国家审计理论建设专栏

大数据时代电子政务云安全审计策略构建研究

王会金[a],刘国城[b]

(南京审计大学 a. 政府审计学院;b. 会计学院,江苏 南京 211815)

[摘　要]电子政务是实现国家信息化战略的重要基础。在大数据时代,电子政务云安全面临着严峻的挑战,数据泄密、账户劫持、系统漏洞等因素阻碍着政务信息化的发展。查错纠弊是审计的基本职责,云安全审计作为一种监督手段,有效迎合了电子政务云的安全管控需求。面对云计算的复杂性,如何建立一套成熟的电子政务云安全审计策略体系已成为亟待解决的热点问题。在理论回顾的基础上,设计电子政务云安全审计框架,确定电子政务云安全审计模式和技术方法,分析电子政务云安全审计风险的构成,探索基于基础设施安全、数据信息安全、应用服务安全、安全组织管理等模块的电子政务云安全审计机制,形成具有可行性、科学性的电子政务云安全审计体系。研究结论从审计视角为大数据时代电子政务云的安全管理实践提供了理论支持,是电子政务云安全审计策略构建的实践参考。

[关键词]大数据;电子政务;政务云;云审计;云安全;安全审计;云应用

[中图分类号]F239.43　　[文献标志码]A　　[文章编号]1004-4833(2021)04-0001-09

电子政务是国家机关在政务活动中,使用各类网络技术、现代信息技术与办公自动化技术为社会公众提供在线服务、信息发布以及互动反馈等功能的一种管理模式。电子政务云的发展需要大数据、云计算、区块链等智能科技的有力支撑。2016 年 12 月,国务院办公厅印发的《"互联网+政务服务"技术体系建设指南》中提出,促进云计算、大数据、物联网、移动互联网等在政务服务中的应用,不断提升政务服务便捷化、个性化、智慧化、安全化水平。在大数据时代,云应用是基于云计算的终端和云端互动的应用,其优势是跨平台性、资源整合、轻量性、易用性和节约成本,但也面临着计算机病毒、假冒窃听、内部威胁、业务欺骗、信息泄露等严峻的安全问题。审计具有查错纠弊、监督保障、促进管理等功能,以独立的第三方视角促进电子政务云安全建设是审计重要的业务内容之一。审计主体有必要紧跟大数据时代潮流,深入探索电子政务云安全审计的体系结构与运行机制,力求推进电子政务云安全管理的动态化、立体化与智能化。

在网络安全、信息安全以及云计算安全受到极大威胁的大数据时代,电子政务云的安全问题亟待学界的高度关注。电子政务发展至今已经历网络建设、系统建设和数据赋能三个阶段。与其他云安全审计比较,电子政务云安全审计的内容不仅包括互联网、政务外网、政务专网、政务内网等方面的安全审计,而且涵盖有关电子政务的云辅助决策系统、云政务服务系统、云生态监测系统、云市场监管系统和云社会管理系统等方面的安全审计,且应包含有关电子政务云的数聚、数享与数治等方面的安全审计。当前,我国缺乏一套成熟的信息系统安全审计体系与经验,电子政务云也不例外。在大数据时代,对电子政务云安全审计策略开展系统性研究,具有重要的学术价值,具体表现为:(1)借鉴和吸收国内外相关思想,能够科学建立适用于电子政务云特色的信息安全审计标准;(2)基于工程学视角,分析电子政务云的安全审计框架,将会拓展政务云安全审计模式;(3)基于免疫监视思想,研究安全风险的构成及其评价,将会丰富政务云审计监控方法;(4)基于系统论视角,将云审计规范、云风险估计、云审计模块、云取证机制、云漏洞防御等要项整合于一体,分析彼此之间的逻辑关联,探索整体和局部的辩证关系,提炼整体功能与价值的普遍性规律,建立电子政务云安全审计理论体系,能够创新电子政务云安全审计理论。

[收稿日期]2021-04-05

[基金项目]国家社会科学基金项目(17BJY213);江苏高校哲学社会科学研究重点项目(2018SJZDI102)

[作者简介]王会金(1962—),男,浙江东阳人,南京审计大学党委副书记、副校长、政府审计学院教授,博士生导师,博士,从事审计理论与实务的研究,E-mail:whjwc@nau.edu.cn;刘国城(1978—),男,内蒙古赤峰人,南京审计大学会计学院教授,博士,硕士生导师,从事云审计理论的研究。

一、文献回顾

电子政务云是将传统的政务应用迁移至云系统中,基于云技术对政府功能实施再造,并依托 IT 技术在云中实现流程办理以及服务职能的信息化平台。安全是电子政务云有效运行的前提。当前,针对电子政务云安全的文献主要集中于:(1)风险分析。姜茸等认为电子政务云安全风险来源于应用服务层和云终端,主要体现在虚拟化、API、软件漏洞等方面[1];刘国城认为电子政务云安全风险集中于管理、实施、安全等领域,并分属于"开发与获取""人员管理"等若干要项[2]。(2)控制技术。胡俊等基于推理和角色的访问控制技术设计云政务系统的混合访问控制模型[3];池亚平等基于 OpenStack 与 Shibboleth 的 Keystone 安全组件技术,建立一种细粒度的电子政务云跨域访问控制系统[4]。(3)保障策略。黄瑞锋和张会宁等建立电子政务云关键服务的 OWL 描述机制以及云用户任务的安全调度策略[5-6]。(4)监管政策。在电子政务云安全监管政策方面,欧盟制定《政务云安全框架》、美国出台《云安全指南》[7]、日本发布《信息安全管理基准》[8],相关标准能够为我国构建电子政务云安全管理框架提供借鉴。

