材料科学数据共享工程标准草案

材料数据访问控制规范

（征求意见稿）

（本稿完成日期：2010 年 11 月）

2010-11 发布

目　录

前　言

本标准草案（《材料数据访问控制规范》）是在科学数据共享核心数据的基础上进行扩展而成的材料领域的数据访问控制标准。

材料数据访问控制在规范的数据模型基础上，进一步规范数据存取控制手段、数据操作函数、参数、单位转换等内容，并针对不同用户、不同数据源的数据访问权限制定规范化的控制标准。

本标准是在科学数据共享标准化工作组的数据访问控制标准制定人员的协助下，同材料领域的专家共同制定完成的。

本标准草案主要起草单位：北京科技大学，中科院金属研究所，西北工业大学。

材料数据访问控制规范

1 范围

本标准定义了访问一个材料领域具体对象所需要的数据存取控制手段、数据操作函数、参数、单位转换等材料数据访问控制的相关规范及内容。

本标准适用于材料科学数据共享中心（网）以及参加材料科学数据中心（网）的各个单位子系统或资源节点的数据访问控制的权限管理。

本标准的制定有利于材料科学数据共享数据集的管理，提高数据库建库质量，促进数据加工的规范化、标准化，实现数据交流与共享。

本标准是制定材料领域数据访问控制标准的基础。

2 规范性引用文件

下列规范性引用文件通过本部分的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准。但是，鼓励根据本标准达成协议的各方，研究是否可使用这些文件的最新版本。但是不注日期的引用文件，其最新版本适用于本标准。

SDS/T 2132—2004 数据元标准化原则与方法（科学数据共享技术标准）

SDS/T 2134—2004 数据交换格式设计规则（科学数据共享技术标准）

SDS/T 2321—2004 科学数据中心建设规范（科学数据共享技术标准）

SDS/T 2322—2004 科学数据网建设规范（科学数据共享技术标准）

SDS/T 2133 -2004 材料科学数据模式描述标准

SDS/T 2213—2004 材料科学数据共享工程数据与服务注册规范

SDS/T 2221.2—2004 材料科学数据共享工程数据访问服务接口规范

GB/T 13725-2001 建立术语数据库的一般原则与方法（中华人民共和国国家标准）

GB/T 17532-1998 术语工作计算机应用词汇（中华人民共和国国家标准）

GB/T 7408 数据元交换格式信息交换日期和时间表示法（eqv ISO 8601）

GB/T9387.1-1998 信息技术开放系统互连基本参考模型第 1 部分：基本模型(idt ISO/IEC 7498-1:1994)

GB/T9387.2-1995 信息处理系统开放系统互连基本参考模型第 2 部分：安全体系结构(idt ISO 7498-2:1989)

GB/T 18794.1-2002 信息处理系统开放系统互连开放系统安全框架第 1 部分：概述(idt ISO/IEC 10181-1:1996)

GB/T 18794.2-2002 信息处理系统开放系统互连开放系统安全框架第 2 部分：鉴别框架(idt ISO/IEC 10181-2:1996)

GB/T18794.3-2003 信息技术开放系统互连开放系统安全框架第 3 部分：访问控制框架

Unified Modeling Language 1.5　统一建模语言 1.5（OMG）

3　一致性要求

在材料领域科学数据共享工程中直接使用本标准时数据访问权限应与本标准保持一致，材料领域专用数据访问控制标准必须遵循本标准的规定。

4　术语

本标准采用下列术语和定义。

访问控制（Access Control）

按用户身份及其所归属的某预定义组来限制用户对某些信息项的访问，或限制对某些控制功能的使用。

访问权限（Access Authorization）

根据在各种预定义的组中用户的身份标识及其成员身份来限制访问某些信息项或某些控制的机制。

权限管理（Authorization Management）

根据系统设置的安全规则或者安全策略，用户可以且只能访问自己被授权的资源。

访问控制信息（Access Contorl Information，ACI）

用于访问控制目的的任何信息，其中包括上下文信息。

访问控制证书（Accessc Ontrolc Ertificate）

包含 ACI 的安全证书。

访问控制策略（Access Contorl Policy）

定义可发生访问控制条件的规则集。

访问请求（Accesse Request）

操作和操作数，它们构成一个试图进行的访问的基本成分。

科学数据资源（Scientific Data Resources）

特指以公益性和基础性为研究应用价值的数据资源，包括观测、监测、调查、试验、实验以及研究等科学技术研究活动过程中产生的原始性数据，以及按照不同科技活动需求进行系统加工整理的各类数据。

