云环境下数字学术信息资源安全保障的标准化推进*

万莉[1]，吕美娇[2]
（1. 南昌大学新闻与传播学院，南昌 330031；2. 武汉大学信息管理学院，武汉 430072）

摘要：云环境下，数字学术信息资源安全保障涉及服务链中诸多机构和社会用户，具有多元组合服务特征，因此推进安全保障的标准化是必须面对的社会问题。在此背景下，本文立足国内外现状，进行国家层面的学术资源云服务系统安全保障标准化推进分析，从学术信息资源安全审查、组织与服务安全责任划分、安全保障三方面进行标准化推进探索，结合现实情况提出对策建议。

关键词：数字学术信息；安全保障；标准化
中图分类号：G203
DOI：10.3772/j.issn.1673-2286.2017.07.004

云计算环境下我国学术信息资源建设正处于迅速发展阶段，与学术信息资源云服务同步的云安全保障已成为服务组织与实施中不可回避的问题。鉴于学术信息云服务利用的普遍性和服务链诸多机构组合的现实，在安全保障中推进标准化建设显得十分重要。从整体上看，云计算环境下国家学术信息资源安全保障是一项社会化系统工程，需有章可循，以确保其安全保障措施的可靠性。其中，信息安全标准一直是我国信息安全保障体系的重要组成部分，其实践发展为我国信息资源云安全保障的全面实现提供组织基础。同时，云安全标准作为衡量云服务用户安全目标与云服务提供安全能力的标尺，对云计算环境下国家学术信息资源安全保障的改进有重要支撑作用[1]。目前，云安全问题已成为制约数字学术信息云服务发展的关键因素，亟需推动云安全标准化建设，提升云服务整体安全保障能力。

1 国家学术信息资源云系统构建安全的标准化

目前，国内外诸多云安全标准化研究组织在开展云计算安全标准方面的工作。美国国家标准与技术研究院立足为云计算的高效应用提供标准服务，专注于为政府提供云计算安全相关策略与技术路线，于是先后推出《云计算标准路线图》《云计算参考体系架构》等。

ISO/IEC JTC1/SC27的云安全标准化推进主要集中在安全评估、身份管理与隐私保护、安全技术与机制、信息安全管理体系、安全控制与服务等方面，信息安全技术领域发布《供应商关系的信息安全》，内含云服务安全技术指南；信息安全管理领域发布《基于ISO/IEC 27002的云计算服务的信息安全控制措施使用规则》着重云计算环境下信息安全管理问题的解决；身份管理与隐私技术领域发布《基于ISO/IEC 27018公共云计算服务的数据保护控制措施实用规则》[2]。

云安全联盟重点关注云计算环境下最佳安全方法的确定，被广泛认可的《云计算关键领域安全指南》提出架构、治理和实施规则，还推出《云计算的主要风险》和云计算安全威胁的调查报告[3]。

我国云计算标准的研究正处于与国际标准融合的阶段，于2012年成立全国信息安全标准化委员会云计算标准工作组，负责我国的云计算标准化工作（涉及云安全框架、云安全技术、云安全服务和云安全管理）。

* 本研究得到国家社会科学基金重大项目“云环境下国家数字学术资源信息安全保障体系研究”（编号：14ZDB168）资助。

全国信息安全标准化技术委员会已完成《信息安全技术云计算服务安全指南》和《信息安全技术云计算服务安全能力要求》的草案。

从云安全研究现状看，国内外标准化组织主要集中于云安全机构、安全管理等基础或通用标准。欧美国家政府机构主要关注政府部门的云计算安全保障，行业标准化协会则关注云计算安全技术和互操作安全。国内外更多的云计算安全标准尚处于草案和试行阶段，国家学术信息资源云服务安全标准，需要从总体上进行构架。

