政务大数据安全防护能力建设:基于技术和管理视角的探讨

孙轩，王焕骁

引用本文

孙轩，王焕骁. 政务大数据安全防护能力建设:基于技术和管理视角的探讨[J]. 计算机科学, 2022, 49(4): 67-73.

SUN Xuan, WANG Huan-xiao. Capability Building for Government Big Data Safety Protection:Discussions from Technologicaland Management Perspectives[J]. Computer Science, 2022, 49(4): 67-73.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.211000010

政务大数据安全防护能力建设:基于技术和管理视角的探讨

孙　轩[1,2,3]　王焕骁[1]
1 南开大学周恩来政府管理学院　天津 300350
2 南开大学计算社会科学实验室　天津 300350
3 南开大学数字城市治理实验室　天津 300350

摘　要　政务大数据是新时期数字政府建设的核心资产,对推动政府功能服务升级和经济、社会创新发展具有重要意义。但在复杂的网络流通环境下,为了保障政务大数据的合理、有序和可靠利用,其数据安全防护能力建设不容忽视。在技术层面,政务大数据安全防护涉及网络安全(Network Security)、平台安全(Platform Security)和应用安全(Application Security)等核心要素;在管理层面,政务大数据安全防护则需要重点关注人员素养(Personnel Quality)和制度质量(Institutional Quality)这两方面的内容。在理论探讨的基础上,给出了具体的技术和管理能力指标,并进一步对省级机关单位 *A* 的建设实践进行了分析。

关键词:政务大数据;数据安全防护;能力建设;技术应用;管理制度
中图法分类号　TP391

Capability Building for Government Big Data Safety Protection:Discussions from Technological and Management Perspectives

SUN Xuan[1,2,3] and WANG Huan-xiao[1]
1 Zhou Enlai School of Government,Nankai University,Tianjin 300350,China
2 Computational Social Science Laboratory,Nankai University,Tianjin 300350,China
3 Digital Urban Governance Laboratory,Nankai University,Tianjin 300350,China

Abstract　Government big data is the core asset for digital government construction in the new era,and it is of great significance to the upgrade of government functions and services and the development of economic and social innovation. However,in a complex network circulation environment,in order to ensure the rational,orderly,and reliable use of government big data,capability building for data security protection cannot be ignored. On the technical aspect,government big data security protection involves several core elements,including the network security,platform security,and application security,and on the management aspect,government big data security protection needs to be focused on personnel quality and institutional quality. On the basis of the oretical discussions,specific technical and management capability indicators are given,and the construction practice of provincial-level agency unit *A* is analyzed.

Keywords　Government big data,Data safety protection,Capability building,Technology application,Management system

1　引言

随着现代信息技术的发展,政府的功能、形态和运行方式正在发生着巨大变化。十八届三中全会首次提出“国家治理体系和治理能力现代化”的建设理念,而在十九大报告中,我党进一步明确指出“强化电子政务基础创新,支撑数字中国建设”的发展方向。在政府机构内部,依托云计算平台,通过各级政务数据中心建设,不同单位和部门得以有效整合与协同,实现了“一网统管”“一网通办”等一体化数字管理与服务;面向社会公众,政府部门则根据《促进大数据发展行动纲要》积极推动政务数据开放与共享,通过各种形式的互联网平台建设,助力社会多元共治与公共服务的改革、创新。

从业务处理、问题分析到应用服务,政务大数据是新时期数字政府建设的核心资产,其数据安全问题也日益成为影响我国经济、社会发展,甚至是国家安全的重要因素。在实际工作中,大数据需要持续流动和更新。只有通过数据的流通和使用,其功能价值才能被不断挖掘和实现[1]。然而,复杂的网络流通环境也使得政务大数据的完整性、保密性、可用性和可控性都面临严峻挑战。不仅数据泄露、越权访问、数据篡改、数据丢失、侵犯用户隐私等信息安全问题频发,而且其数据

到稿日期:2021-10-08　返修日期:2022-01-14
基金项目:天津市社会科学基金规划项目(TJGL19-005);中央高校基本科研业务费专项资金(63192205)
This work was supported by the General Program of Social Science of Tianjin(TJGL19-005) and Fundamental Research Funds for the Central Universities(63192205).
通信作者:孙轩(sunxuan@nankai.edu.cn)

安全防护的复杂性和难度也大大高于传统的信息安全管理过程。

长期以来，面对网络和信息安全问题，我们习惯于从技术层面寻求应对策略和解决方案，包括：加密存储与传输、访问验证与控制、系统漏洞扫描和网络攻击追溯等。通过各种技术手段和方法，努力将核心数据和敏感信息保留在一个可控的有限范围内。但是，随着数字化时代的来临，我们正面临一个全新的议题，即数据的内容开放与信息保护同等重要。此时，大数据安全防护不仅是一个技术问题，它更涉及管理层面的制度建设与行为约束。

