科学数据共享的安全管理问题研究

李善青 郑彦宁 邢晓昭 支凤稳
（中国科学技术信息研究所，北京 100038）

摘要：数据安全是科学数据共享的重要前提之一，其高价值性和集中存放的特点使科学数据容易成为被攻击和破坏的目标。大数据技术的发展将会深刻影响科学数据的安全管理方式，带来一系列新的要求和挑战。文章在梳理科学数据安全相关定义的基础上，从机密性、完整性和可用性3个层面分析了科学数据共享过程中的安全需求，讨论了用于保护科学数据安全的关键技术及发展趋势。最后提出了大数据背景下加强科学数据共享安全管理的建议。

关键词：科学数据；大数据；数据共享；安全管理；关键安全技术
中图分类号：G311 **文献标识码：**A **DOI：**10.3772/j.issn.1674-1544.2019.03.002

Study on Security Managements of Scientific Data Sharing

LI Shanqing, ZHENG Yanning, XING Xiaozhao, ZHI Fengwen
(Institute of Scientific and Technical Information of China, Beijing 100038)

Abstract: Data security is one of the important promises for scientific data sharing, its high scientific value and centralized storage characteristics make scientific data an easy target of attack and destruction. The development of big data will bring new requirements and challenges which would significantly affect the security managements of scientific data. This paper firstly gives the definition of scientific data security and analyzes new security requirements of confidentiality, integrity and availability. And then, some key security techniques are investigated and their development trends are also analyzed. Finally, we draw useful conclusions and give suggestions of enhancing security managements of scientific data sharing in big data era.

Keywords: scientific data, big data, data sharing, security management, key security techniques

0 引言

国务院于 2018 年 3 月发布的《科学数据管理办法》明确指出，由政府预算资金资助形成的科学数据应当按照“开放为常态、不开放为例外”的原则，面向社会和相关部门开放共享。科学数据的开放共享，一方面将极大地推动科学技术的快速发展，提升科技竞争力；另一方面也会带来一系列的数据安全问题，而且面临极其复杂和严峻的形势。科学数据作为一种基础性、战略性的科技资源，具有极其重要的科学价值。数据一旦被窃取或破坏，造成的危害和损失是不可估量的。另外，国家依托科学数据中心实现科学数据的开放共享，具有集中存放、统一共享的特

作者简介：李善青（1981—），男，中国科学技术信息研究所副研究员，研究方向：科技资源管理和数据挖掘（通讯作者）；**郑彦宁**（1965—），男，中国科学技术信息研究所研究馆员，研究方向：竞争情报理论和方法；**邢晓昭**（1988—），女，中国科学技术信息研究所助理研究员，研究方向：科技成果成熟度评价；**支凤稳**（1987—），女，中国科学技术信息研究所副教授，研究方向：情报学。

基金资助：国家科技基础条件平台专项课题“大数据背景下加强科学数据管理和共享服务的关键问题研究”（2017DDJ1ZZ13）；中国博士后科学基金面上资助项目“科学数据共享模式及驱动机制研究”（2018M641446）。
收稿时间：2018 年 8 月 20 日。

点。该特点进一步加剧了科学数据安全的严峻性，因为平台一旦遭受入侵，危及的可能是整个学科领域的全部数据。因此，科学数据共享的安全管理是一个不容忽视的关键问题，必须给予足够的重视。

目前，专门针对科学数据安全管理的研究还很不成熟，发表的论文数量有限。随着大数据技术的发展和普及，大数据的安全与隐私保护已逐渐成为新的研究热点。这些研究工作对大数据背景下加强科学数据的安全管理具有重要的参考意义。在标准制定方面，国际标准化组织正在开展《信息技术大数据参考架构》的编制，美国国家标准与技术研究院于2015年9月发布了《NIST大数据互操作性框架》（NIST SP 1500系列标准）。这些标准中都有专门的章节对大数据的安全和隐私保护进行阐述和规定。我国信息安全标准化技术委员会在2016年4月成立了大数据安全标准特别工作组，主要负责制定和完善中国大数据安全领域标准体系，包括《信息安全技术个人信息安全规范》《信息安全技术大数据安全管理指南》等国家标准。在大数据安全和隐私保护的研究方面，形成了一系列的综述性的研究成果[1-9]。这些文献分析了大数据背景下数据安全和隐私保护的特点及面临的挑战，对相关技术的发展现状进行了综述，但其研究角度不尽相同。如曹珍富等[2]侧重于数据加密的角度；陈兴蜀等[5]对法律法规、标准、数据生命周期和大数据平台等进行了全面的综述；吕欣等[6]建立了大数据安全和隐私保护技术体系的参考模型，从数据层、应用层、接口层以及系统层等维度进行分析和综述。