学术信息资源云信息系统构建是云计算环境下国家学术信息资源建设的重要组成部分，虽然我国学术信息资源云信息系统构建的相关标准还未出台，但仍需开展相关工作，以保障云计算环境下信息系统的安全性及数据的可用性。传统信息系统安全标准已相对完善，信息安全等级保护管理方法从定级、备案、建设整改、等级测评和监督检查五个方面明确信息安全等级保护的工作步骤[4]。云计算环境下国家学术信息资源系统仍然具有传统信息系统的特征，国家学术信息资源云服务平台在进行安全保障的过程中可参考信息安全等级管理办法，落实云计算环境下国家学术信息资源云服务平台保护措施。

国家学术信息资源云信息系统的安全保障，需要明确学术信息资源云计算数据中心的安全保护等级以及安全边界。一般而言，云计算数据中心由多个信息系统组成，其正常运行需对多个信息系统的安全保护等级进行划分，对关键信息系统进行重点保护。因此，制定国家学术信息资源云安全定级标准很有必要。

无论是传统信息系统，还是云信息系统的构建都需要满足基本的安全建设要求。传统信息系统主要参照《信息系统安全等级保护基本要求》，对信息系统建设所涉及的基本安全防护要求进行规范[5]。国家学术信息资源云计算数据中心的构建，同样需要制定基本的安全防护参考规范。在此基础上，云计算环境下的国家学术信息资源系统应构建在管理、技术上的支持体系，明确面对新的安全风险情况下的基本防护要求。

学术信息资源服务机构和云服务提供方需要根据云信息系统出台的安全保护标准，对学术信息资源云计算数据中心的安全防护措施是否达到等级保护要求进行判定。目前，云服务已经在全球范围内开展，面向不同国家、不同领域进行应用，应对不同学术信息云用户的安全防护需求，就云安全的等级防护达成一致，从而开展广泛的云安全评估工作，促使云计算环境下信息系统的规范化实施。对于云计算环境下国家学术信息资源系统建设的协调与监督工作，也具有重要的标准化指导意义。

2 云计算环境下国家学术信息资源安全审查标准化

云计算环境下国家学术信息资源安全是国家信息安全的重要组成部分，我国面向国家安全以及公共利益的保障，推出网络审查制度。在审查过程中，将云计算纳入网络审查范围，通过云安全审查对云计算平台以及国家学术信息资源安全提供保障。云安全审查标准是推动云计算环境下国家学术信息资源安全审查的重要依据[6]。目前，我国云计算服务安全审查制度仍在不断完善，主要参考美国联邦政府的云计算服务安全审查制度（FedRAMP），通过建立云安全基线进行安全审查[7]。我国在借鉴美国安全审查经验的基础上，构建对于云服务提供商的安全审查依据，并制定《信息安全技术云计算服务安全能力要求》[8]。

云计算环境下国家学术信息资源建设要求各学术信息资源机构在面向公众的共享服务组织中，将学术信息资源数据迁移到云端存储。为保障云计算环境下国家学术信息资源数据的安全，需要云服务提供方对学术信息资源服务机构提供的云服务进行安全审查。云计算环境下国家学术信息资源建设参与的学术信息资源服务机构众多，为避免出现各学术信息资源服务机构重复审查的问题，拟由国家学术信息资源建设管理部门进行统一的安全审查。由学术信息资源服务机构参与，在参照相应规范的基础上构建云安全基线。由云计算环境下学术信息资源建设的管理部门或委托的第三方评估机构，对云平台提供的服务进行评估，并根据评估结果对云服务提供商进行安全审查；安全审查结果可对学术信息资源服务机构公开，以减少重复审查，提高云安全审查效率。

《信息安全技术云计算服务安全能力要求》对云服务提供商提出应具备基本安全能力的要求，其内容涉及云计算平台用户信息以及业务信息安全。上述标准的制定和执行，对云计算环境下国家学术信息资源安全保障具有重要意义[9]。在《信息安全技术云计算服务安全能力要求》的基础上，构建云服务提供商的安全审查要求（见表1）。