2017 年，习近平总书记在参加中共中央政治局集体学习时曾指出："要切实保障国家数据安全，要加强关键信息基础设施安全保护，强化国家关键数据资源保护能力，增强数据安全预警和溯源能力"；2020 年 12 月，全国信息安全标准化技术委员会和工信部先后发布了《信息安全技术 政务信息共享数据安全技术要求》和《电信和互联网行业数据安全标准体系建设指南》；而 2021 年 6 月 10 日，第十三届全国人民代表大会常务委员会第二十九次会议审议通过了《中华人民共和国数据安全法》。为了保障政务大数据的合理、有序和可靠利用，相关法律、法规和管理制度得到不断完善。

从技术到管理，我国日益重视政务大数据的安全防护能力建设。但相比宏观层面的努力，在实际工作中，各级政府部门的理论认知和实践应用都还存在诸多不足：一方面，政务大数据安全防护的技术和管理能力提升缺少明确的指标参考；另一方面，政府机关单位的软、硬件环境改善缺乏有效的经验借鉴和案例指导。

2 相关理论研究

总体而言，大数据安全指大数据全生命周期的信息安全，即在数据采集、流动、存储、应用和销毁过程中，保证数据不被窃取、不被泄露，保持数据真实性及质量的能力和状态。全球最权威的 IT 研究与顾问咨询公司 Gartner 曾指出：大数据和云存储环境正在改变数据的存储、访问和处理方式，未来 80%的大型组织将面临大数据的重大安全问题，信息安全管理则必须采用以数据为中心的全新方法[2]。

2.1 大数据安全技术

在技术层面，西方发达国家一直以来都十分重视对大数据安全的理论和实践研究。其中，考虑到大数据应用的生命周期特点，Mehmood 等将大数据安全防护过程划分为生成、存储和处理 3 个不同阶段，通过访问控制、数据伪造等手段防止数据的非授权采集和隐私泄露，采用数据加密和完整性验证方法保证大数据的存储安全，并凭借隐私保护数据发布和隐私保护数据挖掘来实现大数据的处理安全[3]。为了保障网络环境下的数据安全，Cardenas 等采用对抗式机器学习以及稳健统计等方式来减轻恶意插入数据的不良影响[4]；Erdmann则认为在数据处理时应当通过聚合算法将典型数据转换为非典型数据，以降低用户被识别出来的风险[5]。

相比国外，国内在大数据安全技术领域的研究起步较晚，无论是从研究规模还是层次上，都与西方发达国家有一定差距。但随着相关产业和应用的快速发展，大数据安全防护问题也开始得到技术领域越来越多的关注。Wang等认为目前的安全防护技术难以满足大数据时代的信息安全需求，在对现有技术进行系统化梳理的基础上，指出了大数据安全技术进一步发展的突破口[6]；Chen 等从大数据生命周期安全和大数据平台安全两个角度分析了目前大数据发展面临的安全问题，并提出大数据安全在标准缺口、关键技术难点和大数据安全分析 3 个方面的现实问题[7]；Wei 等从数据加密角度，对大数据的密码使用、完整性校验、访问控制、密文数据去重与可信删除、密文搜索等内容进行了深度分析[8]；而 Tian 等则致力于可信固态硬盘（Trusted SSD）的设计、开发，尝试在硬件层面保障大数据的存储安全[9]。

2.2 大数据安全管理

自 1999 年开始，由于金融、电信等行业的信息安全问题频发，仅依靠当时的信息安全产品和技术手段已无法有效应对可能出现的各种风险，进而提出了"三分技术，七分管理"的口号，旨在通过对管理手段的强化，来解决越来越多的信息安全问题。此后，众多专家、学者一致同意并倡导在使用技术的同时重视信息的安全管理。以世界信息安全标准 ISO27001[10] 为例，其全部 14 个控制区域中，只有 3 个区域是纯粹的技术要求，其他 11 个区域都需要采取信息安全管理手段来实现。

而在大数据安全管理方面，美国学者 Tankard 认为集中存储、管理的大数据不应仅仅围绕数据应用建立安全防护体系，其管理工作需要更多地关注数据本身的特征[11]。此后，Kshetri 通过分析、调研，将隐私、安全和收益等目标要素与数据的收集、存储、共享和可访问性问题联系起来，明确指出大数据的存储和管理风险会随着数据体量大小、多样性和复杂度的提升而有所增加[12]。

