ICS 35.080
L 77

SZDB/Z

深圳市标准化指导性技术文件

SZDB/Z 17.7-2008

深圳市电子政务应用服务规范 第7部分：访问控制服务接口规范

Electronic Government Application Service Specification—

Part 7 : Access Control Service API Specification

2008-11-18 发布　　2008-12-01 实施

深圳市质量技术监督局发布

目　次

前　言

SZDB/Z 17-2008《深圳市电子政务应用服务规范》目前分为10个部分：

——第1部分　《总则》
——第2部分　《应用系统分类及代码规范》
——第3部分　《应用系统描述规范》
——第4部分　《组织身份模型数据规范》
——第5部分　《应用服务运行管理框架规范》
——第6部分　《组织身份服务接口规范》
——第7部分　《访问控制服务接口规范》
——第8部分　《单点登录服务接口规范》
——第9部分　《电子表单服务接口规范》
——第10部分　《业务流程服务接口规范》

本部分为SZDB/Z 17-2008的第7部分。

本技术规范适用于深圳市各级党政机关的信息化建设工作。对于本部分未能涵盖的内容将依据本技术规范的编写原则对本部分内容进行扩充。

本技术规范文件由深圳市信息化领导小组办公室、深圳市福田区信息中心提出。

本技术规范文件由深圳市信息化领导小组办公室归口。

本技术规范文件由深圳市信息化领导小组办公室、深圳市福田区信息中心、北京有生博大软件技术有限公司共同起草。

本技术规范文件主要起草人：贾兴东、陈朝祥、张雁、高新辉、王克照、石卫宁、赵斌、李淼、周礼洪、杨海波、王姝、张焕焕、刘用军、梁文龙等。

本技术规范文件为首次发布。

深圳市电子政务应用服务规范
第7部分：访问控制服务接口规范

1 范围

本部分定义了权限管理模型，给出了访问控制框架的组成部分和各部分的技术要求，规定了权限访问接口、权限管理接口和数据集权限接口，提出了访问控制技术要求。适用于应用系统的资源权限控制和数据权限控制。

本部分主要用于深圳市各级党政机关的信息系统规划与建设，以及电子政务信息系统建设的系统集成商、软件开发商和监理单位进行信息化规划、建设。适用于对应用系统的资源和数据进行授权、权限控制，提供权限管理服务。

2 规范性引用文档

下列文件中的条款通过本部分的引用而成为本部分的条款。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部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

SZDB/Z 17.1 -2008　电子政务应用服务规范 第1部分：总则

SZDB/Z 17.4 -2008　电子政务应用服务规范 第4部分：组织身份模型数据规范

SZDB/Z 17.6 -2008　电子政务应用服务规范 第6部分：组织身份服务接口规范

ISO/IEC 9075: 1992, Information Technology-Database Language SQL

3 权限管理模型

3.1 概述

访问控制是针对越权使用资源的防御措施。基本目标是为了限制访问主体（用户、进程、服务等）对访问客体（文件、系统等）的访问权限，使计算机系统在合法的范围内使用，决定用户能做什么，也决定代表用户的程序能做什么。