云安全审计是以现代审计理念为核心,跟踪云用户行为,揭示云应用漏洞,改善云计算性能,对云规程及其应用政策开展全过程监督的活动。有关云安全审计的理论研究较为分散,尚未形成完整的体系。在云存储安全方面,秦志光等基于双线性对技术和默克尔哈希树提出分层次索引结构的动态数据完整性存储审计方案[9];徐洋等针对云端大数据安全存储问题,基于代数签名技术提出数据持有性审计策略[10];邵必林等基于数据的可恢复证明、持有性证明和所有权证明设计云存储安全审计协议[11]。在云日志安全方面,赵春晔等和郭涛敏等采用改进的关联规则挖掘算法分析云用户行为日志的异常信息,建立云日志安全审计方案[12-13]。在云外包数据安全方面,柳玉东等基于字符串相等检测协议制定面向全生命周期的云外包数据安全审计措施[14]。云安全审计面临着多层服务、多租户、虚拟化、跨域共享等方面的挑战[15-16],为提升云安全审计质量,有必要科学搭建云安全审计平台[17],该平台的优势是增加云安全审计效率、提升云安全的保密性、降低云审计风险以及保障云安全审计数据传输的通畅性[18]。

电子政务云安全审计是对电子政务云的内外部用户行为进行全过程监督,对电子政务云操作步骤开展全过程追踪,监测安全漏洞和滥用行为,捕捉电子政务云用户异常轨迹,记录电子政务云安全事件,以强化对电子政务云安全的控制与管理[19]。通过文献梳理我们发现,学术界在电子政务云安全以及云安全审计等方面已取得一定的积累,但有关电子政务云安全审计的理论文献还极为匮乏,难成体系。尽管政务大数据实现了云操作,但电子政务云在每一构成要素上都面临着严峻的威胁。审计具有成熟的理论与方法,以审计为视角探索电子政务云安全问题,将会通过交叉领域融合研究进而推动学术理念创新。

二、理论分析

从审计的本质来看,美国会计学会(AAA)1972 年发布的《审计基本概念公告》中提出的审计系统过程论得到学术界的普遍认可,该观点认为"审计是以客观性要求收集和评价与经济活动事项相关认定的证据,并确定其与既定标准的相符程度,最终把结果向利益相关者传递的系统性过程"。审计的系统过程论概括地说明了审计对经济活动事项如何查、怎么查等问题。在实施恰当的审计程序并获取充分、适当的审计证据后,审计可对鉴证业务提供高水平的合理保证,即审计的本质是审计对经济事项的鉴证、评价和监督作用。在此作用下,一方面,审计的信息理论认为审计可以使经济信息更加可靠;另一方面,审计的受托责任理论认为审计由委托方、受托方和审计机构的三方关系产生,是一项独立的经济监督活动,通过审计可实现委托方对受托方的监督。

电子政务云是在数字化背景下发展形成的一种政府经济活动数据生成系统,该系统可通过应用集成平台和数据交换平台协调多层级政务云平台。与审计的信息理论对应,电子政务云生成的数据信息在当前数据要素市场化配置改革的制度安排下,政府云数据已经逐渐由"上云"转为"云上",政府云建设重点向基层政府转移,这在一定程度上说明了政府云数据的内部共享协同进一步扩大;同时,政府云数据开放的广度也逐渐提高,有试点城市已经面向社会开放相应数据,通过政府云数据与社会数据融合以最大化数据要素价值。然而,可靠性是数据价值的"灵魂",对电子政务云的构成要素进行安全审计可以对数据生成的过程控制进行评估与测试,发现数据生成过程的安全漏洞,改善数据生成系统性能,最终提高政府内部数据利用效率以及政府云数据与社会数据

的融合效率，从而增进数据要素价值。此外，与审计的受托责任理论对应，若把各层级政府看作分级的委托代理关系，参与电子政务云的政府部门一定程度上可以看作政务云系统中执行数据生成与交换的代理人，上级政府可以看作统筹参与政务云系统的政府部门以生成可靠经济信息的委托人。若要保证电子政务云系统运行的有效性，委托人可聘请独立的审计机构进行审计鉴证以保证电子政务云系统生成信息的可靠性。对电子政务云的安全审计可捕捉电子政务云内外部用户的异常轨迹，发现代理人用户的道德风险行为，也即安全审计作为独立的经济监督，可强化对电子政务云系统安全关键要素的控制与管理。因此，电子政务云的安全审计可充分发挥审计的鉴证、评价与监督作用，既能增进数据要素价值，又能加强对电子政务云的控制，保证电子政务云系统的有效运行。基于此，本文从基础层、应用层和体系层着手设计电子政务云安全审计框架，并开展有关电子政务云安全审计方向的学术研究，以期为电子政务云安全管理实践提供理论与现实支持。

三、电子政务云安全审计框架设计

对电子政务云安全进行审计是一项复杂的工程，应遵循独立性、客观性、整体性、重要性、相关性和可操作性等原则。电子政务云安全审计框架是包含在理论系统内的各个基本要项的集合体。设计电子政务云安全审计框架应该包含审计模式、审计方法、风险分析、模块取证、审计体系等要素，它们具有整体性、抽象性和前瞻性等特征，并在总体框架之下相互作用、运行有序、辩证统一[20]。本文尝试构架大数据时代电子政务云安全审计框架，如图 1 所示。电子政务云安全审计框架由基础层、应用层和体系层三部分组成。基础层以电子政务云安全审计的本质属性为基本导向，涵盖审计模式、审计技术、审计方法等内容。应用层以电子政务云安全审计的业务特征为逻辑起点，涵盖固有风险分析、控制风险分析、检查风险分析、审计模块取证等内容。体系层以电子政务云安全审计的体系建设为发展动力，涵盖审计标准规范、风险评价流程、审计取证机制、漏洞防御机制、威胁监测机制等内容。基础层是电子政务安全审计事项的根基与起点，应用层是电子政务安全审计过程的演进和实施，体系层是电子政务安全审计经历的凝结与整合。基础层、应用层、体系层三者之间相辅相成，有机演进，在理论中寻求指引、明晰方向，从实务中发现问题、积累经验、总结规律，促进电子政务云安全审计知识创造，并进一步通过理论和实践的深度融合进而推进云安全审计理论的丰富与完善。