表 1 云服务提供商的安全审查要求

安全要求	安全要求描述
系统开发与供应链安全	在开发云计算平台时对云服务提供商提供保护和可靠的资源配置，同时对下级供应商进行安全管理
系统与通信维护	应保护云计算平台以及网络通信安全
访问控制	应进行用户身份标识及鉴别，并限制授权用户的可执行操作和使用功能
配置管理	对云平台进行配置管理
运营维护	定期维护云计算平台的设施、软件、技术、工具，并进行记录
应急响应与云灾备	为云计算平台制订应急响应计划、事件处理计划，确保灾备恢复能力
合规审计	应根据安全需求和用户要求，开展相应的合规审计工作
风险评估与持续监测	对云计算平台进行风险评估，并进行持续安全监测
人员管理	应确保与云业务和用户数据接触的相关人员履行其安全责任，对违反规定的人员进行处罚
物理与环境保护	确保机房位于国内（不包括港澳台），机房选址、设计、控制等符合相关要求

云计算环境下国家学术信息资源安全审查，需要在云安全审查的通用标准上进行拓展，针对云计算环境下国家学术信息资源安全的特征，在实践探索基础上建立规范。云计算环境下国家学术信息资源云存储的数据安全、用户隐私保护、跨云认证、知识产权保护等问题都需要进一步探讨，以确立符合实际和具有可操作性的云安全基线。

3 云计算环境下学术信息资源安全责任划分标准化

云计算环境下学术信息资源安全建设以及云服务提供的安全保障实施，一般由云用户和云服务提供者以基于协议的形式，对安全问题及相应的责任进行约定。目前，基于SLA的服务等级协议虽然可起到一定的约束作用，但在实际执行中云服务提供商通常无法达到预期的服务质量要求[8]。由于云计算环境下的调查取证困难，因此云安全责任认定常难以有效进行。在实施云计算环境下国家学术信息资源安全保障的过程中，需要与云服务提供商基于相关标准框架明确双方的信息安全保障责任与义务。

云计算环境下安全责任的划分与云计算服务模式密切相关，如SaaS、PaaS、IaaS用户承担的安全管理责任不同[10]。在不同的服务模式下，安全责任的边界和内容也不一样，越接近IaaS，云用户承担的安全责任越大。云服务模式与控制范围的关系如图1所示。

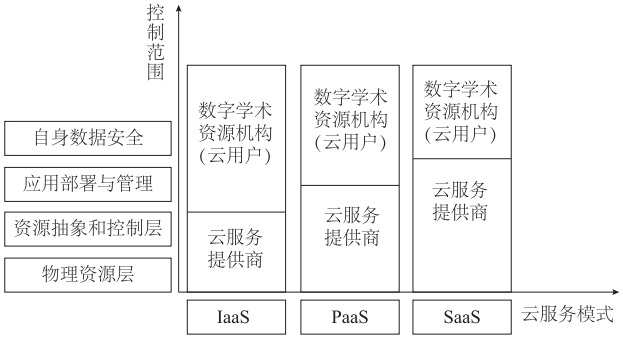

图 1 云服务模式与控制范围的关系

在SaaS中，云服务商需要承担物理资源层、资源抽象和控制层、操作系统、应用程序等的相关责任；用户需要承担自身数据安全、用户端安全等的相关责任。在PaaS中，云服务商需要承担物理资源层、资源抽象和控制层、操作系统、开发平台等的相关责任；用户需要承担应用部署与管理，以及SaaS中客户应承担的相关责任；在IaaS中，云服务商需要承担物理资源层、资源抽象和控制层等的相关责任，用户需要承担操作系统部署与管理，以及PaaS、SaaS中用户应承担的相关责任。目前，云服务提供商间的协同合作已成为一种趋势，为提高竞争力、优化资源配置，越来越多的云服务提供商采用其他供应商的产品与服务。如SaaS、PaaS服务提供商可能依赖于IaaS服务提供商的基础资源服务。在这种情况下，安全保障措施涉及云供应链中其他服务提供商的参与。因此，云计算安全措施的实施责任有四类，如表2所示。