近年来，从大数据的实际应用发展状况出发，我国相关领域的学者针对大数据安全管理问题开展了一系列研究探索。其中，大数据安全管理的政策法规是研究的重点内容之一，例如：Feng 等从大数据的隐私保护、信任和访问控制等多个不同角度出发，指出只有将技术手段与相关政策法规结合，才能更好地解决大数据安全保护问题[13]；Tian 认为大数据涉及公共利益，需要通过立法手段来防范安全漏洞[14]；Han 则认为数据安全立法应兼顾安全和自由，实现多元共治是其最终目标[15]。此外，也有大量研究针对大数据安全防护的工作要点进行讨论，例如：Hu 等在分析、整理多个行业大数据安全管理需求的基础上，指出大数据安全问题涉及移动数据安全、易攻击目标、用户隐私保护、数据安全存储、数据安全进化和信任安全等多个维度，且针对不同问题需要采取不同的安全保障策略[16]；Huang 等认为，降低或回避大数据的信息安全风险需要从组织所处的内、外部环境出发，在基础设施、数据分析、数据管理、技术漏洞以及数据自身可信度、现有法律法规、行业内自律性、个人隐私意识、黑客攻击 9 个层面采取应对策略[17]。与此同时，也有研究从国家甚至全球治理的角度出发，对大数据的安全防护工作进行宏观探讨：Xu 在分析大数据积累所产生的世界性影响的基础上，指出在大数据时代中国所面临的安全管理能力、存储及处理能力、应用能力以及人才培养能力等多方面的挑战，并提出了相应的对策和建议[18]；Liu 等则认为传统的安全防护手段已经难以满足大数据

安全管理的现实需求，国家应该进一步完善相关安全标准、法律法规和监管体系[19]。

2.3　政务大数据安全

与传统的信息安全相比，大数据安全更加注重数据应用的安全性，即：在不暴露用户敏感信息的前提下，对数据价值进行充分挖掘和有效利用。特别是对于政务大数据而言，其公共属性决定了数据的安全防护工作需要在信息共享与隐私保护之间寻求一个最佳平衡点，既确保个人、企业隐私和政府秘密不被泄露，又能通过数据的开发、开放促进社会经济发展。

正如 Meng 等所述，如果仅仅为了保护隐私就将所有的数据加以隐藏，那么数据的价值根本无从体现[20]。在数字时代，政务大数据不仅是政府部门提升管理决策质量、优化公共服务供给的重要依据，也是政府、企业、民众多主体互动、协作的基础[21]。针对数据开放与数据安全间的平衡关系，Zhang 等认为个人隐私保护与政府数据利用之间相互制衡、彼此促进，在对中美两国政策法规进行对比、分析的基础上，提出了具体的应用发展建议[22]；Cai 等则从多个方面分析了美国政府数据开放的政策、法规和机构设置，为我国政务数据开放和安全防护提供了重要启示[23]。

而在应用平台建设方面，Yu 认为我国政府的数据管理部门应加强大数据安全意识的培养，强化自主研发和部门间合作，构建政务大数据资源开放平台，并通过政务大数据管理促进国家治理的现代化发展[24]。Du 通过对美、英、澳政府数据开放平台的隐私政策进行梳理和分析，建立了较为系统的评价指标体系，并在此基础上对我国政务数据开放平台的隐私保护现状进行评价，认为其数据安全防护能力整体较差，用户隐私面临严峻挑战[25]。

3　技术视角下的政务大数据安全防护

政务大数据的安全防护离不开技术层面的能力建设。由于政府部门间的大数据应用通常基于云计算平台，采用分布式存储、管理方式，且涉及多用户间的共用、共享和功能交互，因此其安全防护技术包含网络通讯、加密传输、身份验证、智能合约等多方面的内容。虽然保障大数据安全的技术手段多样，但现有的法律、法规和技术标准为政务大数据安全防护搭建了总体框架，明确了其基本工作思路和要求。

3.1　现有法律、法规及技术标准

目前，我国涉及网络信息安全的法律法规主要包括《中华人民共和国网络安全法》（以下简称《网络安全法》）、《网络安全等级保护条例》《中华人民共和国计算机信息系统安全保护条例》《中华人民共和国计算机信息网络国际联网管理暂行规定》《计算机信息网络国际联网安全保护管理办法》和《互联网信息服务管理办法》。其中，《网络安全法》是我国为网络空间管辖颁布的第一部法律。该法律虽然以“网络安全”命名，但数据安全是其重要组成部分。该法律不仅强调“关键信息基础设施”的保护工作，也明确提出了采取“数据分类、重要数据备份和加密等措施”来维护网络数据完整性、保密性和可用性的相关技术要求[26]。

与此同时，由公安部牵头组织印发的《信息安全等级保护管理办法》，特别是 2019 年出台的“等保 2.0”相关国家标准[27]，更将信息安全防护技术要求细分为具体的应用类别。在大数据安全防护方面，其根据应用场景的不同给出相对应的系统概念和模型，并明确了可供参考的安全控制措施。目前，“等保 2.0”中针对大数据的测评指标是政府部门大数据安全自查时应当遵循的最新标准。