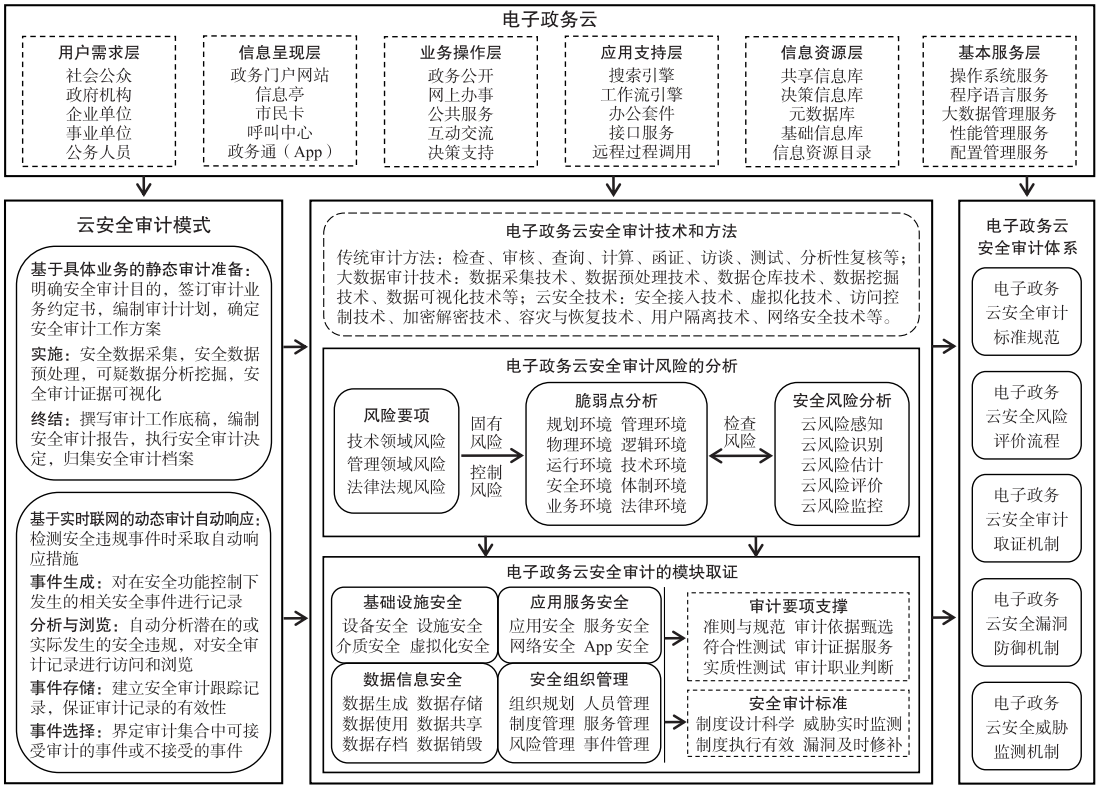

图 1　大数据时代电子政务云安全审计的体系架构

四、电子政务云安全审计基础层要素设计

从电子政务云安全审计基础层要素的分解来看,电子政务云安全审计基础层包含审计模式、审计技术方法等体现云安全审计本质属性的要素。

(一)电子政务云安全审计的模式

电子政务云安全审计模式有两种类型以供审计主体参考和借鉴。一是基于具体业务的静态审计。该种模式经历如下过程:(1)准备,内容涵盖明确审计任务和重点、签订审计业务约定书、判断重要性水平、编制审计计划和具体方案等;(2)实施,主要是通过对有关电子政务云安全的大数据进行采集、预处理、分析和可视化,开展符合性测试与实质性测试,识别云风险,发现云漏洞,并对取证资料的充分性、客观性、合规性等方面进行分析和鉴定;(3)终结,内容涵盖整理工作底稿、编制安全审计报告、执行审计决定以及促进审计整改。二是基于实时联网的动态审计。该种模式经历如下过程:(1)自动响应,主要是指当被审事项遇到潜在攻击时所采取的自动响应措施,如进行实时报警、中断服务或终止违例进程等;(2)事件生成、分析与预览,内容涵盖对在安全功能控制下发生的相关安全事件进行记录,定义可审计事件清单,在线自动分析潜在的或实际发生的安全违规操作,对系统形成潜在攻击的特征事件进行匹配,以及授权云用户对安全审计记录进行访问和浏览;(3)事件存储与选择,内容涵盖建立安全审计跟踪日志并保证审计存储的有效性,界定审计集合中可接受审计的事件或不接受的事件,并要求审计系统提供相应的安全控制措施。