表 2 云计算安全责任

责任方	实施责任
云服务提供商	在PaaS中，云服务提供商对云平台及相关工具进行维护
云用户	在IaaS中，云用户需要承担操作系统部署及管理
云服务提供商与云用户	制订应急响应、防护计划等由云服务提供商与云用户协商确定，共同承担责任
责任第三方	云服务提供商采用第三方提供商的软硬件服务，对风险进行转嫁，由第三方提供商承担相应的责任

云服务提供商所提供的云平台满足安全标准，并

不意味着云服务提供商的安全能力达到合同要求。一般而言，需第三方审计机构对云服务提供商进行测评，测评结果可作为云用户选定云服务提供商的参考[11]。当云用户通过评估选定云服务提供商，需要云服务提供商对其信息安全保障进行申明，使云用户迁移到云端的数据受到合理保护。

4 结语

云计算环境下国家学术信息资源安全面临诸多新的复杂问题，无法参照传统环境下的安全保障措施进行保护。云计算环境下国家学术信息资源建设中的安全标准建设和实施问题，需要在现有信息安全标准和云计算安全标准基础上，围绕国家学术信息资源云系统构建的安全标准化体系、云计算环境下数字学术信息资源的安全审查标准构架和安全责任划分标准完善进行标准化推进。同时，为进一步健全国家数字学术信息资源云安全标准化推进中的制度建设，实现学术信息资源数据迁移、存储、管理、开发，以及应用安全标准的采用，需从制度、系统和技术上全面实现。

参考文献

[1] 王惠莅,杨晨,杨建军.云计算安全和标准研究[J].信息技术与标准化,2012(5):16-19,27.

[2] 颜斌.云计算安全相关标准研究现状初探[J].信息安全与通信保密,2012(11):66-68.

[3] CSA.Securityguidance for critical areas of focus in cloud computing V3.0[EB/OL].[2017-05-27].https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

[4] 王文文,孙新召.信息安全等级保护浅议[J].计算机安全,2013(1):68-71.

[5] 公安部信息安全等级保护评估中心.信息系统安全等级保护基本要求:GB/T 22239—2008[S].北京:中国标准出版社,2008.

[6] 高林.关于云安全审查国家标准制定的思考[J].中国信息安全,2014(6):104-105.

[7] 顾伟,刘振宇.英美网络安全审查机制及其启示[J].信息安全与通信保密,2017(3):72-78.

[8] 何明,沈军.云计算安全测评体系研究[J].电信科学,2017,30(Z2):98-102.

[9] 云计算服务安全能力要求[EB/OL].(2015-05-08)[2017-06-10].http://wenku.baidu.com/view/3e5d836b19e8b8f67d1cb95e.html?from=search.

[10] 林闯,苏文博,孟坤,等.云计算安全:架构、机制与模型评价[J].计算机学报,2013,36(9):1765-1784.

[11] PATEL A,TAGHAVI M,BAKHTIYARI K,et al.An intrusion detection and prevention system in cloud computing: a systematic review[J].Journal of Network and Computer Applications,2013,36(1):25-41.

作者简介

万莉，女，1985年生，博士，讲师，研究方向：数字信息资源管理与服务，E-mail：393506143@qq.com。
吕美娇，女，1987年生，博士研究生，研究方向：信息安全，E-mail：416852559@qq.com。

Standardization Promotion of Digital Academic Information Resources Security under Cloud Environment

WAN Li[1], LV MeiJiao[2]
(1. School of Journalism & Communication, Nanchang University, Nanchang 330031, China;
2. School of Information Management, Wuhan University, Wuhan 430072, China)

Abstract: In the cloud environment, the security of digital academic information resource involves many organizations and social users in the service chain, and has multiple combinations of service features. Therefore, promoting the standardization of safety guarantee is a social problem. In this context, this article based on the reality at home and abroad, carried on analysis of academic resources cloud service system security standardization promotion from the national level; from the academic information resources security review, the division of security responsibilities for the organization and services of academic information resources, and the organization of academic information resources security guarantee, explored the promotion of the standardization; furthermore, put forward countermeasures and suggestions combined with reality.

Keywords: Digital Academic Information; Safety Guarantee; Standardization

（收稿日期：2017-07-06）