科学数据中心资源和用户访问控制体系

曹乔卓然[1]，陈祖刚[2]，李国庆[2]，李静[2]
1. 郑州大学地球科学与技术学院，河南 郑州 450052；
2. 中国科学院空天信息创新研究院，北京 100094

摘要
大数据时代，各个国家及政府普遍重视科学数据开放并积极推动数据共享，广泛开放共享的数据对全过程数据安全保障提出了新的挑战。在借鉴国际科学数据共享最新政策与分析我国实际状况的基础上，提出了科学数据中心资源和用户访问控制体系。通过在开放系统平台中应用数据分级、用户分类以及系统访问权限控制策略，解决了数据中心资源安全共享缺乏系统性方案的问题。研究成果已被应用于国家对地观测科学数据中心的实际业务工作中，取得了良好的效果。

关键词
大数据平台；资源共享；用户分类；资源分级；授权访问控制

中图分类号：P209 文献标志码：A doi: 10.11959/j.issn.2096-0271.2022009

Resource and user access control system of scientific data center

CAO Qiaozhuoran[1], CHEN Zugang[2], LI Guoqing[2], LI Jing[2]
1. School of Geo-Science & Technology, Zhengzhou University, Zhengzhou 450052, China
2. Aerospace Information Research Institute, Chinese Academy of Sciences, Beijing 100094, China

Abstract
In the era of big data, all countries and governments generally attach importance to the opening of scientific data and actively promote data sharing. The wide opening and sharing of data poses new challenges to the whole process of data security. Based on the latest policies of international scientific data sharing and the actual situation in China, the resource and user access control system of scientific data center was put forward. Through the application of data classification, user classification and system access control strategy on the open system platform, the problem of lack of systematic scheme for resource security sharing in the data center was solved. The research results have been applied to the practical work of the National Earth Observation Scientific Data Center and achieved good results.

Key words
big data platform, resource sharing, user classification, resource classification, authorization access control

0 引言

近年来，随着科学研究进入数据驱动的第四范式，科学数据资源成为国家重要的战略性支撑资源。为了促进科学数据资源共享，提高科学研究的支持保障水平，国内外越来越重视科学数据的管理，兴建了一大批科学数据中心。例如美国国家空间科学数据中心（National Space Science Data Center，NSSDC）、英国数字保存中心（Digital Curation Centre，DCC）、英国数据档案（UK Data Archive）中心以及澳大利亚国家数据服务（Australian National Data Service，ANDS）中心等[1]。2019年，我国科学技术部和财政部发文，成立了国家高能物理科学数据中心、国家基因组科学数据中心、国家天文科学数据中心等20个国家级科学数据中心，我国海量科学数据管理与共享工作也进入了新的发展阶段。

科学数据中心的兴起带来的不仅仅是各学科新的发展机遇，往往也伴随着大量科学数据资源的开放共享中较大的安全风险问题。例如，网络病毒和黑客肆意侵犯用户隐私，数据资源易泄露、丢失，数据安全管理机制不完善，访问权限管理不严密等[2-3]。因而，各国政府普遍非常重视科学数据安全工作，并相继开展相关法律法规的制定工作。2016年，欧盟通过了《通用数据保护条例》，讨论了数据使用者、数据管理者及数据本体间的关系，提出要对敏感数据进行分类[4]。2018年，我国国务院办公厅印发《科学数据管理办法》，着重强调了要保障科学数据安全，要求科学数据必须分级分类管理，从而更好地支撑国家科技创新、经济社会发展和国家安全。

保障科学数据安全共享需要构建包括系统层面、数据层面和服务层面的科学数据安全框架[5]。对数据、用户进行分类分级、建立系统访问权限控制体系是搭建科学数据安全框架的重要内容，也是实现科学数据有序管理与共享的一个可行的方法。

分类分级是实现数据安全的基石，是科学数据中心有序管理各项资源的基础，分类分级管理极大程度地平衡了数据安全与数据开放之间的关系[6]。分类分级是将数据资源划分为学科范畴明确、访问等级清晰的数据产品，并把使用数据的用户依据自身的特征划分为数据需求清晰一致的群体，进而实现不同分类分级的数据和用户之间的关联匹配，确保合适的数据资源被合适的用户获取和使用。系统访问权限控制是数据信息安全防范和保护的核心策略之一，有效保证了系统资源不被非法使用[7]。系统访问授权控制机制授予合法用户访问特定资源的权限，并拒绝非权限用户访问。系统访问权限控制体系的建立降低了系统维护成本，保障了系统运行安全。明确而完整的服务访问授权体系对于提高数据中心的服务质量和优化用户的使用体验具有重要作用。