在技术要求分类上，“等保 2.0”采用的是传统的自底向上的标准体系，涉及物理环境、通信网络和计算环境 3 个层面。在具体要求方面，安全物理环境仅要求机房位于中国境内；安全通信网络提出了对大数据平台承载应用及流量分离的要求；安全计算环境则提出了大量针对大数据平台以及数据处理流程中的详细技术要求，具体包含身份鉴别、资源存储管理、工具组件管理、数据访问控制、数据全生命周期管理、数据应用审计等技术要求。

3.2　政务大数据安全防护技术要点

政府机关单位的网络和应用系统由行业主管部门和地方网信办指导建设，一般都符合“等保 2.0”的物理环境要求。因此，政务大数据安全防护的技术要点主要集中于通信网络和计算环境方面。其相关内容涉及网络安全技术、平台安全技术和应用安全技术等。

政务大数据的网络安全技术既包含以防火墙和入侵检测为代表的传统信息安全技术，又包括近年来逐渐兴起和推广的网络安全态势感知[28]、APT（Advanced Persistent Threat）攻击防护[29]和网络回溯分析[30]等现代网络安全防护技术。从纯粹的软件功能实现到软、硬件一体化应用，这些技术手段正在被越来越多地固化为特定的网络安全产品，而相应设备的综合防护与日志分析能力则成为网络安全技术关注的焦点。

政务大数据的平台安全技术致力于解决分布式、多用户平台所带来的各种潜在的数据安全问题，以确保不同功能服务在动态、随机、复杂和开放环境下的有效性[31]。其中，用户资源的高效、安全共享以及个性化、多层次安全防护体系的构建是平台安全的核心内容。为了实现该目标，相关系统需要基于虚拟化层次结构对底层故障进行有效屏蔽[32]，基于用户间的信任关系对网络数据流进行逻辑划分与隔离[33]，并通过自动化程序对平台资源进行可靠管控[34]。

政务大数据的应用安全技术强调数据应用框架的整体可靠性。面对网络计算过程中错综复杂的功能操作，它通过对数据管理系统的漏洞和缺陷进行修复、完善，使得恶意访问和非法信息获取的难度大大增加，进而提高应用抵御外部攻击和信息泄露的能力。为了保证相应安全防护功能的实现，其需要解决的技术问题包括数据组件的身份认证、数据访问的边界保护、数据内容的协调管理和数据操作的动态审计等[7]。

3.3　政务大数据安全防护技术指标

根据相关技术要点，政务大数据安全防护能力在宏观层面包含网络安全、平台安全和应用安全 3 个核心要素；而在微观层面，各核心要素背后又分别涉及多项具体的能力指标内容（见表 1）。

（1）网络设备防护（Network Equipment Protection）指标

关注于设备的功能完备性，主要考查设备运转是否正常、是否定期维护巡检、是否能够维持特征库的最新版本，以及其配置是否符合国家法律、法规的相关要求。

(2)网络日志分析(Network Logfile Analysis)指标关注于设备的日志存储与分析能力，主要考查设备安全防护日志的保存时长，以及能否在日志分析的基础上对可能存在的各种安全威胁进行有效防御。

(3)平台故障屏蔽(Platform Fault Shielding)指标关注于系统的底层稳健性，主要考查相关云计算平台的虚拟化功能和故障时期的资源调配能力，以及是否拥有足够资源以满足数据容灾和虚拟机漂移等技术应用需要。

(4)平台流量划分(Platform Dataflow Division)指标关注于系统的安全域分割与隔离能力，主要考查 SDN(Software Defined Network)网络技术的使用情况，以及不同实现方式下数据流分离技术的实际应用水平。

(5)平台资源管控(Platform Resource Management)指标关注于系统的资源监测与调控能力，主要考查平台是否具备实时运行状态的监测页面和接口，是否支持计算和存储资源的灵活调整和管控，以及相关技术的应用情况。

(6)应用身份鉴别(Application Identity Authentication)指标关注于功能服务的接入可靠性，主要考查大数据应用的身份标识和验证能力，以及能否对多用户、多终端环境下的数据采集、导入和导出等应用操作进行自适应配置。

(7)应用访问控制(Application Access Control)指标关注于功能服务的访问授权能力，主要考查大数据应用是否具备相应的数据安全标记功能，以及基于安全标记的细粒度访问控制与多角色应用协调的技术水平。

(8)应用数据管理(Application Data Management)指标关注于功能服务的数据协同能力，主要考查大数据应用针对不同类别、不同级别数据的差异化管理功能，以及为满足多用户数据使用所采取的各种安全保障手段。

(9)应用操作审计(Application Operation Audit)指标关注于功能服务的操作追溯能力，主要考查大数据应用对数据采集、处理、分析和挖掘等过程的跟踪记录情况，以及相关操作数据的收集汇总和集中审计功能。

表 1 政务大数据安全防护技术能力建设指标

Table 1 Government big data security protection technical capacity building indicators

