引文格式：祁琼,张莉,裴利利,等. 一种基于RBAC的国土调查数据访问控制模型[J]. 地理空间信息, 2025, 23(1): 17-20. doi:10. 3969/j.issn. 1672-4623.2025.01.004

# 一种基于RBAC的国土调查数据访问控制模型

祁　琼[1]，张　莉[1*]，裴利利[2]，张　斌[3]
（1. 湖北省空间规划研究院，湖北 武汉 430071；
2. 松滋市自然资源和规划局，湖北 松滋 434200；3. 武汉大学 资源与环境科学学院，湖北 武汉 430079）

**摘　要：**对事前防范访问控制进行了研究，提出了针对国土调查数据的访问控制模型（LSD-RBAC）。该模型对RBAC模型进行空间重定义，对主客体进行时空扩展。结合国土调查数据的移动应用场景，关注主体的移动特征；在权限中扩展了时空范围、要素图层、属性特征等约束，支持细粒度的访问控制。根据LSD-RBAC模型和国土调查数据的访问控制过程，设计并实现了移动环境下访问控制系统。结果表明，LSD-RBAC模型能完成多条件约束下的国土调查数据访问控制。

**关键词：**空间数据处理；国土调查数据；访问控制
**中图分类号：**P208　　**文献标志码：**B　　**文章编号：**1672-4623（2025）01-0017-04

## Access Control Model for Territorial Survey Data Based on RBAC

QI Qiong[1], ZHANG Li[1], PEI Lili[2], ZHANG Bin[3]
(1. Hubei Spatial Planning Research Institute, Wuhan 430071, China;
2. Songzi City Natural Resources and Planning Bureau, Songzi 434200, China;
3. School of Resource and Environmental Sciences, Wuhan University, Wuhan 430079, China)

**Abstract:** Based on the geographical information data security technology, we studied the precautionary method of access control of territorial survey data. We proposed an access control model for territorial survey data, called LSD-RBAC. This model redefines the RBAC model in space, and expandes the subject and object in space and time. Combined with the mobile application scenarios of territorial survey data, the model pays attention to the movement characteristics of subject, and expands the constraints of spatio-temporal range, element layer and attribute characteristics, and supports fine-grained access control. Based on the access control process of LSD-RBAC model and territorial survey data, we designed and implemented an access control system in mobile environment. Experimental result shows that the LSD-RBAC model can complete the access control under the multi-condition constraint of territorial survey data.

**Key words:** spatial data processing, territorial survey data, access control

国土调查数据用途广泛，但缺乏严格的脱密规程，导致其应用场景和开放程度受到限制，严重影响了国土调查成果的转化效率，因此设计严格的数据访问控制策略非常必要。空间数据保护技术包括加密技术、访问控制技术和数字水印技术等[1]。访问控制技术通过设定访问控制规则，限制用户的行为和操作，防止用户对未授权资源进行访问[2]。目前对访问控制模型的研究集中于对强制访问控制模型、自主访问控制模型和基于角色的访问控制模型进行空间应用的扩展，其中基于角色的访问控制模型较受关注，主要研究方向包括模型设计、授权方法、策略管理和实现[3-6]。基于角色的访问控制模型包括两种思路：①以位置为扩展的关键点，将主体的位置变化作为访问控制授权状态变化的核心；②关注客体资源的空间特征，制定访问控制策略时重点考虑客体的空间约束。第一种思路重点考虑主体的移动特征对用户访问授权的影响：SRBAC模型[7]能根据用户的空间位置做出授权决策，将角色定义为空间角色，角色权限只能在特定空间范围内才能激活；基于上下文的访问控制模型[8]采用层次式的位置模型，并在构建访问控制策略时引入逻辑位置，可实现建筑物房间层次的访问控制，粒度更细。第二种思路的模型中GEO-RBAC[9]是一个完备的空间访问控制模型，对其中要素进行了空间重定义，引入主体位置特征，并将角色的激活与主体的位置信息关联起来。该模型除了将角色扩展为空间角色外，权限集中的约束也扩展为空间约束，包括