当前，我国各个科学数据中心缺乏明确而完善的数据和用户分类分级体系以及面向数据管理和共享服务系统的访问权限控制策略来保障科学数据中心安全、高效地开展科学数据共享工作。本文借鉴国际科学数据共享最新政策，并与我国实际状况相结合，提出了一套完善的面向科学数据中心的数据、用户分类分级体系和业务系统访问权限控制策略，并以国家对地观测科学数据中心（National Earth Observation Data Center，NODA）为例，应用本文提出的分类分级体系与业务系统的访问权限控制策略，最终形成一个科学数据业务有序管理与安全共享服务平台。

1 数据共享安全控制方法研究进展

在数据密集型研究范式背景下，国内外科学数据中心十分重视海量数据开放共享过程中面临的安全问题，展开了相关研究，提出了一系列保障科学数据安全共享的方法和政策，并进行了实践。

美国国家海洋与大气管理局（National Oceanic and Atmospheric Administration，NOAA）鼓励以进一步分析或重用的形式提供数据。例如，数据必须以机器可读的格式编码，最好使用现有的开放格式标准；必须充分记录数据，最好使用开放元数据标准；根据NOAA信息质量指南，应进行数据质量控制，并在元数据中引用质量控制过程和结果的描述。世界数据系统（World Data System，WDS）通过在工作流中使用持久标识符实现准确的数据访问与引用，从而完成对平台数据的保护与控制。国际地球观测组织（Group on Earth Observations，GEO）提出了地球观测数据的免费且不限制重复使用、不超过复制和分发成本的情况下提供、最短时间提供3项共享原则，该原则已经被国际社会和各国政府广泛接受。中国国家海洋科学数据中心（National Marine Data Center，NMDC）将用户划分为普通用户、个人认证用户和单位认证用户3种类型，并规定了各类别用户可浏览、检索和收藏下载指定海洋数据和产品的范围以及单日数据订单下载规模。中国国家微生物科学数据中心（National Microbiology Data Center，NMDC）制定了数据库访问协议，将数据访问权限分为完全公开和协议公开两种类型，并规定了不同类型用户对数据访问与使用的许可条件。国家基础学科公共科学数据中心面向科学数据资源的组织管理与资源发现，发展了基于元数据的数据检索、基于语义网的查询、关联扩展以及基于用户行为分析的相关度修正4项新增的科学数据资源建设与服务规范。

当下，国际通用的数据授权许可协议是知识共享协议（creative commons license，又称CC协议）。它是一种创作授权方式，允许作者选择不同的授权条款和参考不同国家著作权法制定相应的版权协议。该协议的适用范围非常广泛，兼容性较强，适用于多种形式的数据资料，是开放数据应用非常理想的许可协议。截至2016年，全球已有50多个国家基于CC协议发布了基于各国国情的不同版本，应用CC国际通用版本许可协议的国家包括美国、英国、澳大利亚、加拿大等国家[8]。

由此可见，国内外的科学数据中心仅仅对科学数据安全共享框架中的数据分类分级、访问权限控制、数据政策制定的某一方面或者某一个具体的技术点进行了研究，其保障数据安全的策略和技术都是独立的，缺少将三者统一为一个整体的系统性解决方案。科学数据共享是一个涉及数据生产、传输、存储、管理、共享和应用的全生命周期流程，单方面或者单个技术点的数据安全保障措施难以实现科学数据的安全开放共享。因而，各个科学数据中心迫切需要科学数据安全共享的系统性操作方案，并将其实际应用到日常工作中。

2 科学数据资源分级体系

资源分级是采用明确的、规范的方法，区分资源的敏感性和重要程度差异，从而确定资源的级别[9]。合理的资源分级能够保证在符合法律法规和监管要求的前

提下，对最关键和最有价值的资源采取最高级别的防护，同时减少不必要的投入[10]。数据的分级规则是客观并可以被校验的，即通过数据自身的属性和分级规则就可以判定其等级，已经分级的数据也是可以复核和检查的。

科学数据资源是科学数据共享服务系统的内容和结果。我国科学数据共享需要考量的因素有：数据资源的知识产权、数据资源的分发、数据资源的演绎、数据资源的溯源、数据资源可否开放共享给国外用户等。