访问控制决定了谁能够访问系统，能访问系统的何种资源以及如何使用这些资源。访问控制能够阻止未经允许的用户有意或无意地越权获取数据。

3.2 访问控制基本概念

主体（Subject）：或称为发起者(Initiator)，是可以访问资源的实体，通常指用户或代表用户执行的程序。

客体（Object）：是需要保护的资源，又称作目标（target）。

授权（Authorization)：是可以对资源执行的动作，例如读、写、执行或拒绝访问。

3.3 访问控制服务原理

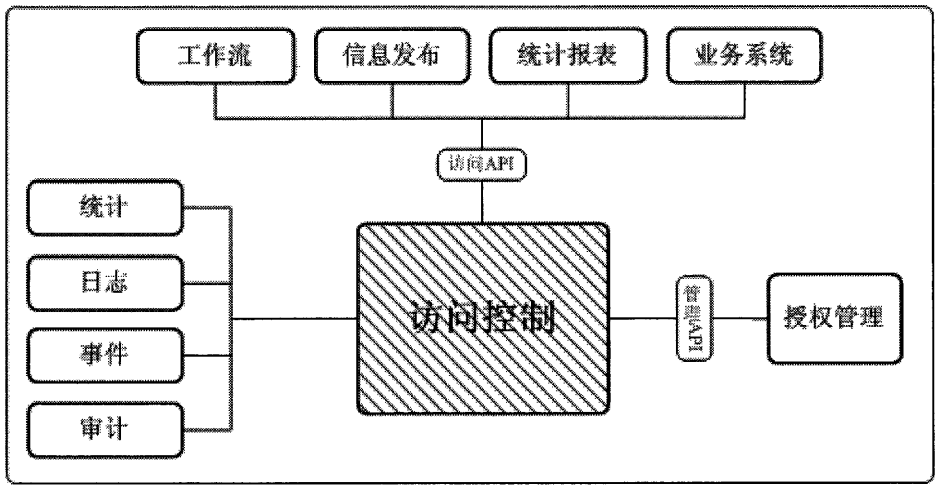

图1　访问控制模型示意图

通过建立统一的访问控制模型，提供统一的权限访问接口和管理接口，提供统计、日志、事件、审计、查询等功能，实现应用系统权限管理的一致性、易管理和易维护。

通过权限访问接口，为各应用系统提供统一的访问策略和权限控制。通过权限管理接口，使各应用系统能够创建自己的访问控制资源并进行权限分配。

3.4　权限管理模型

根据电子政务体系对访问控制的要求，访问控制模型参考Constrained RBAC模型，并在此基础上进行扩展，增加Actor对象，即用户（User）和角色（Role）的集合；增加域（Domain）对象，即授权的作用范围；增加用户（User）和权限（Permission）的关系，即除对角色授权外，单个用户（User）可以直接授权。

基本概念定义：

操作者（Actor）：执行者、参与者。

包含用户（User）和角色（Role）的集合总称，可以是应用系统的代理（agent），或其它任何能够发起请求的对象。可以反向包含自身，即树状结构。接口中引用的 actorUID 泛指用户（User）对象、角色（Role）对象和代理对象（agent）的 UID 值。

用户（User）

发起请求的主体，对应组织机构中得 Person 对象，或者一个应用代理程序（agent）。可以通过授权管理对用户直接进行授权。

角色（Role）

一组具有相同属性或者业务需求的人员集合，是授权的主体，可以是组织模型中的机构、部门、用户组、角色、岗位等。组织机构类型参见第 4 部分《组织身份模型数据规范》。

资源（Resource）：对象（Object）。

资源或对象，被授权对象。可以反向包含自身，即树状结构。

操作（Operation）：权限类型。

是访问控制可以执行的最小功能项，被 Actor 调用或执行。

许可（Permission）：同义词：Privilege。

是一个许可，对在一个或多个 Resource 上执行的 Operation 的许可。

会话（Session）：

每个 Session 是一个用户到多个 Role 的映像，当一个 Actor 启动它所有角色的一个子集的时候，建立了一个 Session。每个 Session 和单个的 Actor 关联，并且 Actor 可以关联到一个或多个 Session。

域（Domain）：

描述作用范围，也叫作用域。通过分配不同的对象（Actor、Resource、Operation），生成授权范围，授权是在域的范围内进行。

3.5 模型实体描述

3.5.1 执行者（Actor）

属性列表	中文名称	数据类型	值域	约束	说明
uid	唯一标识	字符串	ID..100	非空	
name	名称	字符串	C..200		
description	描述	字符串	C..2000		
type	类型	字符串	C..20	非空	执行者的类型，可以是组织模型中的实体对象，也可以是应用程序代理等类型。
icon	图标	字符串	C..100		
createDateTime	创建时间	日期	D19		如2008-10-01 13:01:01
tabIndex	序号	整数	N		
properties	扩展属性	键值对			键值对应的数据结构，如键为"name"，值为"张三"。

3.5.2 资源（Resource）

属性列表	中文名称	数据类型	值域	约束	说明
uid	唯一标识	字符串	ID..100	非空	
name	名称	字符串	C..200		
description	描述	字符串	C..200		
type	类型	字符串	C..20		描述资源类型的字符串。
icon	图标	字符串	C..100		
createDateTime	创建时间	日期时间	D19		如2008-10-01 13:01:01
tabIndex	序号	整数	N		
properties	扩展属性	键值对			键值对应的数据结构，如键为"name"，值为"张三"。