(二)电子政务云安全审计的技术方法

电子政务云安全审计技术和方法既包含传统审计方法,又包括大数据审计方法,还应融合云安全技术。传统审计的基本方法有详查法、抽查法、顺查法、逆差法、函证法、测试法、审阅法、核对法、复核法和盘存法等,辅助方法有访谈法、推理法、归纳法和分析性复核等。在大数据时代,电子政务云安全数据将大批量地以图片、文档、文本、日志、图像、音频、XML、HTML 等异构化方式呈现。有关电子政务云安全的结构化数据能够运用二维表结构表达并实现,它们存储于 Oracle、SQL Server、MySQL、Access、DB2 等关系型数据库中,审计主体运用常规检索方法便可实现对它们的单表检索、多表检索以及多库检索。然而,有关电子政务云安全的非结构化数据具有多源异构等特点,它们无法运用关系型数据库中的二维表结构进行逻辑表示,审计主体运用大数据采集、预处理、分析、可视化等方法开展审计取证将会取得更为理想的效果。大数据采集涵盖 OA、网络爬虫、字段式过滤、元搜索、射频识别等技术,大数据预处理涵盖分布式存储、云清洗、标签抽取、数据加载等技术,大数据分析涵盖自然语言处理、文本挖掘、机器学习、聚类分析等技术,大数据可视化涵盖散点图、标签云、维入栈、流式地图等技术,它们构成大数据审计技术体系,共同推进电子政务云安全审计取证。此外,审计主体还需精通政务云安全技术,如安全接入技术、虚拟化技术、访问控制技术、加密解密技术、容灾与恢复技术、用户隔离技术、网络安全技术、防火墙技术、软件开发技术、Web 应用技术等,它们反映着电子政务云的生成逻辑,运用上述技术对有关疑点开展实质性测试,极大地方便了对审计证据的确认和获取。

五、电子政务云安全审计应用层要素设计

从电子政务云安全审计应用层要素的分解来看,电子政务云安全审计应用层包含风险分析、审计模块取证等体现云安全审计业务特征的要素。

(一)电子政务云安全审计的风险分析

美国注册会计师协会(AICPA)在 1983 年提出传统审计风险模型,即审计风险 = 固有风险 × 控制风险 × 检查风险。风险导向模式下,电子政务云安全审计风险由固有风险、控制风险和检查风险三要素构成。基于电子政务云安全的固有风险是指在不考虑内部控制的情形下,电子政务云因自身问题或环境因素而发生重要安全事件以及产生重大安全损失的可能性。有关电子政务云安全的固有风险集中在技术、管理和法规等领域。基于技术领域的固有风险寓于 IaaS 层、PaaS 层和 SaaS 层之中,其中,IaaS 层技术风险主要包括虚拟机内部资源冲突、虚拟机之间相互攻击、虚拟机之间及其与外部系统之间的通信风险、数据存储及迁移中的安全风险、虚拟机监视器安全漏洞及其访问权限被非法用户截取等内容;PaaS 层技术风险主要包括因组件失效、多用户并发访问、服务器频繁增减等方面引发的数据处理风险以及因开发环境不安全、编程模型不明确、编程接口过于复杂等方面引发的云开发风险;SaaS 层

技术风险主要涵盖多租户架构下的应用隔离风险、补丁与应用程序不兼容、客户端外设端口引发数据泄露以及数据传输风险等方面。基于管理领域的固有风险主要涵盖服务终止、权限管理混乱、安全边界不清晰、数据归属不明确、内部人员恶意操作以及供应链中断等方面。基于政策领域的固有风险主要涵盖滥用特权、隐私数据保护不当、服务等级协议违反、治理政策不一致、隐私保护风险、政策遵从性风险以及责任界定风险等方面。上述风险由其所处环境及其自身性质所决定,同电子政务云安全审计风险呈正比例关系,并独立于内部控制活动。

基于电子政务云安全的控制风险是指电子政务云发生某类重大安全事件,但该事件未被内部控制及时发现并纠正的可能性。有关电子政务云安全的控制风险由两个方面构成,一是电子政务云内部控制制度设计的健全性与科学性,二是电子政务云内部控制制度执行的有效性与时效性[21]。当前,电子政务云管理者极为关注硬件和业务流程方面的建设,但对内部控制建设却有所忽视。有关内部控制建设问题需要引起政府部门、云平台建设商、云应用开发商、云服务运营商等多方主体的共同重视。内部控制建设滞后,内控体系运行不畅,有关条款笼统模糊或者错误疏漏,内控执行力度不足,都将引发控制风险,进而无法基于本质层面防御固有风险。

基于电子政务云安全的检查风险是指电子政务云存在某类重大安全事件,但审计主体为将审计风险降至可接受水平而实施相关程序后没有发现该类问题的可能性。检查风险与审计业务操作的有效性直接相关,也是审计主体唯一能够控制的风险要素。电子政务云安全审计检查风险的影响因素涵盖审计人员的职业判断能力、审计方案的科学性、审计证据的适当性、审计技术的适当性、审计依据的适当性、符合性测试的恰当性、分析性审核的合理性以及审计抽样的合理性。大数据时代电子政务云安全审计涉及公共管理学、审计学、大数据科学、云计算科学、安全科学等多学科领域知识,其业务特色要求审计主体必须精通上述学科领域的知识。然而,培养兼备多学科知识的审计人才是一个长期的过程,加之目前尚无成熟的安全审计规范以供借鉴,因此,对于如何降低电子政务云安全审计的检查风险问题,还有待于审计主体的高度重视、统筹规划和多措并举。