第一作者简介：祁琼（1983—），硕士研究生，高级工程师，主要从事自然资源调查监测、地理信息系统及遥感应用工作，E-mail：123167296@qq.com。
通信作者：张莉（1978—），本科，工程师，主要从事自然资源调查监测、地理信息系统及遥感应用工作，E-mail：398893481@qq.com。

空间尺度[10]、要素图层[11]、空间关系[12]、授权图层[13]、上下文[14]等，能实现对地理空间数据灵活、细粒度的访问控制。空间的表达离不开时间，扩展时间约束[15-16]能使模型更加完善；但上述模型也存在一定问题，对空间概念的理解过于简单，只关注主体的移动特征，未考虑空间数据的时效性和主体访问的时间限制等。鉴于此，本文提出了一种针对国土调查数据的访问控制模型（LSD-RBAC），探讨了模型的时空角色、权限、会话等基本元素以及空间范围、时间范围、属性特征等扩展元素，并定义了模型元素层次结构。通过制定访问控制的规则和策略，描述了国土调查数据访问控制流程，构建了以LSD-RBAC模型为基础的访问控制系统并进行功能验证。

## 1 LSD-RBAC模型定义

### 1.1 国土调查数据结构和特征

国土调查成果包括数据成果、图件成果、文字成果和数据库成果。其中，数据成果包括土地分类、土地权属、耕地坡度分级、耕地细化调查、耕地质量等要素图层数据；图件成果基于数据成果生产，包括土地利用现状、地权权属、国土调查图集等地图数据；文字成果为各种调查、技术、分析报告；数据库成果是上述成果的集成，包括国家、省、市、县4级土地利用和专项调查数据库。国土调查成果特征包括：①数据量大、类型多，以湖北省为例，全省共包含103个县级行政单位，每个县包含30多个空间要素图层，每个空间要素图层包含2万~30万个调查图斑；②数据规范，土地利用数据库对空间要素分层、要素属性结构、属性值代码进行了明确定义，规范性降低了解密难度，但增加了加密和控制策略的设计难度；③应用场景复杂，需在确保数据安全的前提下服务野外调研需求，面临数据的采集、传输、使用等全过程安全控制要求。

国土调查数据的权威性、应用广泛性与其保密性的矛盾导致数据公开难度大、适应审批制度的访问流程复杂，进而阻碍其信息化创新应用。国土调查数据访问控制面临的困境包括：①国土调查数据安全与隐私算法的合规问题，即公开是发挥数据资料效能的必由之路，而公开的前提是通过加密算法保证其安全可控、可追溯；②面向业务角色的数据范围、要素类别、专题粒度的访问控制问题，即提供不同行政单位、不同业务部门、不同应用场景对国土调查数据多尺度多粒度数据访问的管控机制；③国土调查数据变更业务与检索业务交叉的复合业务流程增加了访问控制的复杂性，即年度调查数据的更新、审核、审批涉及的数据作业权限与一般业务访问权限导致的数据时序问题增加了访问控制的难度。

### 1.2 模型结构

对RBAC模型进行空间重定义，考虑要素图层、时间约束、空间约束等对访问控制的影响[17]。将国土调查数据特征与RBAC模型相结合，构建LSD-RBAC模型能满足国土调查数据访问控制的需求[18]。LSD-RBAC模型包含用户、角色、操作、权限、会话、时间、位置、时空尺度、属性等元素。LSD-RBAC模型为包含时空信息的用户分配一个角色，该角色在一定的时空条件下才能被激活，角色是约束的权限集，权限集由时间、空间、图层、属性等特征组成。用户到激活角色的映射会形成一系列会话，创建这些会话的前提是用户的时空特征满足角色激活的时空条件。