	Core Elements	Capability Indicators
Government Big Data Security Protection Technical Capacity	Network Security	Network Equipment Protection
		Network Logfile Analysis
		Platform Fault Shielding
	Platform Security	Platform Dataflow Division
		Platform Resource Management
		Application Identity Authentication
	Application Security	Application Access Control
		Application Data Management
		Application Operation Audit

4 管理视角下的政务大数据安全防护

管理对于政务大数据的安全防护至关重要。然而，区别于技术层面的设备、平台和功能服务升级，在管理层面，政务大数据安全防护能力建设的核心是人员和体制，包括人员的安全意识和安全能力培养、数据应用与管理的相关规章制度建设等。而国内外的先进案例为政务大数据安全防护能力建设提供了宝贵经验。

4.1 国内外政务数据安全管理体系

美国是世界上最早发展电子政务应用的国家，其业务体系相对成熟和完善。近年来，在大力推动政务数据开放、共享的同时，政府也高度重视网络数据的安全防护问题。一方面，美国政府注重对普通人员和专业技术人员的数据安全意识培养，通过多种渠道宣传普及相关知识，构建了一整套网络安全标准、知识体系和资质认定方法；另一方面，美国政府认识到信息安全情报共享在应对网络安全威胁工作中的重要作用，建立了从联邦政府至各地方、涵盖多个行业的网络安全信息共享组织机构；与此同时，白宫和国土安全部都从自身角度提出了相应的网络安全风险应对策略，将国家保护和计划局升级为网络安全和基础设施安全局，并在局内成立国家风险管理中心，通过政府部门与私营机构的信息共享和协调运作来应对关键基础设施可能遇到的各种安全威胁。

英国也是较早开展电子政务建设工作的国家之一。为了保障网络数据安全，其政府部门出台了一系列规划法案和标准。一方面，由英国标准协会编写的 BS7799 标准为各种机构进行信息安全管理提供了一个完整的体系框架，并被国际标准化组织采纳，成为 ISO17799 国际标准；另一方面，英国通过立法和机构设置的方式进行信息安全管理权责划分，不仅授权警察、国家安全等执法机构在必要时对数据信息进行合法监控，而且成立了网络安全办公室、网络安全行动中心和网络安全应急指挥中心；另外，2016 年 6 月由英国下议院文化、媒体和体育委员会发布的《网络安全：个人在线数据保护》报告还对个人数据保护涉及的政府部门、企业、服务商和用户的具体工作提出了明确的指导意见。

与西方发达国家相比，我国的电子政务应用虽然起步较晚，但政务大数据安全防护管理工作发展迅速。在情报共享方面，我国已经建立了以国家网络与信息安全信息通报中心为核心的网络信息安全检测、通报、预警和处理全流程工作机制；在安全意识方面，各级政府部门也逐渐从“以系统为核心”的传统信息安全保障理念转向“以数据为核心”的信息安全防护理念。目前，我国正在努力构建政务大数据的开放、共享平台，相关数据资源包括国家统计数据(data. stats. gov. cn)、中国政府数据(www. gov. cn/shuju/)，以及源自各省、直辖市、自治区的开放数据内容。但面对数据开放带来的一系列信息安全问题，现有的数据管理体系面临极大挑战。首先，网络安全信息共享的组织协调机构成立不久，缺乏有效的政企信息共享与协作激励机制；其次，不完善的网络信息安全管理制度增加了政府部门对自身数据的安全防护难度，数据被泄露、盗取、篡改的风险依然存在；再次，网络信息安全事务的责任划分还不明确，各部门的监管职权配置极易出现交叉和重叠。

4.2 政务大数据安全防护管理要点

由国外经验和国内情况分析可知，人员的安全防护意识

和防护能力提升是应对大数据安全威胁的关键，可靠的安全防护制度则是各组织机构信息安全防护体系构建的基础。

人员方面，政务大数据安全防护需要人们在头脑中建立起基本的信息安全意识，即对数据安全问题和数据存储、传播介质的损坏保持应有的警觉。与此同时，参照信息安全保护相关的测评内容，不仅要求设备供应商具有一定的安全建设资质和运维服务能力，而且单位内部管理人员也要主动提升其自身的信息系统安全操作、检查与循环整改能力[35]。在有限的技术条件下，相关人员的信息安全知识、能力素养在很大程度上决定了政府机构的数据安全防护水平。

制度方面，政务大数据安全防护是一个系统工程，各项网络保护和数据管理工作的开展都需要相应的体制、机制约束。网络安全情报共享机制的建立有助于提升政府部门对新型黑客攻击和木马病毒的防护能力[36]；数据操作规范、管理流程和保护方案的制定使得不同类别、不同等级数据的采集、存储、处理、应用、流动、销毁等全生命周期行为过程得以有序推进[37]；而各相关主体责任与义务的明确划分对数据安全防护措施的有效施行也至关重要[38]。在特定体系框架下，只有依法、依规地对数据资源进行管理，才能确保政务大数据的存储和应用安全。

