、农业部、商务部、劳工部、卫生与人类服务部、住房与城市发展部、交通部、能源部、教育部、退伍军人部、环保署、联邦应急管理局、中情局、社安局、小企业管理局、陆军、

海军、空军、国家航空航天局、国际发展局、总务局、国家科学基金、核管会以及人事管理办公室。

美国联邦政府每年花在IT设施及服务上的经费大约为800亿美元。美国《联邦云计算战略》认为,美国联邦政府的信息技术应用环境存在着资产利用率低下、资源分散、系统冗余、管理混乱以及采购和交货周期长等问题,比如数据中心的利用率只有27%。云计算模式能够在整合IT资源的情况下有效地帮助政府应对上述问题,提供高可靠性和创新性的服务。为通过云迁移整合联邦政府IT资源,美国确定到2015年至少将现有的2100个数据中心精简掉800个,实行政府IT设备改造“云优先”政策,要求各部门两年半内将3项IT服务实现向云的转移。

在云迁移的过程中,每个部门都按照选择一需求一管理的云迁移决策程序进行。在选择阶段,主要迁移那些需要提高效率、减少运行成本、实现技术更新的IT服务,迁移安全要求明确、市场成熟度高、网络接入和数据交互性好以及部门积极性高且IT设施需要更新的IT服务;在需求阶段,要集成提出本部门的综合云服务要求,与云服务提供商签署有效的合约并确定可以实现的预期价值;在管理阶段,要实现IT资源从固定资产向服务的转变,主动监管与云服务提供商签署的合约的执行情况,未雨绸缪,定期进行评估。

下面分别以一个IT服务的云迁移和一个部门的云迁移为例介绍联邦政府机构的云迁移情况。

1. 陆军体验中心(AEC)顾客关系管理(CRM)的云迁移

2008年,陆军体验中心认识到自身需要一套新的人员管理系统CRM,以了解人员的活动和和使用电子设备情况,并帮助招聘人员管理招聘流程。当时,该机构已经有一个使用10年的数据系统,建立CRM系统的一个选择是升级已有的数据系统。经过研究,该机构决定实现云迁移,确定采用软件即服务(SaaS)的解决方案。

在这一决策过程中,该机构主要考虑了以下因素:一是节约成本。升级已有数据系统,需要50万美元到100万美元,而采用SaaS只需用5.4万美元。二是功能性。升级老系统不能满足功能需要,而且升级所需时间长。如果采用SaaS解决方案,则很快就可以完成,并满足所有功能需要,而

且具有功能扩展性的优点。三是技术创新性。老系统即便升级,也不能随时利用不断更新的IT技术,而SaaS则能做到这一点。四是安全性。SaaS方案能够保证AEC数据接入、数据独立、数据储存的绝对安全。五是技术可行性。SaaS方案能够满足AEC利用现有设施追踪人员管理数据的需求,与员工终端设备兼容,并能实时管理和使用数据系统。六是现有技术能力。AEC认为自己具有云迁移的技术条件。七是现有系统老化情况。AEC的现有系统已不堪重负,到了报废阶段。经过采用云计算方案,AEC已经可以处理比原招募中心多5倍的工作量。

2. 国土安全部的云迁移

美国国土安全部目前主要有私有云和公共云两种模式,其中私有云通过本部门的两个数据中心实现,主要是管理敏感但非机密的信息;公共云通过云服务提供商实现,主要是管理非敏感的信息。仅通过私有云,国土安全部就节省了近10%的投入。

国土安全部计划建设9个私有云,分别是:①邮件即服务(EaaS),在部机关和联邦应急管理局推广这项服务,2012年底将有10万人使用;②共享节点即服务(SHPTaaS),将总部和美国公民和移民服务局的用户迁移到云服务,截止2011年底有9万用户,这一迁移将极大地提高国土安全部的信息共享能力;③发展和试验即服务(DTaaS),通过这项云迁移,可以在一个工作日获得所需的新服务器以及任何所需要的试验和应用管理工具,而在云迁移前,获得IT服务则需要半年;④基础设施即服务(IaaS),这一云迁移与DTaaS是互补的,主要提高虚拟开发服务,包括操作系统、网络、储存等,已于2011年底实现;⑤工作地点即服务(WPaas),主要是提供强大的虚拟电脑、远程接入以及其他移动服务;⑥项目服务器即服务(PSaaS),主要是提供一个强大的管理平台,员工可以在上面发布项目进展情况,从而能在不同的办公室、处室、小组之间共享信息;⑦授权即服务(AuthaaS),在25个联邦与合同雇员中提供授权服务,大大减少了重复劳动;⑧案例和关系管理即服务(CRMaaS),将诉讼案件管理与补偿、客户关系以及法规监察迁移到云服务;⑨业务信息即服务(BIaaS),推动单位项目和开支的透明化,公开投资周期、财务、人力资源、

资产管理以及其他信息等。

除私有云外,国土安全部还制定了建设3个公共云的目标,其中两个公共云已经开始建设,第3个将在2012年启动。一是认证即服务(IDPaaS)公共云,主要是向在美国的居民提供免费、快速的求职查询和资格认证服务;二是企业信息发布即服务(ECDaaS)公共云,主要是保障面向公众的网络服务,目前国土安全部这一业务范围的服务有70%采用了云迁移;三是网络内容即服务(WCMaaS)公共云,主要是利用公共云的开发源代码软件提升美国移民和海关、美国公民和移民服务以及联邦应急管理局等网站的服务质量。