总的来看,分析电子政务云安全审计风险所遵循的基本思路是明晰各类风险的构成,感知“固有风险源”,调查“控制风险源”,审核“检查风险源”,挖掘关键风险诱因,判别是否具备风险转化条件,做好风险识别,建立风险模型,估计风险发生的概率与后果,实施风险评价。结合人机工程学思想,电子政务云安全审计风险“源”来自于人、机、环境三要素,人的因素是指有关电子政务云安全及其审计的各方参与者因自身的生理、心理以及可靠性等问题而引发的风险,机的因素是指因电子政务云中各项物件的设计问题而引发的风险,环境的因素是指因业务、规划、管理、运行、技术、安全、物理、逻辑、体制、法律等方面的环境问题而引发的风险。审计主体应针对每一风险要项,分别从人、机、环境三方面着手,揭示可能对电子政务云系统造成损害的潜在攻击或风险事件,发掘可能会被威胁利用并对电子政务云资产造成损害的薄弱环节或瑕疵,基于威胁和脆弱性甄别电子政务云所蕴含的各种安全风险。针对特定的电子政务云安全审计风险,不同的诱因对应着不同的风险转化条件,且风险可能导致的后果也有所差异。对此,审计主体可通过如下方法做好对电子政务云安全审计风险的有效识别:其一是分解法,即将风险诱因及其后果进行多层次细分,由大系统分解成小系统;其二是故障树法,即运用图解的形式对审计风险诱因及其逻辑关联做出形象的描述;其三是情景分析法,即通过数字、图表和曲线等形式,描绘电子政务云安全审计风险在某种状态下的动态发展趋势,进而对关键动因及其影响程度的未来变化作预测和判断。风险估计是审计主体以历史资料为基础,对发生云安全审计不利事件的可能性以及造成的损失采用概率统计等方法进行定量估计的过程,包含确立评估范围、系统调研、确定评估方法、制定评估方案等步骤。因风险影响要素之间具有多种组合方式,审计主体可选用二维矩阵或交叉相乘等方法对风险估计开展运算。风险评价是风险估计活动的深化,审计主体需要事先划分风险评价等级,并对风险估计结果进行等级化处理,进而明确风险监控措施。对不利事件发生概率进行评价,应充分考虑脆弱性被利用的难易程度、攻击设备能力、攻击者的专业技术程度以及资产吸引能力等因素。对不利事件损失进行评价,应充分考虑云资产本身、业务延续性以及对政府部门的影响程度等因素。审计主体需要权衡电子政务云安全审计风险控制成本与风险估计值之间的关系,并确定一个可接受的风险范围。对于可接受范围内的风险,保持原有的风险管理措施。对于超出可接受范围的风险,则通过修正原有措施或构建新措施对固有风险、控制风险和检查风险进行管控,并对各类风险的发展和变化实施全程监测。

(二)电子政务云安全审计的模块取证

1. 基础设施安全审计分析

电子政务云基础设施由物理基础设施资源和虚拟基础设施资源组成。物理基础设施安全包含设备安全、设

施安全、介质安全及它们所处的环境安全。虚拟基础设施安全是指以虚拟化技术为中心所构建的虚拟资源的安全[22]。对于电子政务云物理基础设施安全审计,审计主体应从人为因素或自然因素视角出发,对设备、设施、介质的状态及运行活动进行审查和评价,并就其真实性、正确性、有效性、合规性和合法性发表客观公正的审计意见。针对设备设施自身是否安全,审计主体首先应基于设备标识、锁定装置、监控报警等方面察看防盗和防毁情况;其次是基于屏蔽防护、干扰防护、抑源防护、隔离防护、滤波防护等方面审查防电磁泄漏情况;再次是基于调整器、UPS、操作规程等方面审查电源保护情况;最后是基于设施维护、设备处置、设备复用、设备转移等方面审核设备保护情况。针对介质安全审计,需要审查介质的防自然损害情况,查看是否建立有效的级别和权限,核验介质的备份、转移、清除和销毁是否遵从有关制度,查看涉密存储介质是否在非涉密计算机中使用以及是否采取有效的技术防范。此外,安全可靠的运行环境是物理基础设施安全的重要内容之一,审计主体需要在分析安全综合部署策略科学性的基础上,判断机房选址是否合理以及电能供给是否充足,测试防水、防火、防雷击、防鼠害、防静电等工作细节是否到位,审验湿度、温度、洁净度是否达到有关规定的要求,并进一步提出审计整改方案。

虚拟基础设施涵盖宿主机、虚拟机、虚拟机监控器、客户机等组件。虚拟基础设施的安全问题不仅来自于虚拟机之间、虚拟机与宿主机之间以及虚拟机控制中心等方面的安全威胁,而且来自于虚拟机蔓延的风险以及云虚拟化安全管理疏漏。有关电子政务云虚拟基础设施的安全审计有必要从宿主机安全、虚拟机安全、虚拟机监控器安全三个方面入手。首先,审计主体应测试宿主机系统的安全性,尝试直接使用宿主机系统的快捷键监控虚拟机资源的使用情况,或尝试获取存储在宿主机中的虚拟机镜像文件,检查宿主机在远程管理、补丁更新、访问控制、入侵监测等制度设计方面的严谨性,判断攻击者利用宿主机攻击虚拟机的可行程度。其次,审计主体应强化对虚拟机在隔离、监控、防护等方面的取证,测试虚拟机之间的隔离能力是否在最大程度上降低彼此干扰,关注云管理中所部署的虚拟机安全监控框架的固有缺陷及其完善策略,判断虚拟机之间的二层流量交换是否为合法访问以及有关访问中是否存在恶意攻击行为。最后,审计主体应检查虚拟机监控器安全机制的健全性,检测是否采用可信计算等技术对虚拟机监控器进行完整性保护,审查是否通过规范管理员操作或加强防火墙防护等方式多维度构建虚拟机监控器的安全防御体系。

2. 数据信息安全审计分析

近年来,通过安全审计发现,电子政务数据信息安全治理中存在的问题主要体现在数据信息安全工作统筹管理薄弱,数据信息安全治理工作规范性不足,数据信息安全有效防护措施不到位,数据信息安全应急处置能力欠缺以及数据信息安全技术防护水平不高等方面。数据信息安全审计的基本任务是基于安全生命周期对数据信息的机密性、完整性和可用性进行取证,及时发现薄弱环节,并提出改进建议。电子政务云数据信息的安全生命周期包含生成、存储、使用、共享、存档、销毁等阶段,每一阶段都面临着不同程度的安全问题。针对数据信息的生成,审计主体应评估篡改用户数据或修改用户权限进而促使用户丧失权利的可能程度,检查是否划分数据安全级别并建立识别标签,察看是否对数据实施权限管理且进行预处理。针对数据信息的存储,审计主体首先应测试数据存放的位置是否准确,传统的安全域划分是否有效,网络传输服务是否顺畅,静态存储是否安全,动态存储是否机密以及是否存在数据存储的去重攻击与欺诈资源消费攻击;其次,云存储的安全控制方法主要集中于数据加密、密钥管理、密文检索、访问控制等方面,其中,加密算法分为对称密码和非对称密码,密钥管理分为初级密钥管理、二级密钥管理和主密钥等管理,密文检索分为结构化数据、半结构化数据、非结构化数据等不同形式的检索,访问控制分为自主访问控制、强制访问控制和基于角色的访问控制。审计主体应基于上述各类方法的不同特点和应用场景,检查它们在电子政务云存储应用中的科学性,审查相关制度在设计上的科学性以及在执行上的有效性,并监督电子政务云存储层下数据安全服务目标的实现情况。