3.5.3 操作类型（Operation）

属性列表	中文名称	数据类型	值域	约束	说明
operationKey	关键字	字符串	ID..100	非空	如add、update等，不能以减号开头。
operationName	名称	字符串	C..200		如增加
operationValue	值	整数	N		如“1”
description	描述	字符串	C..2000		
createDateTime	创建时间	日期时间	D19		例:2008-10-01 13:01:01
tabIndex	序号	整数	N		

3.5.4 域（Domain）

属性列表	中文名称	数据类型	值域	约束	说明
uid	唯一标识	字符串	ID..100	非空	
name	名称	字符串	C..200		
description	描述	字符串	C..2000		
createDateTime	创建时间	日期时间	D19		例:2008-10-01 13:01:01
tabIndex	序号	整数	N		

3.6 访问控制规则

1. 授权方式

正向授权，开始时假定主体没有任何权限，然后根据需要授予权限。

2. 权限继承

权限的继承通过对象的父子关联实现，如果设置为可继承，则执行者子对象自动继承父对象的权限，子资源自动继承父资源的权限。

3. 权限过滤

通过设置相应的权限过滤规则，控制资源的权限继承，过滤当前资源节点从父节点继承获得的访问权限。

4. 再授权

再授权是指权限拥有者将自己拥有的权限再分配给其他用户，这个授权过程称之为再授权过程。再授权中的权限具有包含关系，即只能授予自己拥有的权限。

5. 权限回收

权限回收是指系统回收已经分配给用户的权限。

根据不同的情况，通过权限继承得到的权限，如果父权限被回收，子权限必定被回收；通过再授权得到的权限，根据设置不同规则，可规定父权限被回收，保留或回收子权限。

6. 权限排斥

权限的排斥主要是指当用户拥有权限 A 时，则不能同时再拥有权限 B。通过定义权限排斥规则，通过静态方式或者动态方式计算权限排斥。

7. 负权限

负权限是指操作者不应该拥有的权限。负权限通过权限计算叠加完成，计算时负权限优先。

8. 权限等效

权限等效是指如果设置用户B等效于用户A，则用户B拥有用户A的所有权限。A称为被权限等效对象，B称为权限等效对象。权限等效具有时效性。

4 访问控制接口

接口命名空间：egov.appservic.ac。

访问控制接口分为权限访问接口、管理接口、数据权限接口三类。

4.1 权限访问接口

4.1.1 权限判断

4.1.1.1 判断 Actor 对 Resource 是否有指定操作权限

服务名称	AccessControl.hasPermission	
服务说明	判断 Actor 对象对资源对象是否具有指定的操作权限。	
参数列表	参数名称	参数说明

	actorUID	String 类型，指定执行者的唯一标识，如果 actorUID 为 null，抛出 IllegalArgumentException 异常。
	resouceUID	String 类型，指定资源对象唯一标识，如果 resouceUID 为 null，抛出 IllegalArgumentException 异常。
	operationKey	String 类型，指定操作类型关键字，如 add、update 等，如果 operationKey 为 null，抛出 IllegalArgumentException 异常。
异常处理	AccessControlException	如果无法正常返回结果，则抛出此异常，如权限计算错误等。
	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如通过 actorUID 无法得到相应的 Actor 对象等。
返回值	boolean 类型。如果具有指定操作权限返回 true，否则返回 false。	
备注		

4.1.2 权限查询

4.1.2.1 获得 Actor 对象对 Resource 的操作类型

服务名称	AccessControl.getOperations	
服务说明	获得 Actor 对象对指定资源具备的操作类型。	
参数列表	参数名称	参数说明
	actorUID	String 类型，指定执行者的唯一标识，如果 actorUID 为 null，抛出 IllegalArgumentException 异常。
	resourceUID	String 类型，指定资源对象唯一标识，如果 resouceUID 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如通过 actorUID 无法得到相应的 Actor 对象等。
返回值	String 数组，返回包含符合条件的 operationKey 数组，如果是负权限，在 operationKey 前用一个减号表示。	
备注		