在上述大数据安全和隐私保护的研究工作的基础上，本文将结合科学数据共享的特点，对大数据背景下科学数据安全的定义、数据共享的安全需求和相关技术现状进行梳理和讨论，为相关研究和政策制定提供有益参考。

1　定义与流程

目前已有的研究工作尚未对科学数据的安全进行明确的定义和描述。本文在借鉴数据安全[10]、信息安全[11]和网络安全[12]等相关定义的基础上，结合科学数据本身的特点，对科学数据安全进行如下定义：通过必要的技术和管理措施，保护科学数据在其全生命周期中免受破坏性外力和非授权操作的侵害，保持科学数据的机密性、完整性和可用性。科学数据的生命周期大致可以划分为以下几个阶段：采集生产、汇交整合、加工整理、共享使用、长期保存和退出销毁等。本文将重点研究科学数据在共享使用过程中的安全问题。

科学数据共享使用的过程如图1所示。科学数据在进入共享服务平台之前需要进行涉密审查，对于涉及保密的数据不纳入共享服务的范围，对于非涉密数据则根据相关政策和服务要求将其转化为不同权限的可共享数据。有些科学数据本身不属于保密数据，但通过与其他数据进行关联分析和挖掘可能得出涉密的信息，这类问题是涉密审查需要解决的难点问题。存储管理是科学数据共享的基础，需采用科学、规范的措施对科学数据进行存储和管理，以保证数据的完整性和可用性。当用户发出使用数据的请求后，平台的访问控制模块会首先验证用户的身份，然后判断用户的请求是否在授权范围内。如果通过认证，则调用相应的服务将数据提供给用户，否则拒绝用户的请求。数据传输可以根据数据的权限和安全需求选择直接传输、加密传输和离线传输等。在大数据时代，科学数据共享面临复杂和严峻的安全形势，需应对不断出现的新的安全威胁，因此科学数据的所有操作历史和用户的所有访问记录对数据共享服务平台的安全分析至关重要，需要进行完整的记录和保存，以便进行后续的安全审计和行为预测等。