数据使用是指云用户通过终端界面开展数据访问与检索,或对数据进行增减、修改、删除等操作。针对数据信息的使用,审计主体需要从身份识别、访问控制、资源监控、制度遵从等视角审查是否对用户身份进行严格审查,合法用户是否存在非法操作,是否存在安全漏洞使得攻击者能够恶意访问数据库以及是否存在注入式攻击、跨站点脚本、伪造的跨站点请求、未经验证的重定向和转发等情况。针对数据信息的共享,审计主体应评估共享数据是否有遗失、泄露、损坏或被篡改的可能性,检测云管理者是否通过日志文件或特定代理工具对数据共享活动实施监控,是否对邮件、App、数据库、文件系统等设计完备的加密方案,是否出台完善的制度以强化对共享数据的安全搜索和安全编辑。针对数据信息的归档,审计主体应检查非现行的数据档案是否始终保持在“稳定状

态”,审查云管理者是否采取高级保护技术或加密技术遏制档案泄密,是否采用严格的服务水平协议对云归档服务公司进行制约以及是否建立成熟的云档案安全管理制度。针对数据信息的销毁,审计主体应测试无效数据是否被云服务商真正删除以及销毁后的数据能否被重新恢复,审查基于时间的可信删除、覆写、强磁场销毁、整体高温销毁等方法在实践中是否得以正确应用,介质中的数据残留是否被彻底擦除以及是否严格遵守数据信息销毁管理规定。

3. 应用服务安全审计分析

云应用服务是完成业务逻辑或运算任务的特定应用及服务,是云计算技术在云应用层的具体体现。电子政务云应用服务是指终端用户通过网络与云端同步互动,以按需、易扩展的方式获得所需服务。电子政务云的应用服务安全包括系统服务安全、软件应用安全、网络安全和 App 安全。对于系统服务安全审计,审计主体应开展有关电子政务云平台自身的环境、性能、功能、架构、系统以及电子政务云应用程序的质量等方面的审计取证,采用面向云的回归测试技术检测电子政务云自身的可扩展性、兼容性、连通性、安全性和用户隐私保护程度,运用端到端应用系统回归测试技术检测电子政务云应用程序的兼容性、可伸缩性以及端到端的互操作性、功能性、集成性和安全性,评价云计算的可靠性、云平台的可维护性与云资源的访问控制。软件应用安全审计聚焦于软件功能、软件安全和软件维护三个方面。针对软件功能审计,审计主体应选取吞吐量、响应时间、资源使用率、最大并发用户数、聚合宽带等评价指标,采用负载测试、并发测试、压力测试、容量测试等方法,运用云环境模拟实际用户使用负载,审查软件的强度及整体性能。针对软件安全审计,应选用模糊测试、基于故障注入的安全性测试、基于故障树分析的安全性测试、基于 Petri 网的安全性测试等方法发现软件的安全漏洞,检测是否存在破坏软件保护机制、故意导致软件失败、设法截取软件口令、伺机非法侵入等恶意行为,审查软件的安全功能运行是否与安全功能需求相一致。针对软件维护的审计,应分析软件的适应能力和持续服务能力,审查软件功能是否易于增减以及软件故障是否能够在规定的时间内及时修复,评价软件服务的稳定性与易修正性。

当前,网络安全形势面临着严峻的挑战,内部威胁、网络攻击、隐私泄露等各类安全事件频繁发生,网络安全问题亟待重视。对于网络安全审计,审计主体应对拒绝服务攻击、中间人攻击、网页篡改、网络嗅探、端口扫描、跨站脚本攻击、CC 攻击等问题开展实质性测试,审查电子政务云管理者在事前是否检测用户访问 Web 应用的权限,在事中是否对 Web 异常行为开展实时监控以及在事后是否识别并拦截各类攻击行为,对是否在第一时间修补 Web 漏洞进行取证,判断协同云管理者共同建立科学的预警响应机制。此外,防火墙是集网页保护、网络防护、应用交付、负载均衡于一体的网络整体安全防护技术,其能够有效抑制来自网络的攻击。审计主体应测试 Web 应用防火墙的适用性和有效性,浏览防火墙中的日志记录并查找潜在的安全威胁,审查其是否及时得以修复或加固升级,而且还需检查云管理者是否对防火墙无法解决的安全问题建立完善的防控机制。对于 App 安全审计,审计主体应关注静默下载、山寨应用、恶意传播、隐私窃取、远程控制、系统破坏、窃取资金、跨平台感染等移动应用中的恶意行为,对 App 开展漏洞扫描和渗透测试,审查 App 应用是否存在不安全的身份授权、逆向工程、无关的功能以及代码质量问题等情况,评价云 App 应用下的安全防护策略,基于审计视角提出 App 安全加固方案。