### 1.3 模型元素

1）定义 $U$ 代表模型中的用户，是访问请求的发起人，系统会根据用户情况为其分配角色，用户通过角色拥有权限，从而获得对其权限范围内国土调查数据的访问资格。$U=\{u_1,u_2,\cdots,u_n\}$，$U_{\mathrm{Attr}}$ 为用户具有的属性，包括用户发起访问请求的位置和时间。

2）定义 $R$ 代表角色，是一个或一群用户在组织内可执行操作的集合，代表用户在组织内的职能或任务。作为国土调查数据的扩展，LSD-RBAC模型中的角色是拥有时空范围的时空角色。时空角色是包含角色名、角色空间范围和时间范围的三元组。同一角色名与不同时空范围的组合对应着不同的时空角色，如外业人员作为一个角色，表示承担外业人员角色的用户只能在指定的外业区域和时间内完成相应的工作，而角色同为外业人员但工作空间范围不同则认为是不同的时空角色。角色是访问主体与客体之间的桥梁，是模型的核心元素，是用户与权限之间的代理层，起到解耦用户与权限的作用。时空角色既是用户的集合，又是权限的集合，用户、角色与权限之间是多对多的关系，一个用户可以拥有多个角色，一个角色也可以被分配给多个用户；一个角色可以拥有很多权限，一个权限也可以被配置给多个角色。

3）定义PRM代表权限，是对客体的操作。权限采用三元组的形式，即 $<\mathrm{op},\mathrm{ob},\mathrm{fc}>$，其中op为操作；ob为资源，本文中指国土调查数据细化到图层的数据；fc为空间约束，包括对国土调查数据的时空约束、属性约束和图层约束。定义PRMS代表权限

集，是所有对国土调查数据访问权限的集合。每个角色都会指向一个权限集，时空角色拥有的权限集是PRMS的子集。权限集内容包括角色对数据可执行的操作、数据所属的要素图层、国土调查数据的属性信息集等。时空角色权限集用于显示时空角色能够访问的国土调查数据要素图层，以及能够对这些图层中地理实体进行何种操作。对国土调查数据权限集做了两个方面的扩展：①对操作的扩展，国土调查数据操作既包含增删改查等普通操作，又包含空间数据的缩放、漫游、平移、旋转等空间操作；②增加对要素图层的支持，限定时空角色能够访问的图层。$PRMS = 2^{OPS \times OBS \times FCS}$，表示权限集PRMS是操作集OPS、对象集OBS和空间约束集FCS的笛卡尔积的幂集。

4）定义S代表会话，系统在用户登录成功和用户激活角色时建立。用户建立会话时会查询当前用户拥有的角色，并将这些角色加载到会话中，以备后续用户请求访问时使用。用户访问资源需要先激活角色，通过角色获得相应的权限，才能进行访问，因此会话中包含用户、角色和权限。对于会话，存在以下定义：$S \to U$ 为会话到用户的映射，一个会话只能关联一个用户；$U \to 2^S$ 为用户到会话集的映射，表示一个用户可以关联多个会话；$S \to 2^R$ 为会话到角色的映射。

5）定义LC代表空间位置，是主体在空间中的分布状态，可描述用户的位置以及角色能被激活的空间范围等。为使系统能够根据用户所处的位置做出授权决策，必须获得发出访问请求设备的位置信息。空间位置包括物理位置（RPOS）和逻辑位置（LPOS）。物理位置包含经纬度信息，是所有可能物理位置的集合，从用户使用的移动设备GPS功能上获取。逻辑位置是物理位置的抽象，无明确的坐标信息，而是通过对象的概念对位置进行分类描述。引入逻辑位置有助于策略的描述和判断，还可表达相等、包含、相交、相离等逻辑关系。逻辑位置的表达能力强于物理位置，因此访问控制中物理位置通常需要转换为逻辑位置，以便于策略的判定。定义位置映射函数MF将物理位置转换为逻辑位置。

$$MF(rp) = lp, rp \in RPOS, lp \in LPOS$$

6）定义TM代表时间信息，是角色对国土调查数据资源访问时间范围的权限约束，最小粒度为小时，包含3个参数，即 $T = \{time1, time2, periods\}$，time1为起始时间，time2为终止时间，格式均为年月日；periods为时间段的集合，可包含一天中的多个时间段。时间可以约束国土调查数据，用以约束客体本身的时间属性，也可以约束角色，用以约束主体的访问时间。周期时间采用日历作为时间集，包含年份、月份、星期、天数和小时，其中小时是最小粒度的定义。