四、结语

在政府机构广泛热议云计算的时候,云计算这一新技术其实早已进入寻常百姓家,人们普遍使用的gmail、hotmail等电子邮箱就是一种公共云的SaaS。在服务模式上,云计算也不是一个新鲜概念,比如人们对电的使用,就是这样一种模式,每家每户不必都建自己的电站、电网等基础设施,只需按照消费的电量支付费用。由于信息处理能力、传输能力以及接入能力的增强,云计算在技术层面上已基本成熟,在政府部门的推广的主要障碍是安全问题。

从美国的实践看,政府机构迁移到云的信息均为非机密信息,而且涉及到敏感内容的非机密信息全部采用私有云。对于企业来说,云迁移将提供新的发展空间,带来新的收入,扩大新的市场;对于政府来说,云迁移将提高工作效率,降低政府开支,提升服务水平。正是由于这个原因,在对待云迁移的态度上,企业是积极游说,政府是谨慎推进,国会疑虑重重。问题的焦点还有,政府和企业,也就是云服务提供商和使用者之间是否能建立起足够的信任。云环境下的安全问题,比如信息窃取、信息攻击、内鬼泄密、安全漏洞等,在传统环境下同样存在。从政府决策看,美国联邦政府在确保信息安全的前提下推行云计算的态度是积极的,走在了其他国家的前头。

美国在云计算战略中提到的云计算国际标准、数据主权,以及国际环境下的数据互操作性等问题,也需要任何一个正在或准备推行云计算的国家进行深入的思考。■

参考文献:

- [1] Opening Statement, the Honorable Ben Quayle (R-AZ): “The Next IT Revolution?: Cloud Computing Opportunities and Challenges [R/OL]. (2011-09-21). http://science.house.gov/sites/republicans.science.house.gov/files/documents/hearings/092111_quayle.pdf.
- [2] TechAmerica Foundation. Statement of Michael Capellas: “The Next IT Revolution? Cloud Computing Opportunities and Challenges [R/OL]. (2011-09-21). http://science.house.gov/sites/republicans.science.house.gov/files/documents/hearings/092111_Capellas.pdf.
- [3] Written Testimony of Dr. Daniel A. “The Next IT Revolution? Cloud Computing Opportunities and Challenges” [R/OL]. [R/OL]. (2011-09-21). http://science.house.gov/sites/republicans.science.house.gov/files/documents/hearings/092111_Reed.pdf.
- [4] Written Testimony of Nick Combs: “The Next IT Revolution? Assessing the Opportunities and Challenges of Cloud Computing” [R/OL]. (2011-09-21). http://science.house.gov/sites/republicans.science.house.gov/files/documents/hearings/092111_Combs.pdf.
- [5] Statement of Dr. David McClure: “The Next IT Revolution? Cloud Computing Opportunities and Challenge” [R/OL]. (2011-09-21). http://science.house.gov/sites/republicans.science.house.gov/files/documents/hearings/092111_McClure.pdf.
- [6] Statement of Dr. David McClure: “Cloud Computing: What are the Security Implications?” [R/OL]. (2011-10-06). <http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20McClure.pdf>.
- [7] Testimony of Mr. Richard Spires: “Cloud Computing: What are the Security Implications?” [R/OL]. (2011-10-06). <http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Spires%20%282%29.pdf>.
- [8] GAO. Testimony, Statement of Gregory C. Wilshusen: “Information Security—Additional Guidance Needed To Address Cloud Computing Concerns” [R/OL]. (2011-10-06). http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Wilshusen_1.pdf.
- [9] Written Testimony of Jim Bottum: “Cloud Computing: What Are the Security Implications?” [R/OL]. (2011-10-06). <http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Bottum.pdf>.
- [10] Statement of James Sheaffer: “Cloud Computing: What are the Security Implications?” [R/OL]. (2011-10-06). <http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Sheaffer.pdf>.
- [11] Kundra Vivek. 25 Point Implementation Plan to Reform Federal Information Technology Management [R]. Washington, DC: the White House, 2009-12-09.
- [12] Kundra Vivek. Federal Cloud Computing Strategy [R]. Washington, DC: the White House, 2011-02.
- [13] TechAmerica Foundation. Cloud First, Cloud Fast: Recommendations for Innovation, Leadership and Job Creation [R]. Washington, DC: TechAmerica Foundation, 2011-08-02.

New progress of U.S. federal government’s cloud migration

WANG Jiacun

(Department of Science & Technology of Shandong Province, Jinan 250101)

Abstract: As an emerging technology in IT sector, cloud computing integrates a number of computer and network technologies. Owing to its great impacts on improving productivities and shaping a new industrial pattern, cloud computing is not only highlighted and utilized by U.S. enterprises and S&T fields, but also gets attention and recognition from U.S. federal government. In order to address the inefficiencies of low IT asset utilization, fragmented demand of resources and duplicative system, U.S. federal government has begun the migration of IT environment to cloud and has made sound progress.

Key words: U.S.; IT industry; cloud computing; cloud migration