4. 安全组织管理审计分析

组织管理是为实现预定目标而对所属资源进行计划、组织、领导、控制的过程。有关电子政务云的安全组织管理建设需要从组织规划、人员管理、制度管理、服务管理、风险管理、事件管理等方面着手,并应经历准备阶段、风险识别与评估阶段、云安全组织管理体系文件建立阶段以及云安全组织管理体系运行与完善阶段。针对组织规划问题, 首先,审计主体应关注云管理者是否制定明确的安全管理策略体系,如动态安全防护策略、内容安全策略、监控及告警策略等,检查各项安全策略是否配有明晰的技术解决方案,测试相关策略之间的一致性与协作性。其次,有关电子政务云安全管理的组织体系包含领导体系、指导体系、执行体系和监督体系,审计主体应关注各体系间的差异,审查不同体系下相关部门的权责分配是否科学以及相应的保障是否到位。针对人员管理问题,审计主体所应关注云管理者如何对维护和保障电子政务云服务正常运转的所有内部人进行管理,检查职务职责确定、岗位候选者审核、任用合同签署等人员任用前的相关流程是否符合规范,审查安全知识培训、安全技能考核、违规违纪处罚等人员任用中的相关措施是否制定科学,察看任用终止或变更的人员是否及时撤销访问权以及限期收回资产。针对制度管理问题,审计主体应关注云管理者是否建立完善的电子政务云安全制度体

系,如弹性计算应用接口制度、数据存储制度、服务质量测评制度、安全能力评估制度、云资源监控制度等,审查安全制度中对目的、范围、职责、规则、指标、流程等要素的阐述是否清晰准确,测试各项安全制度是否得以有效落实。

对云服务进行管理旨在确保云用户隐私安全、提高服务适应性以及增强服务可用性。针对服务管理问题,审计主体应分析云管理者是否具备快速高效的配置能力、灵活弹性的处理能力、广谱实时的检测能力和业务全程防护能力,运用职业判断对云服务程度开展度量,判断服务接口、服务交付、服务运营、服务安全等方面的管控措施是否科学,测试服务目录管理、服务级别管理、服务持续性管理、服务变更管理、服务事项管理、服务请求管理、服务组合管理等活动是否执行到位。针对风险管理问题,审计主体应测试云风险管理岗位职责是否明确,审查云管理者在风险规划、风险识别、风险分析、风险监测等方面的做法是否合情合理,云风险管控措施是否正确高效。1987 年,美国卡内基·梅隆大学提出能力成熟度模型(CMM),并将能力成熟度分为初始级、可重复级、已定义级、已管理级和优化级。审计主体有必要借鉴 CMM 理论,测评电子政务云的风险管理能力成熟度等级,评价风险管控水平,并就如何实现向更高成熟度层级跨越提供建设性思路。针对事件管理问题,审计主体应关注云管理者是否建立安全事件应急工作机制,检查是否对安全事件及其预警进行分级管理,测试设备故障、信息破坏、有害程序、网络攻击等各类安全事件的预警监测策略和应急响应措施是否适当有效。对电子政务云安全事件管理活动开展审计,有助于推进云管理者更好地归纳安全事件背后所隐藏的深层次问题并总结规律,有益于全面把握电子政务云安全变化趋势,进而能够在最大程度上抑制电子政务云安全事故的频繁发生。

六、电子政务云安全审计体系层要素设计

体系是指特定范域内的事物按照一定秩序组合而成的整体。电子政务云安全审计体系层的要素构成主要涵盖:(1)安全审计标准规范。审计主体应基于云安全特点、服务模式(IaaS、PaaS、SaaS)、参与者角色(云基础网络运营商、云客户、云代理商、云服务商)等方面制定有关于电子政务云安全审计的基本要求、参考框架、实施指南、能力标准、技术规范以及管理基准,以此促进审计的标准化和科学化。(2)安全风险评价流程。审计主体应熟知电子政务云安全风险构成,依托层次分析法科学确立安全风险评价指标体系,采用统计、运筹学、系统工程、模糊数学等方法建立若干评价模型,明确它们的使用范围,并确立相应的评价标准,基于不同情形构建各类风险的评价测试流程。(3)安全审计取证机制。审计主体应根据图 1 中各类模块的任务需求、功能需求和策略需求遴选合适的数据挖掘工具与算法,全方位集聚审计依据,精炼审计证据测试、核验、分析及评价流程,构造明晰的证据链条,以充分恰当、客观公正、合法细致为主线构建电子政务云安全审计取证机制,有效推进审计取证中的职业判断、模式发现、知识创造与流程智能。(4)安全漏洞防御机制。漏洞检测技术有动态和静态之分,前者是在程序运行中注入测试数据寻找漏洞,后者是通过分析程序特征寻找异常行为或者使用特定验证技术测试程序的合规性。审计主体需要以技术为中心,构架有关电子政务云安全漏洞的“入侵特征库”“攻击工具库”“技术规程库”“防御流程库”“补丁库”等,全面建立安全漏洞防御机制。(5)安全威胁监测机制。审计主体应基于不同的任务和需求,制定预警规则,界定预警等级,确立安全威胁监测模型及其算法,建立有关电子政务云安全威胁监测的运行实现系统、知识服务系统、可视化处理系统、应急响应系统以及决策支持系统。

七、结束语

2016 年至今,《“十三五”国家信息化规划》与《国家电子政务“十三五”规划》相继发布,两个文件共同提出建立完善政府信息系统安全管理制度规范,防范和化解新技术应用带来的潜在风险,制定政务部门计算机安全配置和审计制度,建立信息系统安全检查制度,加强信息安全检查工作力度,大力提高电子政务信息安全保障水平,提升网络安全保障能力。审计主体需要顺应电子政务云动态监管的迫切要求,并将“大数据科学”引入电子政务云安全审计之中,构建电子政务云安全审计法律法规体系,科学设计电子政务云安全审计框架,完善电子政务云安全审计实施指南,合理遴选电子政务云安全审计模式,明晰电子政务云安全审计技术和方法,准确评估电子政务云安全审计风险,深化有关基础设施安全审计、数据信息安全审计、应用服务安全审计以及安全组织管理审计等模块的流程再造,优化电子政务云安全审计体系,提高电子政务云安全审计检查效果,明确电子政务云安全审计人员要求,以便从全局视角求证电子政务云安全审计问题的解决之道。