数据资源的知识产权主要是指数据资源的作者对知识产权的申明和要求情况，即数据资源是否可以共享、共享的人员范围、数据资源可否供商业使用、使用数据是否需要引用和申明作者的贡献等。数据资源的分发主要是指数据资源能否由数据所有者以外的人提供给其他人，以及数据资源可否再分发等。数据资源的演绎主要是指是否允许用户对数据资源进行更改，以及更改以后的再发布权限要求等。数据资源的溯源主要指是否需要记录数据资源被谁在何种目的下使用等。数据资源可否开放共享给国外用户主要体现科学数据中心的国际化应用水平。

综合考虑这几个方面，同时尽量与国际通用的CC协议相对应，本文将科学数据资源划分为6个级别，即无限制访问、无差别访问、公益性访问、商业性访问、受邀访问、业主访问。不同级别的资源建立了相应的等级描述标识，并用不同的分级代码表示。**表1**展示了资源的具体分级情况和资源分级代码，并列出了各级资源所对应CC协议中的资源级别。

（1）无限制访问（R0）

无限制访问资源是完全开放、无任何访问权限限制的资源，对应于CC协议中的CC-BY-SA类型资源。此资源安全防护等级最低，任何用户（甚至无须注册）都可以查询、使用、下载和传播该资源，并可用于商业目的。用户还可以对该级别资源进行二次修改，修改后的资源需要以相同的授权方式予以共享，共享时需要注明数据的所有者。

表1 本文提出的科学数据资源分级体系

资源分级	分级代码	对应CC协议分级
无限制访问	R0	CC-BY-SA
无差别访问	R1	CC-BY-NC-SA
公益性访问	R2	CC-BY-NC-SA
商业性访问	R3	CC-BY-SA
受邀访问	R4	CC-BY-NC-ND
业主访问	R5	/

（2）无差别访问（R1）

无差别访问资源是对外开放性比较强的资源，对应于CC协议中标注为CC-BY-NC-SA的授权许可的资源。国外注册用户具有访问此级别资源的权限，可以查询、使用、下载或传播该资源。此资源不可用于商业目的，但可以进行二次修改，修改后的资源需要以相同的授权方式予以共享，共享时需要注明数据所有者。

（3）公益性访问（R2）

公益性访问资源对应于CC协议中标注为CC-BY-NC-SA的授权许可的资源。该资源主要供国内实名制注册用户使用，用户可以查询、使用、下载或传播该资源，不可用于商业目的，但可以进行修改。修改后的资源需要以相同的授权方式予以共享，共享时需要注明数据所有者。

（4）商业性访问（R3）

商业性访问资源是具有商业性质的资源类别，对应于CC协议中标注为CC-BY-SA的授权许可的资源。该资源主要面向国内注册用户开放共享，用户可以查询、使用、下载或传播该资源，并用于商业目的。用户可以对该资源进行修改，修改后的资源需要以相同的授权级别予以共享，共享

时需要注明数据所有者。

(5)受邀访问(R4)

此类资源对应于CC协议中标注为CC-BY-NC-ND的授权许可。原则上仅限受邀请和授权的用户查询、使用、下载或传播该资源，不可将其用于商业目的，不可对其进行修改。国内注册用户如需要获取该级别资源，必须提出附加授权申请，审核通过后方可访问。

(6)业主访问(R5)

此类资源是本分级体系中受限最多的资源。一般情况下，仅限资源的所有人或授权管理人查询、使用、下载或传播该资源。该资源可用于商业目的，也可以修改，共享时需要注明数据所有者。国内注册用户如需要获取此类资源，必须提出附加授权申请，审核通过后方可访问。

3 用户分类体系

作为数据中心的业务开展主体和服务受众，用户在科学数据生命周期各个阶段中起着重要作用。然而，面对庞大的国内外用户群体，若数据中心对用户缺少有效而统一的分类和控制，对用户访问权限不加限制，势必影响用户数据使用体验和数据安全。根据不同的用户属性或特征对用户进行分类，可以解决此类问题。用户的多维细分可以更好地管理用户，实现有效的用户行为控制、合理的服务资源配置和数据安全策略的成功实施[11]。对此，本文建立了一种适应我国科学数据中心特色的用户分类体系，并成功应用于科学数据中心的实际运行与服务过程中。

3.1 用户分类

对用户分类前，首先应当建立分类准则[12]。科学数据中心用户的分类就是按照一定的标准与原则，将用户归划为不同的几类角色，从而赋予各类角色不同的访问权限[13]。所谓角色，就是用户在系统内可执行的操作集合，用户通过角色间接地访问平台资源[14]。用户角色与访问权限相关联，不同的访问权限本质是不同类别的用户具备访问和操作平台中不同等级授权的数据资源与服务的能力[15]。