2　数据共享的安全需求

2.1　机密性的需求

科学数据的机密性保护是指只有授权用户才能获取和使用数据，非授权用户则无法获取数据。机密性保护是科学数据开放共享的重要前提

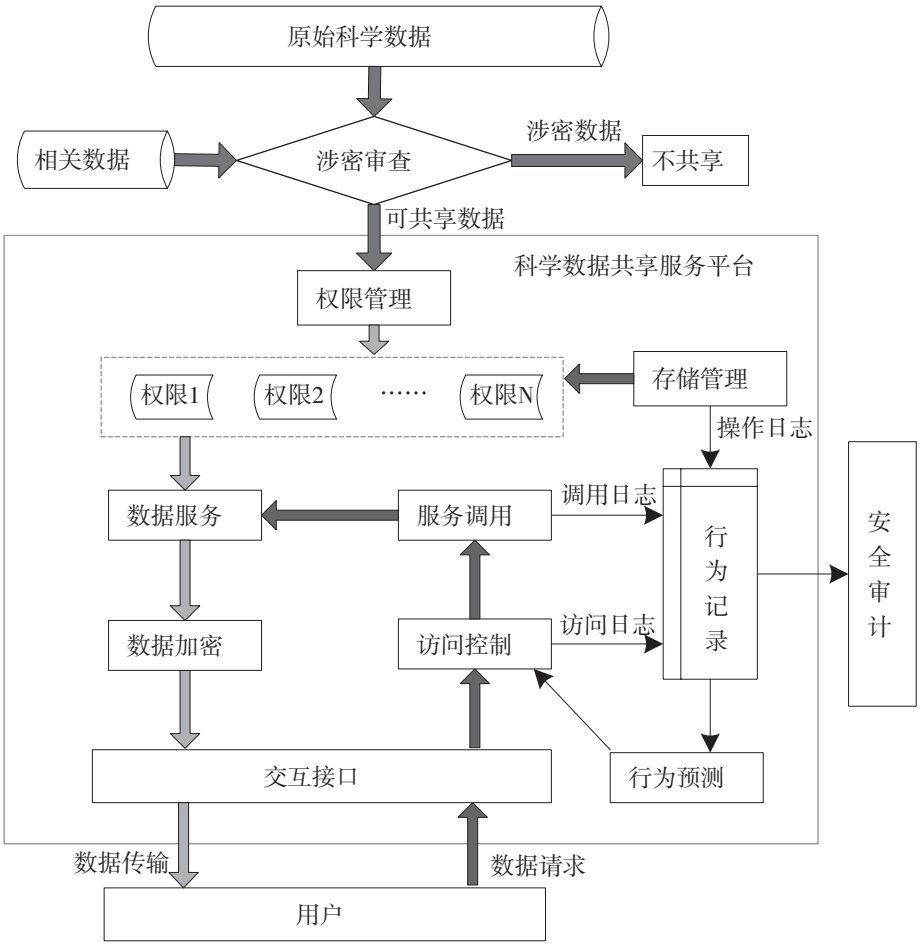

图 1　科学数据共享使用过程的框图

之一。在科学数据共享过程中，涉及机密性的环节包括涉密审查、访问控制和数据传输等。涉密审查的目的在于提前发现涉及公共安全或个人隐私的科学数据，防止这些涉密数据进入数据共享服务平台。大数据挖掘技术的发展对涉密审查提出了更高的要求，因为某些不涉密的科学数据在与其他数据进行整合和关联分析后，也可能从中挖掘出隐藏的有价值的情报。访问控制的本质在于准确匹配用户的权限和数据的权限，使得授权的用户可以访问恰当的数据。基于角色的方法较好地解决了静态环境下小型系统的访问控制问题。大数据时代的来临产生了新的问题：（1）用户角色和数据种类的数量都在不断地快速增长；（2）角色的权限和数据的权限均处于动态变化的过程中。因此，需要一种灵活的、支持细粒度的访问控制技术，能够满足动态、实时控制数据的安全访问。另外一种思路是，通过研发一种新的加密共享技术，既能满足科学数据在不同用户之间协同计算的要求，又能有效保护数据内容的私密性。数据在传输过程中容易被拦截和窃取而导致数据泄漏，通常采用加密的方法予以保护。大体量的科学数据进行加密和解密需要消耗大量的时间和计算资源，还涉及密钥的管理，因此需要一种简单、高效的加密技术以满足大数据加密的要求。

2.2　完整性的需求

科学数据的完整性是指数据在存储和共享的过程中，不被非法授权修改和破坏，保证数据的一致性。完整性是实现科学数据价值的重要保证。在科学数据共享过程中，涉及完整性的环节包括存储管理和数据传输等。如何保证科学数据的完整性是科学数据存储管理需要解

决的重要问题之一。科学数据通常采用数字化的格式存储，其存储介质比较脆弱，可能因断电等因素遭受损坏。科学数据本身具有易被改变且改变后不易察觉的特点，硬件故障、人为的误操作、程序缺陷、病毒或黑客攻击等事件都可能造成数据的损坏或丢失，从而损害数据的完整性。此外，信息技术的快速发展使数据的软硬件载体和技术框架等都处于快速的动态变化之中，因此技术的更新换代可能造成旧技术的淘汰，导致数据的无法使用。体量巨大和种类繁多的科学数据极大地加剧了完整性保护的复杂度，不仅需要额外的大量的存储空间和计算资源，而且需要一套完善的完整性验证机制。显然，对所有的科学数据都进行完整性校验是不切实际的，需要根据数据的重要程度采取不同的方法。数据传输的过程也存在被篡改和破坏的风险，需要在接收数据后对其完整性进行校验，同样也存在上述的问题和要求。