科学数据共享服务（Scientific Data Shared Services）

为提供科学数据共享所提供的技术服务，包括：目录服务、导航服务、数据信息发布、数据检索、数据产品加工、数据以数据产品分发等。

数据服务基础平台（Infrastructure for Data Services）

用于实现科学数据共享服务功能的信息基础设施，主要包括 Internet 服务、数据库服务等。

数据管理（Data Management）

利用数据库、数据仓库、元数据和网络等技术，建立分布式、集中式或集中加分布式数

据管理系统，开展数据接收、组织存储、运行维护、更新、共享交换等工作，实现对数据资源的有效组织和应用。

5 一般性概述

5.1 目标

访问控制基于安全框架的主要目标是对抗涉及计算机或通信系统的非授权操作的威胁。该材料数据访问控制的目标可以概括为：通过进程对数据、不同进程或其他计算资源访问的控制；在一个安全域内，及跨越一个或多个安全域的访问控制；在访问期间对更改授权做出反应的访问控制等。

5.2 适用范围

本规范适用于材料数据访问控制的设计、开发和管理范畴。

主要适用于系统管理人员、实施人员及设计开发人员。

5.3 实施建议

本规范旨在解决材料科学共享网相关数据内容的访问控制问题，权限管理是一种基于权限控制的访问策略，该技术应具备如下特点：

a）可实现用户与数据中心之间的直接身份验证；

b）可实现用户权限的动态更新管理；

c）可保障数据的机密性、完整性；

d）具有高度可扩展性；

e）采用对等思想，具有普适应性；

f）协议的子模块相互独立、灵活，便于取舍。

基于此，建议本项目按照本规定，建立规范的权限管理机制，对材料科学共享网实施统一的数据资源定级、分组及权限控制管理。

6 材料数据访问控制设计方案

6.1 总体设计

材料科学共享网数据访问控制采用基于中心节点进行权限管理的访问控制方案，每个子节点都有不同级别的权限访问控制，通过对用户访问权限的分组配置与数据表权限定制，实现对不同节点数据表的灵活访问控制与个性化定制服务，实现简单、维护方便。

6.2 使用对象

针对材料数据访问控制的使用对象是主节点与各分节点的管理员。各节点管理员可通过各自权限设置模块进行相关权限的分配、分组管理、修改等控制，实现节点间数据访问的跨域授权。