数据中心的用户可分为内部管理人员和外部使用者。内部管理人员的主要职责是对各种与数据相关的业务进行管理与操作。外部使用者是访问数据中心的数据共享服务系统、获取系统数据资源的人员。因而，可将数据中心中的各种用户分为管理员用户与前台用户两大类。**表2**展示了本文提出的用户分类情况和用户角色与其分类代码的对应关系。

3.2 管理员用户(UA)

在科学数据中心系统中，管理员用户是具备科学数据中心管理权限的后台用户，其大类编码为UA。根据管理权限的优先级别和职责范围，又可进一步划分为5个小类的后台管理员用户角色。

- 顶级管理员(UA1)：是整个科学数据中心系统中权限最高的用户角色类别，可对所有的业务环节进行全面管理。顶级管理员负责后台管理系统的整体构建，可对其他后台用户进行授权和管理；拥有分配其他种类用户的权限，并负责审核用户身份和处理低权限用户的访问升级请求。
- 栏目管理员(UA2)：科学数据中心日常业务是分块运行的，栏目管理员负责数据中心各栏目的后台管理工作，可对栏目操作员用户进行授权，执行流程审核和统计等操作。

● 栏目操作员(UA3):是维护数据中心各栏目基本内容与功能的主要用户角色。根据栏目管理员提供的授权范围,对负责的栏目进行相关操作的执行。

● 团队管理员(UA4):是科学数据中心下属的分中心或者合作团队的管理员用户。职责是授权生成团队操作员用户,并且负责审核团队操作员提交的团队内部数据资源。

● 团队操作员(UA5):是为科学数据中心合作团队专门授权的用户角色,负责合作团队的数据上传与更新,以及处理前台用户提交的数据需求订单。

3.3 前台用户(UB)

前台用户是科学数据中心的实际使用者,享有系统提供的各项服务。前台用户的大类编码为UB,依据用户提供的身份标识信息,将前台用户分为3个小类的用户角色。这3类前台用户的区别主要体现在对不同等级的资源访问和操作能力的差异上。

● 公众用户(UB1):系统的“游客”用户,无须进行注册与身份验证,也无须进行实名制审核。这是前台用户中权限最低的角色,仅可访问标识为无级别访问限制的数据和服务等基础平台资源。出于对系统安全性的考量,该类用户不可使用数据中心的订单式服务、实名制服务和数据上传汇交服务等系统服务。

● 国际注册用户(UB2):是科学数据中心的国外用户,主要目的是满足数据资源的国际化共享需求。按照我国对地观测数据共享政策要求,此类用户仅能访问无差别和无限制访问级别授权的数据和服务等资源。在数据上传和汇交方面,为了明确上传数据资源的来源,国际注册用户必须实名上传信息和数据。

表 2 本文提出的用户分类体系

用户大类	用户小类代码	用户角色说明
管理员用户(UA)	UA1	顶级管理员
	UA2	栏目管理员
	UA3	栏目操作员
	UA4	团队管理员
	UA5	团队操作员
前台用户(UB)	UB1	公众用户(无须注册)
	UB2	国际注册用户
	UB3	国内注册用户

虽然数据访查范围有所限制,但是国际注册用户可以使用大多数科学数据中心服务。

● 国内注册用户(UB3):这是前台用户中权限最多也是受众最广的角色,可以访问科学数据中心的无限制访问、公益性访问和商业性访问资源。主要服务于国内的科学数据用户,满足国内各个科研机构和个人对科学数据的需求。国内注册用户需要在数据中心系统中实名注册,且必须由系统进行身份验证。在数据汇交方面,用户还具备上传资源和数据的权限。

4 用户访问权限控制体系

访问控制本身是主体对客体访问权限的把控,只要主体通过授权获得对客体的全部或部分访问权限,就可以获得客体信息[16]。一般情况下,所有的系统平台都会设计自有的访问控制体系,作为控制系统权限的手段。访问控制的基本任务是,识别和确认访问系统的用户,并决定该用户可以对某一系统资源进行何种类型的访问。访问控制的目标是防止对信息系统资源的非授权访问及防止非授权使用信息系

统资源。从本质上看，访问控制体系的主要作用是确保系统的数据资源不会被非法访问，保障系统的安全性。

数据中心的访问控制体系（accessing control policy，ACP）包含用户分类体系、资源分级体系和服务访问授权体系3个部分。如**图1**所示，以国家对地观测科学数据中心为例，这3个部分密切相关、联动服务，构成一套完整的数据资源控制策略框架。在这3个部分的协同配合下，数据中心管理系统根据预先定义的访问控制策略授予用户不同类别的访问权限，从而对不同等级的数据资源的使用过程进行有效控制，完成整个系统的服务过程。