2.3　可用性的需求

科学数据的可用性是保证授权用户对科学数据的访问和使用，不因偶然或人为因素而影响数据的使用。科学数据在共享过程中面临外界不可抗力和人为恶意破坏的威胁，其可用性体现在系统和数据遭到破坏后持续提供数据服务的能力，是影响数据共享服务效能的重要因素。大数据时代对系统的持续服务能力和数据的快速恢复能力提出了更高的要求。系统平台所提供服务的数量和类型都很多，在遭到攻击和破坏时，需要保持当前未完成的会话状态，自动切换到备份系统继续提供服务。数据备份是保证数据可用性的重要方法之一，当原始数据被破坏后，可利用备份对原始数据进行恢复，提升科学数据的可用性。大体量的科学数据进行备份对原本就不富余的存储空间提出了很大的挑战。考虑到不同类型的科学数据对安全性的要求是不同的，可以据此制定灵活的数据备份策略，如重要性较低的数据可采用本地备份，重要性较高的可采用异地备份，最重要的数据需要在上述备份的基础上增加物理备份等。

3　相关技术及趋势

3.1　完整性校验技术

数据的完整性校验技术可以大致划分为两类：数据持有性证明机制（PDP）和数据可恢复性证明机制（POR）。前者的计算代价小，只能用于验证数据的完整性；后者在验证数据完整性的基础上可以恢复被破坏的数据，需要处理校验信息，计算代价很大，不适应于大体量的科学数据，本文对此不进行深入的探讨。数据持有性证明机制常用的验证信息包括MAC认证码、RSA签名、BLS签名等。基于MAC认证码的方法采用的是对称加密体系，而基于数字签名的方法通常采用非对称加密体系。上述完整性校验技术只适应于静态的数据环境，而当数据发生变化时，会导致其他数据块的索引会发生变化，原先生成的校验证据信息就会失效。为适应数据的动态更新，支持动态操作的PDP机制逐渐受到关注和发展，其中常用的是基于跳表的PDP机制[13]和基于MerkleTree的PDP机制[14]。这些方法虽然在一定程度上解决了动态环境下的数据完整性校验问题，但需要较复杂的控制机制和算法，具有较高的计算复杂度。大数据时代，一方面数据的体量非常大，另一方面数据的更新频率不断升高，因此能够适应未来需求的完整性校验技术需要兼顾以上两个新的要求，在支持数据动态变化环境的基础上降低验证算法的计算复杂度，这也将是未来发展的趋势。

3.2　访问控制技术

传统的访问控制技术，如自主访问控制和基于角色的访问控制等，是从系统的角度保护资源的安全，访问权限的控制是静态的，主体获得访问权限后可以长期访问数据资源，主要适应于静态环境下小体量的数据系统。为解决访问权限的动态管理问题，基于任务的访问控制技术从任务管理的角度建立控制策略，主体只有在执行任务的过程中才能获得所需的权限，任务终止后将失去相应的权限。该方法的不足是通用性较差，无法将好的控制策略或规则进行继承和复用。基于

对象的访问控制技术通过构建受控对象描述主体和客体之间的访问权限关联，支持复用、继承和派生等操作。该方法能实现较为复杂的控制逻辑，而且具有较好的灵活性。高级持续性威胁是一种基于系统漏洞的新型的网络攻击技术，具有潜伏周期长和高度的隐蔽性等特点，很难被传统的访问控制技术发现和拦截。基于行为模型的威胁发现技术通过对正常的访问行为进行学习和建模，借助异常行为的挖掘和比对方法发现潜在的威胁。该方法在前期需要大量的标注样本用于训练行为模型。在大数据背景下，系统的访问控制一方面需要一种支持细粒度的可动态管理权限的访问控制技术；另一方面也需要具备一定的学习能力，从海量的系统日志数据中挖掘和学习相关知识用于提升访问控制的安全性。