4.3　政务大数据安全防护管理指标

根据相关管理要点，政务大数据安全防护能力在宏观层面包含人员素养（Personnel Quality）和制度体系（Institutional Quality）2 个核心要素，而在微观层面，其各核心要素背后又分别涉及多项具体的能力指标内容（如表 2 所列）。

（1）用户安全意识（Enduser Safety Awareness）指标关注于政务大数据安全防护的主观认知水平，主要考查数据管理者和使用者对数据安全法律、法规和本单位安全管理规章制度的了解程度及主动执行情况。

（2）管理人员能力（Data Manager Capabilities）指标关注于政务大数据安全防护的技术运用水平，主要考查数据管理者对数据安全防护相关理论知识、技术手段和软、硬件使用方法的掌握程度及实际应用情况。

（3）服务厂商能力（Service Vendor Capabilities）指标关注于政务大数据安全防护的第三方支持力度，主要考查系统网络安全服务商、网络设备维保商、云计算平台维保商和大数据平台供应商的资质水平和技术服务情况。

（4）情报共享机制（Information Sharing Mechanism）指标关注于政务大数据安全防护的协同工作方式，主要考查数据管理单位与政府网信办和上级部门间的安防信息共享、交换关系以及相关操作流程的可靠性与有效性。

（5）数据管理策略（Data Management Strategy）指标关注于政务大数据安全防护的基本工作内容，主要考查政府数字资产安全管理方案以及数据采集、存储、流通和应用等全生命周期操作规范和保护措施的完备性。

（6）职责分工体系（Responsibility Division System）指标关注于政务大数据安全防护的具体工作安排，主要考查各级管理单位和相关服务厂商在数据访问控制、编辑审查、隐私保护等方面权责划分和规定的明确性与合理性。

表 2　政务大数据安全防护管理能力建设指标

Table 2　Government big data security protection management capacity building indicators

	Core Elements	Capability Indicators
Government Big Data Security Protection Management Capacity	Personnel Quality	Enduser Safety Awareness
		Data Manager Capabilities
		Service Vendor Capabilities
	Institutional Quality	Information Sharing Mechanism
		Data Management Strategy
		Responsibility Division System

5　省级机关单位 *A* 的案例分析

在国务院所属部委及其直属机构的指导下，省级政府部门实际承担了地区政务系统建设、日常运行维护、安全保障和数据管理的大部分工作，在大数据应用、管理过程中扮演着重要角色。而为了满足日益丰富的数字化应用需要，各部门运维的系统数量逐年增多，所管理的数据规模也越来越大，涉及经济、文化、教育、医疗等诸多领域。大数据安全防护形势日益严峻。

作为省级政府部门的典型代表，机关单位 *A* 使用自建的云计算平台进行数据管理和应用，并在数据安全防护能力建设方面做出了大量努力。经过多年发展，不仅其技术运行环境不断升级，而且相关管理制度也得到进一步完善。

面向网络安全，机关单位 *A* 于 2012 年之前即完成了网络防火墙和病毒防护网关建设。多年来设备运转正常，按月巡检并进行特征库更新，符合等级保护三级要求。自 2017 年《网络安全法》实施以来，该单位进一步对安全防护设备日志和服务器日志进行分析。相关日志内容均留存 6 个月以上，并由设备维保商负责分析、研判和技术升级。

面向平台安全，机关单位 *A* 一直采用较为成熟的 VMWARE 技术框架对云计算平台进行虚拟化管理。虽然未使用 SDN 网络技术，但该单位通过服务器管理和交换机接口区分也实现了业务流量与管理流量的有效分离。在功能上，基于 VMWARE 的技术框架，机关单位 *A* 可以实现计算和存储资源的集中监测和管控，却无法实现完全的底层故障屏蔽。

面向应用安全，机关单位 *A* 过去仅依靠数据库系统自带的用户认证功能进行应用安全控制和管理。2018 年，在大数据应用平台建成后，其前台访问开始由业务系统鉴别，后台访问由堡垒机鉴别，满足双因素身份认证要求。然而，到目前为止，该系统还不具有基于安全标记的细粒度授权和访问控制功能，且未对应用进行操作审计和分析。

针对人员素养，机关单位 *A* 自 2013 年起就制定了一系列网络安全和数据管理规定，并根据技术发展趋势每年对内部用户开展信息安全意识培训。其所使用的软、硬件系统均通过政府采购招标流程购置，服务厂商具备相应的技术安全资质。而该单位的数据管理员和部门领导都对网络安全环境、信息安全管理制度非常熟悉，且于 2015 年获得 CISP（Certified Information Security Professional）专业证书。