5 数据中心服务访问授权体系

数据中心的服务是指数据中心提供给用户的各种服务功能的总称，包括数据资源、数据业务软件系统操作功能等。数据中心服务的访问授权通过与用户角色权限相关联的证书授权（certificate authority，CA）来实现。数据中心的数据业务系统可分为后台管理系统、数据汇交系统和前台服务系统3个子系统，每个子系统都可提供多项服务，每项服务又可细分为若干种子服务。

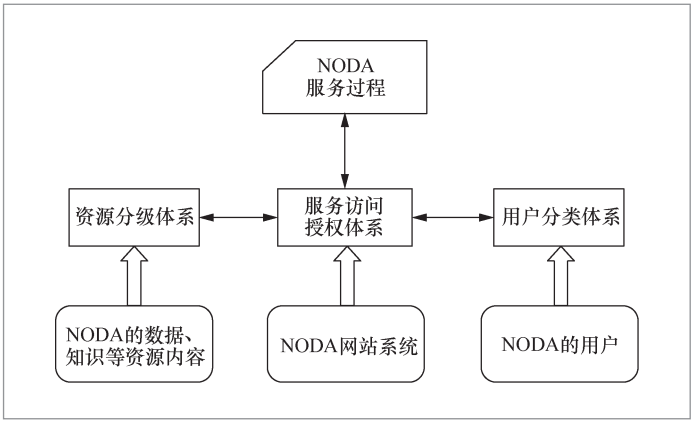

图1 数据中心访问控制体系（以国家对地观测科学数据中心为例）

5.1 数据中心管理业务

后台管理系统是科学数据中心系统的一个子集，承担着数据中心的管理和运维任务。一般提供权限管理、信息发布管理、订单审核、平台动态4种后台管理服务。

后台管理系统中最主要的是权限管理服务。权限管理可分为角色管理和用户管理两个子服务。角色管理服务包括3个操作权限：用户角色的新增、修改、删除。用户管理服务操作权限包括：后台及汇交系统用户新增、修改、删除以及前台用户新增、修改、停用。后台管理系统的使用主体主要是各类管理员用户，不同类型的管理员用户在后台管理系统中的服务访问授权也有所差别。顶级管理员（UA1）享有后台管理系统中的各项权限，栏目管理员（UA2）和栏目操作员（UA3）只能对自己负责的栏目板块进行管理，而团队管理员（UA4）只可管理与本团队工作相关的服务。**表3**展示了各类用户角色在后台管理系统的服务访问授权情况。

5.2 数据汇聚业务

数据汇交系统是数据中心的资源共享系统，负责平台数据资源和服务的交流与更新，主要是提供科研项目成果汇聚业务。数据汇交系统是依据不同的机构、人员和项目的身份提供服务的。每种服务对各自身份类别所属的数据集进行操作，操作权限包括上传、修改、删除、审核。应用本文提出的服务访问授权体系，各类用户角色在数据汇交系统的服务访问授权情况详见**表4**。

表 3 后台管理系统服务访问授权

服务	二级服务	操作权限	UA1	UA2	UA3	UA4	UA5	UB1	UB2	UB3
权限管理	角色管理	角色新增	√	√		√		×	×	×
		角色修改	√	√		√		×	×	×
		角色删除	√	√		√		×	×	×
	用户管理	后台及汇交系统用户新增	√	√		√		×	×	×
		后台及汇交系统用户修改	√	√		√		×	×	×
		后台及汇交系统用户删除	√	√		√		×	×	×
		前台用户新增	√					×	×	×
		前台用户修改	√					×	×	×
		前台用户停用	√					×	×	×
信息发布管理	新闻管理	新闻新增	√	√	√	√		×	×	×
		新闻修改	√	√	√	√		×	×	×
		新闻删除	√	√	√	√		×	×	×
		新闻审核	√	√				×	×	×
	数据发布	数据发布	√	√				×	×	×
		数据召回	√	√				×	×	×
订单审核	订单审核	订单审核	√	√	√	√		×	×	×
平台动态	平台监控	监控数据浏览	√	√	√			×	×	×
	统计报告	数据资源量整体统计	√	√	√	√		×	×	×
		数据贡献者统计	√	√	√	√		×	×	×
		按数据集统计	√	√	√	√		×	×	×
		项目汇交、访问、下载、用户情况	×	×	×	√		×	×	×
		机构汇交、访问、下载、用户情况	×	×	×	√		×	×	×