本文是一种探索性研究,不足之处主要涵盖:(1)仅从宏观方面对电子政务云安全审计问题开展理论分析,缺少微观层面的实证探索;(2)受篇幅所限,在电子政务云安全审计具体模块的论证中,缺少更为生动的案例阐释。未来进一步研究的方向:(1)从尽可能多的体系要素视角丰富电子政务云安全审计建设的理论体系;(2)从尽可能多的监控机制视角探析电子政务云审计运作的深层次作用机理;(3)探求电子政务云安全管理过程的细节,获取尽可能多的实践数据,收集更为丰富的实务案例,从经验数据中挖掘规律,从实务案例中提炼经验,并融入自然科学的理念思维与分析方法,力求提升大数据时代电子政务云安全审计理论研究的科学性与纵深性。

参考文献:

[1]姜茸,张秋瑾,李彤,等. 电子政务云安全风险分析[J]. 现代情报,2014(12):12-16.

[2]刘国城. 基于过程的电子政务云安全审计模式研究[J]. 新疆大学学报:哲学·人文社会科学版,2016(1):28-35.

[3]胡俊,张熠,黄传河. 基于云平台的政务信息系统的访问控制设计[J]. 华中科技大学学报:自然科学版,2013(1):147-151.

[4]池亚平,王艳,王慧丽,等. 基于等级的电子政务云跨域访问控制技术[J]. 计算机应用,2016(2):402-407.

[5]黄瑞锋. 基于云计算政务网络安全集中管理[J]. 云南大学学报:自然科学版,2011(12):260-263.

[6]张会平,郭宁,杨国富,等. 基于社会-技术框架的"互联网+政务服务"网络安全机制研究[J]. 情报杂志,2017(12):16-21.

[7]刘彬芳,刘越男,钟端洋. 欧美电子政务云服务安全管理框架及其启示[J]. 现代情报,2018(10):32-37.

[8]李旖旎,陈文兵,胡世明,等. 日本云安全监管政策及其对我国的启示[J]. 情报杂志,2018(3):99-105.

[9]秦志光,王士雨,赵洋,等. 云存储服务的动态数据完整性审计方案[J]. 计算机研究与发展,2015(10):2192-2199.

[10]徐洋,朱丹,张焕国,等. 云环境下基于代数签名持有性审计的大数据安全存储方案[J]. 计算机科学,2016(10):172-176.

[11]邵必林,李肖俊,边根庆,等. 云存储数据完整性审计技术研究综述[J]. 信息网络安全,2019(6):28-36.

[12]赵春晔,涂山山,陈昊宇,等. 云安全审计中基于日志的用户行为分析[J]. 现代电子技术,2017(2):1-5.

[13]郭涛敏. 基于轻量化关联规则挖掘的安全日志审计技术研究[J]. 现代电子技术,2019(15):83-85.

[14]柳玉东,王绪安,涂广升,等. 全生命周期的云外包数据安全审计协议[J]. 计算机应用,2019(7):1954-1958.

[15]王文娟,杜学绘,王娜,等. 云计算安全审计技术研究综述[J]. 计算机科学,2017(7):16-20.

[16]Birnbaum Z,Liu B,Dolgikh A,et al. Cloud security auditing based on behavioral modeling[J]. International Journal of Business Process Integration & Management,2013,7(2):268-273.

[17]杨丽丽,王会金,刘国城. 管理控制视角下云审计平台的建设及运行研究[J]. 经济问题,2020(6):94-102.

[18]周福萍. 基于云平台的内部审计信息化流程设计[J]. 财会通讯,2018(13):111-115.

[19]王会金,刘国城. 大数据时代政务云安全风险估计及其审计运行研究[J]. 审计与经济研究,2018(5):1-11.

[20]徐薇. 中国政府审计制度理论框架的构建——基于国家治理视角[J]. 思想战线,2019(1):166-172.

[21]刘国城,王跃堂. 云电子商务的安全审计问题研究[J]. 兰州学刊,2017(5):173-186.

[22]黄瑛,石文昌. 云基础设施安全性研究综述[J]. 计算机科学,2011(7):24-30.

[责任编辑:刘　茜]

Security Audit Strategy of E-Government Cloud in Big Data Age

WANG Huijin[a], LIU Guocheng[b]

(a. Nanjing Audit University, b. School of Accounting, Nanjing Audit University, Nanjing 211815, China)

Abstract: E-government is an important foundation for realizing the national informatization strategy. In the era of big data, e-government cloud security is faced with severe challenges. Data leakage, account hijacking, system vulnerability and other factors hinder the development of government informatization. Error detection and correction are the basic responsibilities of auditing. As a means of supervision, cloud security auditing effectively caters to the security management and control requirements of e-government cloud. Faced with the complexity of cloud computing, how to establish a set of mature e-government cloud security audit strategy system has become a hot issue to be solved urgently. On the basis of theoretical review, this paper designs the framework of e-government cloud security audit, determines the audit mode and technology methods of e-government cloud security, analyzes the composition of e-government cloud security audit risk, explores the e-government cloud security audit mechanism based on the modules of infrastructure security, data information security, application service security, security organization management, and generates a feasible and scientific e-government cloud security audit system. The research conclusions of this paper provide theoretical support for the security management practice of e-government cloud in the era of big data from an audit perspective, and provide a practical reference for the construction of e-government cloud security audit strategy.

Key Words: big data; e-government; government cloud; cloud audit; cloud security; security audit; cloud application