4.1.2.2 获得 Actor 对象能以指定操作类型访问的资源

服务名称	AccessControl.getResources	
服务说明	获得指定 Actor 对象能以指定操作类型访问的资源。	
参数列表	参数名称	参数说明
	actorUID	String 类型，指定执行者的唯一标识，如果 actorUID 为 null，抛出 IllegalArgumentException 异常。
	operationKey	String 类型，指定操作类型关键字，如 add、

		update 等，如果 operationKey 为 null，抛出 IllegalArgumentException 异常。
	rootResourceUID	String 类型，指定查询资源的范围，包括其所有子节点。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如通过 actorUID 无法得到相应的 Actor 对象等。
返回值	String 数组，返回符合条件的 resourceUID 数组。	
备注		

4.1.2.3 获得在资源对象上具有指定操作类型的 Actor 对象

服务名称	AccessControl.getActors	
服务说明	获得能以指定操作类型访问指定资源的 Actor 对象。	
参数列表	参数名称	参数说明
	rootActorUID	String 类型，指定查询 Actor 对象的范围，包括其所有子节点。
	resourceUID	String 类型，指定资源对象唯一标识，如果 resouceUID 为 null，抛出 IllegalArgumentException 异常。
	operationKey	String 类型，指定操作类型关键字，如 add、update 等，如果 operationKey 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如通过 resourceUID 无法得到相应的 Resource 对象等。
返回值	String 数组，返回符合条件的 actorUID 数组。	
备注		

4.1.2.4 获取 Actor 数组对资源数组是否具有指定的操作

服务名称	AccessControl.getPermissions	
服务说明	获得 Actor 数组对 Resource 数组是否具有指定的操作类型。 通过传入 Actor、Resource、Operation 的唯一标识数组，判断每一 Actor 对象对每一 Resource 对象是否具有指定的操作类型，返回 boolean 类型的三维数组。	
参数列表	参数名称	参数说明
	actorUIDs	String 数组，指定 Actor 对象唯一标识数组，不包含其子节点。
	resourceUIDs	String 数组，指定资源对象唯一标识的数组，不包含其子节点。
	operationKeys	String 数组，指定的操作类型数组。
	inherit	boolean 类型，是否包含通过继承、等效获得的权限，如果为 true 则包含，否则只包含直接获得的。

异常处理	IllegalArgumentException	如果 actorUIDs、resourceUIDs、operationKeys 数组为 null，抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常。
返回值	boolean 三维数组，分别对应 actorUIDs、resourceUIDs、operationKeys 是否有操作权限。	
备注		

4.2 管理接口

4.2.1 操作者管理

4.2.1.1 创建操作者

服务名称	ActorManager.createActor	
服务说明	在指定的父节点下创建操作者。	
参数列表	参数名称	参数说明
	type	String 类型，操作者的类型，可以是组织模型中的实体对象，也可以是应用程序代理等类型。
	actorName	String 类型，Actor 对象的名称。
	parentActorUID	String 类型，传入 Acotr 对象父节点唯一标识，如果 parentActorUID 为 null，创建在根节点下。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如通过 parentActorUID 无法得到相应的对象等。
返回值	返回已创建的 Actor 对象，包含新生成的 actorUID 值。	
备注		

4.2.1.2 修改操作者

服务名称	ActorManager.updateActor	
服务说明	更新操作者对象。	
参数列表	参数名称	参数说明
	Actor	Actor 对象，用于更新的操作者对象实例
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如不存在此 Actor 对象等。
返回值	boolean 类型，如果修改成功返回 true，否则返回 false。	
备注		

4.2.1.3 删除操作者

服务名称	ActorManager.deleteActor	
服务说明	删除指定的操作者。	
参数列表	参数名称	参数说明
	actorUID	String 类型，操作者唯一标识。如果 actorUID 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果参数不存在，则抛出此异常。

返回值	boolean 类型，如果删除成功返回 true，否则返回 false。
备注	

4.2.1.4 获得操作者对象

服务名称	ActorManager.getActor	
服务说明	获得指定的操作者对象。	
参数列表	参数名称	参数说明
	actorUID	String 类型，操作者唯一标识。如果 actorUID 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如通过 actorUID 无法得到相应的 Actor 对象等。
返回值	返回由 actorUID 指定的 Actor 对象。	
备注		

4.2.1.5 获得操作者包含的子对象

服务名称	ActorManager.getSubActors	
服务说明	获得指定的操作者所直接包含的子对象，不递归。	
参数列表	参数名称	参数说明
	actorUID	String 类型，操作者唯一标识。如果 actorUID 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如通过 actorUID 无法得到相应的 Actor 对象等。
返回值	返回 Acotr 对象数组。	
备注		