5.3 用户服务业务

为了扩大科学数据中心的使用范围和国际影响力，更好地满足国内外不同用户的数据需求，我国数据中心前台服务系统前端设计一般采用中文版和英文版两个同步版本。两者基本结构框架和服务内容大体一致，只在一些细节上有所差异。这种差异主要体现在两个系统版本的各服务栏目下，国内外用户对不同等级资源的下载与订单申请服务访问授权情况有所不同。

表 4 数据汇交系统服务访问授权

二级服务	操作权限	UA1	UA2	UA3	UA4	UA5	UB1	UB2	UB3
数据集汇交	上传	√	√	√		√	×	×	×
	修改	√	√	√		√	×	×	×
	删除	√	√	√		√	×	×	×
	审核	√	√	√			×	×	×

前台服务系统一般提供数据集查找、热点和专题栏目、新闻动态栏目、个人中心、帮助中心5种基础服务。在本文中，主要体现在国际注册用户（UB2）和国内注册用户（UB3）在资源访问权限级别上有所差异，同时也侧面印证了用户分类体系对服务访问授权体系的影响。**表5**展示了各类用户角色在前台服务系统的服务访问授权情况。

从**表5**可以看到，前台服务系统中的国内注册用户（UB3）具备对R0、R1、R2、R3这4个级别数据集的下载与订单申请服务权限，而国际注册用户（UB2）则不具备。在热点和专题栏目、新闻动态栏目、个人中心、帮助中心等服务中心，国际注册用户（UB2）和国内注册用户（UB3）所享有的操作权限也有较大的差别。前台服务系统实现了科学数据中心资源分级和用户分类两大体系的结合，形成数据资源与用户的对应关系，从而建立服务访问授权体系。

6 科学数据中心访问控制体系应用

国家对地观测科学数据中心是我国首批建设的20个国家级科学数据中心之一，是依托于中国科学院遥感与数字地球研究所建设的国家科技资源共享服务平台。历经多年建设，该平台具有了可持续、跨机构、一站式的数据共享服务能力，可提供多维度、多时相、多尺度的对地观测数据与其他相关资料资源。本文提出的数据分级、用户分类以及数据中心服务访问权限控制策略已经在国家对地观测科学数据中心的业务系统中开展了实际应用。

例如，使用系统管理员账号登录NODA内部管理系统后，可对数据中心的角色进行管理，如**图2**所示。主要是新增系统角色和分配角色权限。新增的系统角色是根据实际使用的需要，配置其角色名称、英文标识和角色权限描述，并在权限分配模块中赋予新角色在后台管理系统、前台服务系统、汇交系统中相应的访问权限。

系统管理员还可在内部管理系统中对当前系统中的管理员用户（UA）与普通用户（UB）进行管理，如**图3**所示，主要对各类用户的个人信息进行浏览、审核或编辑，及时删除个人信息异常的各类用户，从而保护系统安全。

当使用不同角色类型的账号登录NODA数据汇交系统时，系统中提供的服务功能也有所区别。以栏目管理员（UA2）账号登录，汇交资源审核栏目下会显示用户上传的数据资源，栏目管理员需要对该数据资源进行审核（如**图4（a）**所示）。栏目管理员逐一审核提交数据资源的标识信息、分类信息、来源信息、版权信息、元数据信息等信息后（如**图4（b）**所示），决定该数据资源是否可以进入NODA数据库，从而提供给具有相应访问权限的用户浏览与使用。此外，还可以进入数据管理模块，管理过往用户提交的各种数据资源（如**图4（c）**所示）。而以国际注册用户

表 5 前台系统服务访问授权

服务	二级服务	操作权限	UA1	UA2	UA3	UA4	UA5	UB1	UB2	UB3
数据集查找	数据集	浏览	√	√	√	√	√	√	×	√
		R0级资源在线下载	√	√	√	√	√	√	×	√
		R1级资源在线下载	√	√	√	√	√	×	×	√
		R2级资源在线下载	√	√	√	√	√	×	×	√
		R3级资源在线下载	√	√	√	√	√	×	×	√
		R4级资源在线下载	×	×	×	√(本团队)	√(本团队)	×	×	×
		R5级资源在线下载	×	×	×	×	√(本人)	×	×	×
		R0级资源离线订单申请	√	√	√	√	√	×	×	√
		R1级资源离线订单申请	√	√	√	√	√	×	×	√
		R2级资源离线订单申请	√	√	√	√	√	×	×	√
		R3级资源离线订单申请	√	√	√	√	√	×	×	√
		R4级资源离线订单申请	×	×	×	√(本团队)	√(本团队)	×	×	×
		R5级资源离线订单申请	×	×	×	×	√(本人)	×	×	×
热点和专题栏目	数据集+	浏览	√	√	√	√	√	√	×	√
新闻动态栏目	信息	浏览	√	√	√	√	√	√	×	√
个人中心	信息	修改	√	√	√	√	√	×	×	√
		注册	×	×	×	×	×	√	×	×
		审核	√	√	√	√	×	×	×	×
帮助中心	信息	浏览	√	√	√	√	√	√	×	√