3.3 数据加密技术

传统的数据加密技术主要有两种：对称加密和非对称加密。对称加密采用相同的密钥进行加密和解密，具有计算量小和加密效率高的特点，但密钥管理复杂度较高，共享前需要进行密钥同步；非对称加密采用不同的密钥进行加密和解密，具有安全性高和密钥管理简单的特点，但其也有计算量大和加密效率低的缺点，只适合对少量数据进行加密。在科学数据共享时，数据发送方需要根据不同的接收方进行密钥和密文的单独管理，造成了大量时间和精力的消耗。代理重加密技术[15]是一种密文之间的密钥转换机制，允许第三方（代理）将使用发送方公钥加密的密文转换为使用接收方公钥加密的密文。该方法在保证不泄漏数据给第三方的同时，不仅提高了数据共享的灵活性，而且减轻了数据发送方密钥管理的负担。上述的方法都是解决端到端的数据加密共享问题，无法适应一对多的加密共享情况。基于属性的加密方法通过对用户私钥设置属性集（或访问结构），为数据密文设置访问结构（或属性集），由属性集和访问结构之间的匹配关系确定其解密能力。常用的两种方法为基于密钥策略的属性加密[16]和基于密文策略的属性加密[17]。前者的数据密文依赖于用户的属性集，适应于静态数据的访问控制。后者的数据密文依赖于访问结构，可灵活控制授权用户的范围。这些加密算法的时间复杂度较高，只有后续对加密算法进行改进和优化以大幅降低其时间复杂度，才能适应大数据时代的要求。

3.4 隐私保护技术

隐私内容的发现和预警技术是隐私保护的前提，是一种主动的保护数据私密性的机制，能提前发现隐私泄露的风险并防患于未然。同时它也是一项复杂的技术，需要整合很多方面的知识，如法律政策、数据挖掘技术等，可目前相关的研究工作还非常少，未来需要加强在该领域的政策引导和研发投入。数据匿名化技术是通过对数据中涉及隐私的属性值进行匿名化处理，从而达到保护隐私的目的。Dwork等[18]提出了一种差分隐私保护技术，通过向查询结果或者分析结果中添加适当的噪声数据来达到隐私保护的目的。该方法需要解决的关键问题是设计恰当的算法保证引入的噪声既能保护数据的隐私，又不影响数据的可用性。另外一种解决思路是通过数据加密的方法，它采用特定的算法对数据进行加密，使加密前后的数据对指定的运算具有结果一致性。近年来，同态加密技术[19]和安全多方计算技术[20]引起了较多的关注，这些方法兼顾了数据的保密性和可用性，但需要进行大量复杂的指数运算，计算效率不高。在大数据背景下，整合多来源数据的关联分析技术是隐私保护面临的重大挑战。可行的应对策略是一方面要发展隐私内容的发现和预警技术，做好前端的隐私保护；另一方面对重点保护的数据可采用加密的方法，在数据的共享和使用过程中保护数据的隐私。

3.5 安全审计技术

安全审计技术的重要作用体现在两个方面，一是用于提前发现系统存在的安全风险，及时采取相应的防护措施，避免安全事故的发生；二是在安全事故发生后，对事故的全过程进行回溯分析，发现导致事故的原因，并对相关责任方进行追责。传统的面向中小系统的安全审计技术取得了一定的进展。但是大数据背景下，大型数据

管理系统的业务逻辑更加复杂，系统操作和用户访问量呈指数增长趋势，而且网络攻击更具隐蔽性，如高级持续性威胁程序可对目标进行长期性和有计划性的攻击等。为应对这些新变化，需要一种细粒度的安全审计技术。一方面要对所有的系统操作和用户访问进行记录和保存；另一方面要从海量、琐细的系统日志里筛选出与安全相关的线索，分析和发现系统存在的安全问题。这既需要借助大数据强大的分析挖掘能力，也需要专业审计人员的综合判断能力。此外，系统需要具备学习的能力，及时将安全审计获取的结果等知识等转化为规则或者模型，从而能够更好地适应快速变化的大数据环境。