6.3 功能框架

6.3.1 访问控制过程描述

材料数据访问控制采用基于中心节点的跨域认证访问方式，其框架流程如图 1 所示。

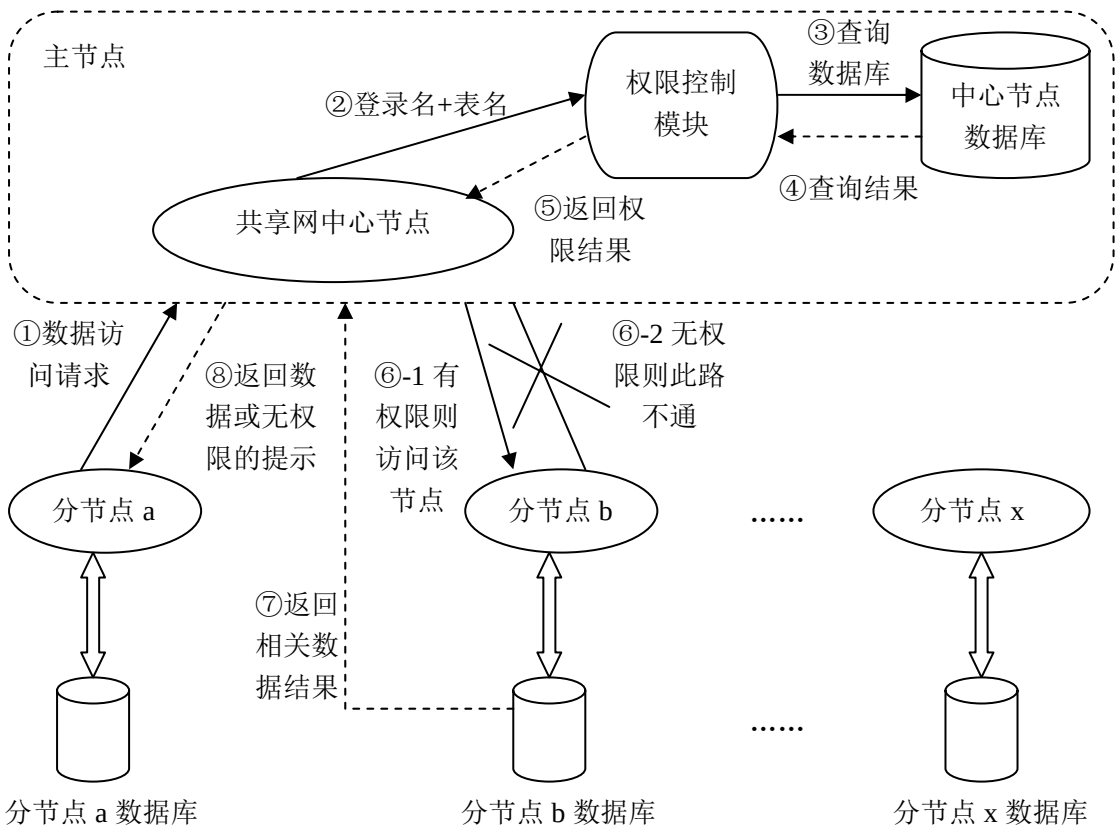

图 1 基于中心节点的数据访问控制

从图中可以看出，在若干分节点中，当 a 节点用户需要访问 b 节点数据时，基于中心节点的跨域数据访问过程为：首先，分节点 a 向共享网中心节点发送数据访问请求；其后由共享网中心节点的权限控制模块在其数据库查询的基础上，对取得的登录名与所要访问的数据表名进行本地访问控制的权限判断，并返回权限结果；如果不允许，则无法访问分节点 b，并向分节点 a 提示该用户针对这个数据表没有访问权限；如果允许，则访问数据表所对应的分节点 b 的数据库，并将相关数据结果通过共享网中心节点返回给发出数据访问请求的分节点 a。

6.3.2 授权过程说明

材料科学共享网的数据访问控制，通过 JSP 页面提供对角色、组、数据库、数据表、相关字段等过滤条件的维护，从而进行相关权限的灵活设置。分节点只有得到授权，才能基于中心节点进行跨域数据访问。其授权过程分为以下几个方面：

（1）用户管理

共享网中心节点赋予各个分节点一个管理员帐号，分节点管理员负责本节点的用户权限管理。系统限制每个管理员只能对本节点的数据资源与用户进行分级和授权，而对其它节点资源则无权管理与授权。如果一个节点的用户申请另一节点的资源，则需要先得到另一个分节点的管理员授权批准。各级管理员通过“用户管理”对所管辖范围内的用户信息进行维护。

（2）权限管理

各级管理员通过“权限管理”对所在节点的数据表及其权限名词进行维护，可针对某些

数据表添加新的权限，或删除已有权限。

（3）权限分组

各级管理员可通过“权限分组”查看该节点的权限分组情况，该模块实现了对某个节点访问权限的分级情况建立相应的分组管理功能，可以实现单一分组的权限修改、删除及新权限组的建立功能。其中，新建权限分组可自动防止重名，一键式修改所有权限功能使得权限修改更加简便、直观。