图 2 NODA 角色管理系统界面

图 3 NODA 用户管理系统界面

（UB2）账号登录后，只有数据管理栏目，仅可查看和修改自身提交的数据资源（如图4（d）所示）。

结合大数据环境下地理信息服务发展的趋势[17-19]，基于本文建立的NODA平台具有如下应用价值：彻底实现了科学数据资源和用户的分类分级，增强了平台系统的安全性，推动了科学数据资源共享服务模式进步，并且促进了时空大数据应用。

7 结束语

科学数据共享事业的日益蓬勃发展对科学数据中心有效和安全管理科学数据资源提出了更高的要求。本文面向科学数据中心数据业务管理需求，制定了完善的资源和用户访问控制策略，并将其实际应用于科学数据中心运营中。本文提出的数据资源分级体系和用户分类体系对数据资源等

（a）栏目管理员数据汇交审核

图 4 NODA 数据汇交系统

（b）栏目管理员数据及审核

（c）栏目管理员数据管理

（d）国际注册用户数据管理

图 4 NODA 数据汇交系统

级和用户访问级别权限做出了明确规定，具有可操作、层次清晰明确等特点；本文提出的用户分类体系不仅融合了国际数据共享政策的最新成果，同时考虑了我国的实际情况，不仅保证了数据的安全性，并且最大限度地保障了科学数据的共享；访问授权策略灵活多样，有效串联了用户分类体系、资源分级体系和服务访问授权体系，顺应科学数据共享服务多样性、个性化的趋势。这套体系不仅可以应用于国家对地观测科学数据中心，还可以推广到其他科学数据中心，具有综合性、稳定性、可持续性、可扩展性等优点。

在未来的研究中，本文的访问控制体系将结合未来实际发展需求与趋势进行进一步的扩充和升级。例如针对不同角色用户偏好与访问控制关联性的相关关系进行深入研究，对访问控制体系做进一步改进，争取使本文提出的科学数据中心资源和用户访问控制体系成为国际认可和推广的体系标准。

参考文献:

[1] 杨行, 屈宝强, 赫运涛, 等. 世界主要国家科学数据资源共享和管理的对比分析和启示[J]. 中国科技资源导刊, 2016, 48(6): 18–25.
YANG X, QU B Q, HE Y T, et al. Contrast analysis and its revelation from scientific data resource sharing and management on main countries[J]. China Science & Technology Resources Review, 2016, 48(6): 18–25.

[2] 张芬. 大数据时代数据的分类分级管理及安全防护[J]. 计算机产品与流通, 2019(1): 129.
ZHANG F. Classified management and security protection of data in the era of big data[J]. Journal of Computer Products and Circulation, 2019(1): 129.

[3] 秦宇. 大数据时代网络安全管理面临的问题及管理措施探析[J]. 网络安全技术与应用, 2021(8): 168–169.
QIN Y. Problems and management measures of network security management in the era of big data[J]. Network Security Technology & Application, 2021(8): 168–169.

[4] 杜宇骁, 龚城, 伏安娜, 等. 哈佛大学Datatags数据分级系统研究及启示[J]. 图书馆杂志, 2019, 38(8): 17–26.
DU Y X, GONG C, FU A N, et al. Research on Harvard Datatags system and its inspiration for China[J]. Library Journal, 2019, 38(8): 17–26.

[5] 包英明. 大数据平台数据安全防护技术[J]. 信息安全研究, 2019, 5(3): 242–247.
BAO Y M. Data security protection technology in big data platform[J]. Journal of Information Security Research, 2019, 5(3): 242–247.

[6] 完颜邓邓, 陶成煦. 美国政府数据分类分级管理的实践及启示[J]. 情报理论与实践, 2020, 43(12): 172–177, 155.
WANYAN D D, TAO C X. The practice and enlightenment of American government data classification and hierarchical management[J]. Information Studies: Theory & Application, 2020, 43(12): 172–177, 155.