4　结论和建议

本文在梳理科学数据安全定义的基础上，分析了在保障科学数据的机密性、完整性和可用性等方面所面临的新挑战和新要求，探讨了相关的安全关键技术的发展现状和未来趋势，包括完整性校验、访问控制、数据加密、隐私保护和安全审计等。这些技术在大数据时代到来之前就已经存在，并在保护科学数据安全方面取得了较好的效果。但是，面对大数据所带来的新的安全要求，这些技术还存在一定的局限性，只有对其进行扩展或者发展新的技术才能适应新的安全形势。科学数据共享的安全不仅是一个技术问题，更是一个管理的问题。我国已经发布了《科学数据管理办法》，它从全局的高度对科学数据的管理提出了总体要求，需要进一步完善与之配套的可落地执行的相关政策和标准。科学数据中心要制定严格的安全管理机制，通过严格的管理发挥安全保护技术的最大效能。

大数据技术的发展虽然给科学数据的安全带来新的挑战，但也为应对复杂的安全问题提供了新的思路和方法。建议未来可重点关注的研究方向包括：（1）研究基于大数据的涉密审查技术，能够敏锐的发现隐藏在海量数据中，借助关联分析与发掘可导致泄密的科学数据。（2）研发智能化的安全审计技术，通过对海量系统日志信息的分析和挖掘，在尽量减少人工干预的基础上能够提前、准确地发现系统存在的安全威胁。（3）大力发展机器学习技术，让计算机学习大量已有的知识和规则，可以完全或部分替代专家对安全事件进行智能化的判断和处理。

参考文献

[1] 冯登国, 张敏, 李昊. 大数据安全与隐私保护[J]. 计算机学报, 2014(1): 246−258.

[2] 曹珍富, 董晓蕾, 周俊, 等. 大数据安全与隐私保护研究进展[J]. 计算机研究与发展, 2016(10): 2137−2151.

[3] MATTURDI Bardi, ZHOU Xianwei, LI Shuai, et al.Big data security and privacy: Areview[J].China Communications, 2014(14): 135−145.

[4] FANG Wei, WEN Xuezhi, ZHENG Yu, et al. A survey of big data security and privacy preserving[J]. Iete Technical Review, 2016, 34(5): 1−17.

[5] 陈兴蜀, 杨露, 罗永刚. 大数据安全保护技术[J]. 工程科学与技术, 2017(5): 1−12.

[6] 吕欣, 韩晓露. 大数据安全和隐私保护技术架构研究[J]. 信息安全研究, 2016(3): 244−250.

[7] 王丹, 赵文兵, 丁治明. 大数据安全保障关键技术分析综述[J]. 北京工业大学学报, 2017(3): 335−349.

[8] 马立川, 裴庆祺, 冷昊, 等. 大数据安全研究概述[J]. 无线电通信技术, 2015(1): 1−7.

[9] 魏凯敏, 翁健, 任奎. 大数据安全保护技术综述[J]. 网络与信息安全学报, 2016(4): 1−11.

[10] Wikipedia.Data security [EB/OL].[2018−08−18] https://en.wikipedia.org/wiki/Data_security.

[11] ISO/IEC 27000: 2018(E).Information technology−security techniques−information security management systems−overview and vocabulary [S].Switzerland, 2018.

[12] 全国人民代表大会常务委员会.《中华人民共和国网络安全法》[EB/OL].[2018−08−18] http: //www.gov.cn/xinwen/2016−11/07/content_5129723.htm.

[13] ERWAY Chris, KÜPÇÜ Alptekin, PAPAMANTHOU Charalampos, et al. Dynamic provable data possession[J]. ACMTransactions on Information & System Security, 2015, 17(4): 1−29.

[14] ATENIESE Giuseppe, BURNS Randal, CURTMOLA Reza. Provable data possession at untrusted stores[C]. The 14th ACM Conference on Computer and Communications Security, Alexandria, USA, 2007: 598−609.

[15] LIANG Kaitai, LIU Joseph, WONG Duncan, et al. An efficient cloud−based revocable identity−based proxy re−encryption scheme for public clouds data sharing[C]. European Symposium on Research in Computer Security. Springer, 2014: 257−272.