（4）用户授权

各级管理员可通过“用户授权”查看各节点用户对需要访问的数据表所在节点的权限组分情况，并可通过修改其相应的权限组名，对该用户进行授权。

该授权过程所对应的使用对象可划分为四类：(a) 系统管理员，在系统中拥有最高权限，可以以任何一个建库单位的单位管理员身份登入系统，维护和管理该单位管理的全部用户、权限组及数据访问控制；(b) 分节点管理员，每个建库单位有一位单位管理员，可以对本单位维护的用户、权限组及数据访问进行控制与维护；(c) 授权用户，是非管理员级别的普通注册用户，没有授权能力，但可以被系统管理员及所在节点管理员授权，并因此获得对某些数据资源的访问权限；(d) 一般用户，即匿名用户，具有通常的访问浏览默认权限，但没有授权控制能力及关键数据的访问权限。

6.3.3 身份验证过程说明

在共享网中心节点建立后，当节点 a 已注册的用户 user_a 请求访问节点 b 的数据表 table_b 时，需在中心节点数据库中根据获得的 user_a 的登录名与 table_b 的表名获得其所对应的源节点 n1 与目标节点 n2，由此获得从 n1 到 n2 所对应的权限组名 group，从而解析出该组名所对应的数据表，并判断所要访问的数据表 table_b 是否存在于这些表中，而后返回权限结果，存在则通过身份验证并调用分节点数据库信息返回相关数据资源，不存在则提示该用户 user_a 对数据表 table_b 没有访问权限。

通过此方式可以实现各个节点的用户向中心节点的平滑迁移，已有用户无须“二次登录”就可以访问相关节点的数据资源，同时不影响中心节点和各分节点新用户的注册，使得数据访问的授权与验证控制更加灵活、便捷。

6.3.4 数据库访问过程

在中心节点需构建五个数据表，分别是用户表（TUSER）、数据模式表（DB_GUIDE）、用户权限表（TUSERPERMISSIONNEW）、权限组表（TGROUP）和权限表（TPERMISSION），这五个表的操作都是由各节点的管理员登录中心节点进行授权管理的。

（1）用户表（TUSER）

LOGIN_NAME（登录名）	NODE_SHORT（节点名）
user_a	n1

根据所获得的用户登录名，在用户表中查询得到其所对应的结点名，即为源节点名。

（2）数据模式表（DB_GUIDE）

TABLE_NAME（数据表名）	NODE_NAME（节点名）

table_b	n2

根据所获得的数据表名，在数据模式表中查询得到其所对应的节点名，即为目标节点名。

（3）用户权限表（TUSERPERMISSIONNEW）

LOGIN_NAME （登录名）	SRC_NODE_SHORT （源节点）	N2 （权限组名）
user_a	n1	group

通过对照将目标节点名与用户权限表的相关列明进行对应，并根据用户名、源节点 n1 与目标节点 n2 在用户权限表中进行查询，得到该源节点用户 a 针对目标节点 b 的数据进行访问时所分配的权限组名。

（4）权限组表（TGROUP）

GROUP_NAME （权限组名）	NODE_SHORT （节点名）	PERMISSION_NAME （权限名）
group	n2	per

根据所获得的权限组名及目标节点的节点名，在权限组表中查询得到相应的权限名。

（5）权限表（TPERMISSION）

PERMISSION_NAME （权限名）	NODE_SHORT （节点名）	PERMISSION （权限名）
per	n2	tn

根据所获得的权限名与目标节点名，在权限表中查询得到相应的权限名，并与最初得到的数据表名 table_b 进行比较，存在则具有权限可以访问，否则无权访问。

6.3.5 各节点任务说明

中心节点和各类分节点所完成的主要任务如下：

（1）中心节点

添加、修改各个分节点路由表的地址信息；接收各个分节点发来信息，并记录、修改、删除分节点的用户信息；维护权限管理及分组相关设置；转发各分节点之间的消息。

（2）提出数据访问请求的分节点 a

主要任务是发送访问授权请求和接收访问请求的反馈结果。

（3）被访问的分节点 b（访问其数据资源）

添加、修改分节点 a 的用户权限分组及相关设置；对各权限组所对应的分节点 b 中的数据资源进行权限配置；修改中心节点针对节点 a 的授权；转发消息。