[7] 黄何, 刘勐, 袁辉. 基于多级属性加密的零信任访问授权控制方法研究与设计[J]. 电力大数据, 2020, 23(6): 51–56.
HUANG H, LIU J, YUAN H. Attribute-based encryption multi-level zero trust access control model research and design[J]. Power Systems and Big Data, 2020, 23(6): 51–56.

[8] 黄如花, 李楠. 开放数据的许可协议类型研究[J]. 图书馆, 2016(8): 16–21.
HUANG R H, LI N. A study of license types of open data[J]. Library, 2016(8): 16–21.

[9] 付德志. 湖北中烟数据分类分级方法研究[J]. 科技经济导刊, 2020, 28(24): 13–15.
FU D Z. Study on the classification method of Hubei tobacco data[J]. Technology and Economy Guide, 2020, 28(24): 13–15.

[10] 李松涛, 谢宗晓. 数据分类/分级及其相关标准解析[J]. 中国质量与标准导报, 2019(4): 14–16.

LI S T, XIE Z X. Data classification and classification and analysis of related standards[J]. China Quality and Standards Review, 2019(4): 14–16.

[11] YANG J J. A framework of user classification model of online user innovation communities based on user innovation value[J]. Open Journal of Social Sciences, 2020, 8(5): 232–244.

[12] YAN M, LI S J, CHAN C A, et al. Mobility prediction using a weighted Markov model based on mobile user classification[J]. Sensors, 2021, 21(5): 1740.

[13] 孙莉娜. 云计算数据中心访问控制研究[J]. 电子技术与软件工程, 2021(1): 186–187.
SUN L N. Research on access control of cloud computing data center[J]. Electronic Technology & Software Engineering, 2021(1): 186–187.

[14] 封孝生, 刘德生, 乐俊, 等. 临近空间信息资源访问控制策略初探[J]. 计算机应用研究, 2008, 25(12): 3702–3704, 3719.
FENG X S, LIU D S, YUE J, et al. Exploration on access control to near space information resources[J]. Application Research of Computers, 2008, 25(12): 3702–3704, 3719.

[15] 韩培强, 王钧. 张家峁矿业公司数字化矿井资源访问授权实现[J]. 电子测试, 2014(8): 65–67.
HAN P Q, WANG J. Access authorization to realize digital mine resources Zhang Jiamao mineral company[J]. Electronic Test, 2014(8): 65–67.

[16] 童遥. 云计算数据中心访问控制方法的研究[J]. 信息与电脑(理论版), 2018(24): 207–208.
TONG Y. Research on access control method of cloud computing data center[J]. China Computer & Communication, 2018(24): 207–208.

[17] 袁存忠, 邓淑丹. 地理信息大数据探讨[J]. 测绘通报, 2016(12): 105–107, 130.
YUAN C Z, DENG S D. Discussion of geographic information big data[J]. Bulletin of Surveying and Mapping, 2016(12): 105–107, 130.

[18] 周星, 桂德竹. 大数据时代测绘地理信息服务面临的机遇和挑战[J]. 地理信息世界, 2013, 20(5): 17–20.
ZHOU X, GUI D Z. Opportunities and challenges of geographic information services in the big data era[J]. Geomatics World, 2013, 20(5): 17–20.

[19] 周顺平, 徐枫. 大数据环境下地理信息产业发展的几点思考[J]. 地理信息世界, 2014, 21(1): 45–50.
ZHOU S P, XU F. Thoughts for developing geographic information industry under big data[J]. Geomatics World, 2014, 21(1): 45–50.

作者简介

曹乔卓然(1997–), 男, 郑州大学地球科学与技术学院硕士生, 主要研究方向为遥感应用、对地观测平台运营与维护。

陈祖刚(1989–), 男, 博士, 中国科学院空天信息创新研究院助理研究员, 国家对地观测科学数据中心数据管理部主任, 主要研究方向为对地观测知识挖掘。

李国庆（1968- ），男，博士，中国科学院空天信息创新研究院研究员，国家对地观测科学数据中心主任，主要研究方向为地球大数据管理和信息挖掘、科学数据共享。

李静（1976- ），女，中国科学院空天信息创新研究院高级工程师，国家对地观测科学数据中心副主任，主要研究方向为地球大数据管理、科学数据共享。

收稿日期： 2021-10-09
通信作者： 陈祖刚，chenzg@aircas.ac.cn
基金项目： 广西创新驱动发展专项资金项目（No.AA20302022）
Foundation Item: Guangxi Innovation Driven Development Special Fund Project (No.AA20302022)