针对制度框架，机关单位 *A* 仅于 2017 年单独购置了互联网信息安全情报服务，目前尚未建立起稳定的情报共享

机制。虽然出台了《A 机关数据应用管理规定》《A 机关数据备份流程》和《A 机关数据恢复流程》等一系列规章制度，但数据的全生命周期行为还没有得到有效规范。单位内部根据其《A 机关信息安全组织机构管理规范》对不同部门的工作进行划分，而机关单位 A 与其他服务提供商之间则通过合同与保密协议的方式明确其各自的权责范围。

基于多维度指标内容，对机关单位 A 近 6 年的大数据安全防护能力建设情况进行综合评价和分析(见表 3)，可知：其在技术和管理方面虽然还存在着一些缺陷，但多年来整体发展较好。一方面，该单位的技术防护能力提升显著，特别是 2018 年以后，随着大数据管理平台的开发，其在应用安全防护方面有了较大突破；另一方面，该单位在管理层面的能力建设还十分有限，除了人员素养提升，一直以来在制度框架方面缺乏足够重视。

表 3 机关单位 A 的大数据安全防护能力建设情况

Table 3 Construction of big data security protection capacity of agency unit A

Core Elements	Capability Indicator	2015	2016	2017	2018	2019	2020
Network Security	Network Equipment Protection	√	√	√	√	√	√
	Network Logfile Analysis	—	—	√	√	√	√
Platform Security	Platform Fault Shielding	—	—	—	—	—	—
	Platform Dataflow Division	√	√	√	√	√	√
	Platform Resource Management	√	√	√	√	√	√
Application Security	Application Identity Authentication	—	—	—	√	√	√
	Application Access Control	—	—	—	—	—	—
	Application Data Management	—	—	—	√	√	√
	Application Operation Audit	—	—	—	—	—	—
Personnel Quality	Enduser Safety Awareness	√	√	√	√	√	√
	Data Manager Capabilities	√	√	√	√	√	√
	Service Vendor Capabilities	√	√	√	√	√	√
Institutional Quality	Information Sharing Mechanism	—	—	√	—	—	—
	Data Management Strategy	—	—	—	—	—	—
	Responsibility Division System	√	√	√	√	√	√

结束语 随着地方政务数据开放、共享和大数据应用的发展，政府机关单位的数据安全问题日益突出。在此背景下，大数据安全防护已成为保障我国数字政府建设成效的重要内容。它不仅涉及技术层面的设备、平台和系统建设，更包含管理层面的人员和制度建设。

特别是省级政府部门，其政务大数据安全防护能力的高低在很大程度上影响着地方政府数字化改革的成败。然而，受传统认知框架的影响，我们在实践过程中往往过度追求技术层面的提升和改进，而忽略了政府部门在管理制度上的改革与创新。相比昂贵的技术产品，可靠、高效的管理机制、策略和体系对于提升大数据安全防护能力同样重要。

参 考 文 献

[1] SUN X, SUN T. Dynamic Urban Governance in a Big Data Computing Environment: Conceptual Connotation and Application Framework[J]. E-government, 2020(1): 20-28.

[2] MARRISON C. Gartner warns of big data security problems [J]. Network Security, 2014(6): 1-20.

[3] MEHMOOD A, NATGUNANATHAN I, XIANG Y, et al. Protection of big data privacy[J]. IEEE Access, 2016, 4: 1821-1834.

[4] CARDENAS A, MANADHATA P, RAJAN S. Big Data Analytics for Security[J]. IEEE Security & Privacy, 2013, 11(6): 74-76.

[5] ERDMANN J. As Personal Genomes Join Big Data Will Privacy and Access Shrink? [J]. Chemistry & Biology, 2013, 20(1): 1-2.

[6] WANG D, ZHAO W B, DING Z M. An Overview of Key Technology Analysis of Big Data Security Assurance[J]. Journal of Beijing University of Technology, 2017, 43(3): 335-349, 322.

[7] CHEN X S, YANG L, LUO Y G. Big data security protection technology[J]. Advanced Engineering Sciences, 2017, 49(5): 1-12.

[8] WEI K M, WENG J, REN K. Big data security protection technology[J]. Chinese Journal of Network and Information Security, 2016, 2(4): 1-11.

[9] TIAN H L, ZHANG Y, XU X H, et al. Trusted solid state-drive: a new foundation for big data security[J]. Chinese Journal of Computers, 2016, 39(1): 154-168.

[10] Information technology—Security techniques—Information security management systems—Requirements: ISO/IEC 27001: 2013 [S]. Switzerland: Schweizerische Normen-Vereinigung (SNV), 2013.

[11] TANKARD C. Big data security [J]. Network Security, 2012 (7): 5-8.

[12] KSHETRI N. Big data's impact on privacy, security and consumer welfare[J]. Telecommunications Policy, 2014, 38(11): 1134-1145.

[13] FENG D G, ZHANG M, LI H. Big data security and privacy protection[J]. Chinese Journal of Computers, 2014, 37(1): 246-258.