7）定义AT代表属性信息，包括元属性和要素属性。元属性MA包括图层名、行政区划、图层要素类型等基本信息。要素属性TA是图层属性表中的属性值，某些属性信息对国防军事、经济发展具有重要意义，若泄漏会存在很大风险，因此将属性特征引入空间约束就是为了保证这些重要的属性信息安全。定义 $TA = <name, value>$，name为属性字段名称，value为单条记录值，用该形式记录需要约束的属性信息，可实现对字段粒度的访问控制。

### 1.4　角色继承与权限继承

1）角色继承亦称角色分层，有利于角色的管理和授权。角色的层次关系说明不同角色虽然具有不同的权限集，但各权限集并不是完全孤立的，角色之间具有偏序关系，即角色权限有大有小，且存在一个角色完全包含另一个角色的情况，这种关系就是角色继承。角色继承表示了角色的偏序关系，在修改单个角色权限时，也会对继承该角色的权限进行修改，实现对用户访问控制权限的更新。$RH \in ROLES \times ROLES$，反映了角色之间的继承关系。$\geqslant_R$ 反映角色的偏序关系，$R_1 \geqslant_R R_2$ 表示 $R_1$ 拥有 $R_2$ 权限集中所有的权限，且 $R_1$ 的所有用户也是 $R_2$ 的用户。继承包含角色的时空关系和权限，若时空角色 $R_1$ 继承自时空角色 $R_2$，则 $R_1$ 具有 $R_2$ 权限集中的所有权限，同时 $R_2$ 角色激活的时空范围包含在 $R_1$ 的时空范围之中。

2）权限继承。空间操作之间存在偏序关系，即有些操作是建立在另一些操作的基础上的，如某个角色拥有更新要素的权限而不拥有获取要素的权限，这显然是没有意义的授权，上述权限之间有依赖关系，在授予角色权限时需要考虑。定义权限依赖规则 $\forall p_1, p_2 \in P$，若 $p_1$ 依赖于 $p_2$，记为 $p_1 \to p_2$。权限继承可认为是操作集的继承，即将权限继承归为操作继承，$op_1 \to op_2$ 表示拥有操作集 $op_1$ 的角色一定拥有操作集 $op_2$，如 $op_2$ 中包括查看、编辑操作，则 $op_1$ 也拥有这些操作（表1）。

## 2　访问控制策略与过程

### 2.1　角色激活

角色激活是指将用户拥有的角色权限集赋予用户。在登录成功后，系统会对用户建立会话，查询用户拥有的时空角色，并将角色加载到会话中。由于时空角色是一个三元组 $<r, lc, tm>$，在会话中角色必须

表1 空间操作的偏序关系

| 空间操作 | 相应依附空间操作 |
|---|---|
| 选择 | 浏览 |
| 浏览 | 创建 |
| 选择、插入 | 创建 |
| 创建 | 修改 |
| 选择、插入、更新、删除 | 修改 |

满足时空约束才能被激活，只有被激活的角色才能依据权限集对地理实体进行各种操作。这种角色激活方式既保证了访问控制的安全又起到管理作用。

用户发起的空间数据访问请求为一个五元组<s, geo, tm, op, ob>，其中s为用户所在的会话，geo为空间范围，tm为发起请求的时间，op为操作，ob为geo空间范围内能操作的要素图层。五元组表示s在tm时间对geo内的ob发起op，前提是用户拥有时间在tm范围，位置在geo的角色集$\{R_1, R_2, \cdots, R_n\}$，这个角色集是$R_s$的子集（图1）。