[16] GOYAL Vipul, PANDEY Omkant, SAHAI Amit, et a1. Attribute−based encryption for fine−grained access control of encrypted data[C].The l3thACM Conference on Computer and Communications Security. Alexandria, ACM, 2006: 89−98.

[17] CHEN Yanli, SONG Lingling, YANG Geng. Attribute−based access control for multi−authority systems with constant size ciphertext in cloud computing[J]. China Communications, 2016, 13(2): 146−162.

[18] DWORK Cynthia. Differential privacy: A survey of results[C]. International Conference on Theory and Applications of Models of Computation. Springer−Verlag, 2008: 1−19.

[19] LI Shundong, DOU Jiawei, WANG Daoshun. Survey on homomorphic encryption and its applications to cloud security[J]. Journal of Computer Research & Development, 2015, 52: 1378−1388.

[20] MALIN Bradley, AIROLDI Edoardo, EDOHO−EKET Samuel, et al. Configurable security protocols for multi−party data analysis with malicious participants[C]. The 21stInternational Conference on Data Engineering. IEEE Computer Society, 2005: 533−544.

（上接第10页）

[23] 甘肃省人民政府办公厅.甘肃省人民政府办公厅关于印发《甘肃省科学数据管理实施细则》的通知[EB/OL].[2019−03−12]. http: //www.gansu.gov.cn/art/2018/9/3/art_4827_390343.html.

[24] 云南省人民政府办公厅. 云南省人民政府办公厅关于印发云南省科学数据管理实施细则的通知[EB/OL].[2019−03−15]. http: //www.yn.gov.cn/yn_zwlanmu/qy/wj/yzbf/201810/t20181008_34145.html.

[25] 湖北省政府办公厅.省人民政府办公厅关于印发湖北省科学数据管理实施细则的通知[EB/OL].[2019−03−21]. http: //www.hubei.gov.cn/govfile/ezbf/201811/t20181121_1371232.shtml.

[26] 安徽省人民政府办公厅关于印发《安徽省科学数据管理实施办法》的通知[EB/OL].[2019−03−20]. http: //www.ahedu.gov.cn/163/view/23617.shtml.

[27] 内蒙古自治区人民政府办公厅. 内蒙古自治区人民政府办公厅关于印发自治区科学数据管理办法的通知[EB/OL].[2019−03−20]. http: //www.nmg.gov.cn/art/2018/11/30/art_1686_241858.html?from=timeline&isappinstalled=0.

[28] 广西科技厅基础研究处.广西科学数据管理实施办法[EB/OL].[2019−03−21]. http: //www.gxst.gov.cn/gxkjt/xxgk/20190131/002004001_5a75ef7e−c703−4149−821c−ec2fe0e11e83.htm.

[29] 昆明市人民政府办公厅.昆明市人民政府办公厅关于印发昆明市科学数据管理实施办法的通知[EB/OL].[2019−03−21]. http: //www.km.gov.cn/c/2019−03−14/2943668.shtml.

[30] 中国科学院办公厅.《中国科学院科学数据管理与开放共享办法》[EB/OL].[2019−03−21]. http: //m.cas.cn/tzgg1/201902/t20190220_4679797.html.

[31] 江苏省政府办公厅.省政府办公厅关于印发江苏省科学数据管理实施细则的通知[EB/OL].[2019−03−20]. http: //www.jiangsu.gov.cn/art/2019/2/26/art_64797_8239962.html.

[32] 人民日报. 科学数据, 如何科学管理[EB/OL].[2019−03−20] http: //paper.people.com.cn/rmrb/html/2018−04/08/nw.D110000renmrb_20180408_1−02.htm.

[33] Freedom of Information Amendment (Reform) Act2010[EB/OL].[2019−03−20].https: //www.legislation.gov.au/Details/C2012C00866.

[34] Privacy Amendment (Enhancing Privacy Protection) Act 2012[EB/OL].[2019−03−20].https: //www.legislation.gov.au/Details/C2015C00053.

[35] Personal Data Protection Act 2012 [EB/OL].[2019−03−20]. https: //sso.agc.gov.sg/Act/PDPA2012.