[14] TIAN W. The Connotation, Current Situation and Basis of Public Big Data Information Security Legislation[J]. Henan Social Sciences, 2018, 26(7): 86-91.

[15] HAN W. The balance of security and freedom-analysis of the purpose of data security legislation[J]. Science Technology and Law, 2019(6): 41-48, 67.

[16] HU K, LIU D, LIU M H. Research on the Security Understanding and Countermeasures of Big Data[J]. Telecommunication Science, 2014, 30(2): 112-117, 122.

[17] HUANG G B, ZHENG L. Research on Big Data Information Se-

curity Risk Framework and Countermeasures[J]. Researches in Library Science，2015(13)：24-29.

[18] XU Y. Challenges and countermeasures facing China in the era of big data[J]. Forum on Science and Technology in China，2015(3)：24-29.

[19] LIU Y，DENG Q，PENG Y S. Security Challenges Facing Data Sovereignty and Privacy Protection in the Big Data Era[J]. Modernization of Management，2019，39(1)：104-107.

[20] MENG X F，CHI X. Big data management：concepts，technologies and challenges[J]. Journal of Computer Research and Development，2013，50(1)：146-169.

[21] CHEN H，WANG X X，DUAN Y Q. Analysis and Research on the Value Orientation of Chinese Government's Big Data Policy [J]. Library and Information Service，2020，64(11)：19-27.

[22] ZHANG X J，WANG W Q，TANG C L. Research on the Policies and Regulations of China-US Government Data Opening and Personal Privacy Protection[J]. Information Studies：Theory & Application，2016，39(1)：38-43.

[23] CAI Q X，HUANG R H. Policy and Regulation Guarantee of U. S. Government Data Opening and Its Enlightenment to my country[J]. Library and Information，2017(1)：10-17.

[24] YU H. Opportunities，Challenges and Countermeasures of Government Data Management in the Big Data Era[J]. Chinese Public Administration，2015(3)：127-130.

[25] DU H H. Research on the Construction of Evaluation System for Privacy Protection of my country's Government Data Open Platform[J]. Journal of Information，2020(3)：172-179.

[26] WANG C H. Analysis of the Six Legal Systems of "Network Security Law"[J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science)，2017，37(1)：1-13.

[27] The network security grade protection system 2. 0 standard is officially released [EB/OL]. (2019-05-16) [2021-09-13]. http：//it. people. com. cn/n1/2019/0516/c1009-31087714. html.

[28] KOU G，WANG S，Tang G. Research on Key Technologies of Network Security Situational Awareness for Attack Tracking Prediction[J]. Chinese Journal of Electronics，2019，28(1)：166-175.

[29] SINGH S，SHARMA P K，MOON S Y，et al. A comprehensive study on APT attacks and countermeasures for future networks and communications：challenges and solutions[J]. Journal of Supercomputing，2016，75：4543-4574.

[30] BREAUX T，BAUMER D. Legally "reasonable" security requirements：A 10-year FTC retrospective-Science Direct[J]. Computers & Security，2011，30(4)：178-193.

[31] LIN C，SU W B，MENG K，et al. Cloud computing security：architecture，mechanism and model evaluation[J]. Chinese Journal of Computers，2013，36(9)：1765-1784.

[32] JAIN R，PAUL S. Network virtualization and software defined networking for cloud computing：a survey. [J]. IEEE Communications Magazine，2013，51(11)：24-31.

[33] FAWCETT L，SCOTT-HAYWARD S，BROADBENT M，et al. Tennison：A Distributed SDN Framework for Scalable Network Security[J]. IEEE Journal on Selected Areas in Communications，2018，36(12)：2805-2818.

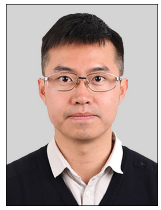
[34] LI B H，LI B，REN W，et al. Research on Resource Security Management Mechanism Oriented to Trusted Cloud Computing [J]. Journal of Cyber Security，2018，3(2)：76-86.

[35] ZHANG K，MA L，XU Y F. Research on Security Assurance System of Complex Information System[J]. Chinese Journal of Management Science，2000(S1)：336-346.

[36] LI J H. Overview of Threat Intelligence Awareness，Sharing and Analysis Technology in Cyberspace[J]. Chinese Journal of Network and Information Security，2016，2(2)：16-29.

[37] DING H F，MENG Q Q，WANG X，et al. Analysis of data security and privacy protection countermeasures of government data opening oriented to data life cycle[J]. Journal of Information，2019，38(7)：151-159.

[38] CHEN C B，CHENG S. Regulatory Responsibility in Government Data Opening：Practical Dilemma and Optimal Path[J]. Journal of Information，2019，38(10)：188-194.



SUN Xuan，born in 1985，Ph.D，associate professor，is a member of China Computer Federation. His main research interests include digital governance，urban computing and smart city.

（责任编辑：柯颖）