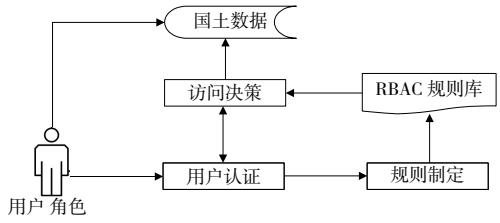



图1 授权决策过程

### 2.2 访问控制过程

具体访问控制流程为：①用户登录，输入用户名、密码，发起认证请求，若认证成功则建立针对该用户的会话，登录成功，若用户名或密码信息错误则拒绝该认证，访问失败；②获取用户当前的时空范围和拥有的角色集，获取角色是空间约束和时间约束，若用户的时空范围包含在角色的时空约束中，则激活该角色，获取激活角色的权限集，归并所有角色的权限集，即当前用户的访问控制约束范围，用户可在该约束范围内进行访问请求；③用户发起访问请求后，根据用户的时空信息和时空角色信息判定访问请求，根据授权决策，若请求访问的区域和权限满足条件，则发起数据请求，对数据进行解密操作，将满足访问权限的空间要素区域返回给用户或提交用户对空间要素的操作，反之则拒绝用户的请求。

## 3 实验结果与分析

实验选择某县国土调查数据中的地类图斑图层和乡镇界线图层，将数据拷贝到移动端。管理员创建角色和权限规则，将权限分配给角色，构建角色的权限集，为用户分配角色。

1）若某一用户的角色拥有在工作日9：00—17：00访问某区数据的权限，其在非授权时间或位置无法访问数据。

2）多元特征约束下的访问控制具体可分为：①无限制情况下可操作所有区域要素图层；②在要素图层约束下，只能访问其拥有权限的图层；③空间约束下的情景，用户只能对所在乡镇的数据实施解密；④用户在其拥有角色所能访问的空间范围之外无法访问数据；⑤用户在属性约束下查看要素属性时，将根据角色的访问权限返回属性数据，具有属性约束的角色无法查看完整的属性数据。

## 4 结 语

本文基于传统RBAC模型，提出了面向国土调查数据的LSD-RBAC模型。该模型从两个方面进行扩展：①对用户和角色都加入时空限制，用户只有在角色时空范围内才能激活角色，即角色为时空角色，具有时空范围，通过关注主体的时空特征，将移动环境的变化纳入访问控制中，提高了模型的安全性；②对模型中的元素进行空间重定义，在权限上扩充了要素图层、时空范围、属性信息等约束条件，使权限集的制定更加细化。在定义访问控制模型并介绍模型结构和模型组成元素的基础上，制定了访问控制规则和策略。实验结果表明，本文提出的访问控制策略能顾及国土调查数据的具体场景，具有重要的应用价值。

## 参考文献

[1] 朱长青,任娜,周子宸,等. 地理大数据安全技术研究现状与展望[J]. 现代测绘,2020,43(6):9-13

[2] 沈海波,洪帆. 访问控制模型研究综述[J]. 计算机应用研究,2005,22(6):9-11

[3] 林家元,方裕,陈斌. 空间数据访问控制研究[J]. 地理与地理信息科学,2008,24(2):9-13

[4] 张德胜,冯登国,陈驰. 一种面向空间数据库矢量数据的授权模型与实现方法[J]. 计算机研究与发展,2011,48(8):1 524-1 533

[5] Ahn G J, Sandhu R. Role-based Authorization Constraints Specification[J]. ACM Transactions on Information and System Security (TISSEC),2000(3):207-226

[6] Hansen F, Oleshchuk V. SRBAC: A Spatial Role-based Access Control Model for Mobile Systems[C]//Proceeding of 7th Nordic Workshop on Secure IT Systems,2003

（下转第33页）