4.2.1.6 获得操作者的父对象

服务名称	ActorManager.getParentActor	
服务说明	获得指定的操作者的父对象。	
参数列表	参数名称	参数说明
	actorUID	String 类型，操作者唯一标识。如果 actorUID 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如通过 actorUID 无法得到相应的 Actor 对象等。
返回值	返回符合条件的 Actor 对象。	
备注		

4.2.1.7 查找操作者

服务名称	ActorManager.searchActor	
服务说明	获得指定查询条件的操作者数组。	
参数列表	参数名称	参数说明

	whereCase	String 类型，查询条件，不包含 where 字符串。查询条件的格式应符合 ANSI SQL 92 中 where 子句对查询条件的要求。
	pageSize	int 类型，每页显示的数目。如果为 0 表示不分页。
	pageNo	int 类型，显示第几页。
异常处理	IllegalArgumentException	如果查询条件不符合要求，则抛出此异常。
	SearchException	如果查询失败，则抛出此异常。
返回值	String 数组，返回符合条件的 actorUID 数组。	
备注		

4.2.2 资源管理

4.2.2.1 创建资源对象

	ResourceManager.createResource	
服务说明	创建资源对象。	
参数列表	参数名称	参数说明
	type	String 类型，描述资源类型的字符串。
	resourceName	String 类型，Resource 对象的名称。
	parentResourceUID	String 类型，Resource 对象父节点的唯一标识，如果 parentResourceUID 为 null，创建根节点。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果参数或对象不存在，则抛出此异常，如通过 parentResourceUID 无法得到相应的资源对象等。
返回值	Resource 对象，返回已创建的 Resource 对象。	
备注		

4.2.2.2 更新资源对象

服务名称	ResourceManager.updateResource	
服务说明	更新资源对象	
参数列表	参数名称	参数说明
	Resource	Resource 对象，用于更新的资源对象。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如不存在此 Resource 对象等。
返回值	boolean 类型，如果修改成功返回 true，否则返回 false。	
备注		

4.2.2.3 删除资源对象

服务名称	ResourceManager.deleteResource	
服务说明	删除指定的资源对象，同时删除子节点	
参数列表	参数名称	参数说明
	resourceUID	String 类型，资源对象唯一标识。如果 resourc

		eUID 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果参数不存在，则抛出此异常，如通过 resourceUID 无法得到相应的 Resource 对象等。
返回值	boolean 类型，如果删除成功返回 true，否则返回 false。	
备注		

4.2.2.4 获得资源对象

服务名称	ResourceManager.getResource	
服务说明	获得指定的资源对象。	
参数列表	参数名称	参数说明
	resourceUID	String 类型，指定资源唯一标识。如果 resourceUID 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如通过 resourceUID 无法得到相应的 Resource 对象等。
返回值	返回资源对象。	
备注		

4.2.2.5 获得资源对象的子对象

服务名称	ResourceManager.getSubResources	
服务说明	获得指定的资源对象直接包含的子对象，不递归。	
参数列表	参数名称	参数说明
	resourceUID	String 类型，指定资源唯一标识。如果 resourceUID 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如通过 resourceUID 无法得到相应的 Resource 对象等。
返回值	返回符合条件的 Resource 对象数组。	
备注		

4.2.2.6 获得资源对象的父对象

服务名称	ResourceManager.getParentResource	
服务说明	获得指定资源对象的父资源对象，如果没有父节点，返回 null。	
参数列表	参数名称	参数说明
	resourceUID	String 类型，指定资源唯一标识。如果 resourceUID 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如通过

		resourceUID 无法得到相应的 Resource 对象等。
返回值	返回符合条件的 Resource 对象。	
备注		

4.2.2.7 查找资源对象

服务名称	ResourceManager.searchResource	
服务说明	获得符合条件的资源对象。	
参数列表	参数名称	参数说明
	whereCase	String 类型，查询条件，不包含 where 字符串。查询条件的格式应符合 ANSI SQL 92 中 where 子句对查询条件的要求。
	pageSize	int 类型，每页显示的数目。如果为 0 表示不分页。
	pageNo	int 类型，显示第几页。
异常处理	IllegalArgumentException	如果参数为空或不符合查询条件，则抛出此异常。
	SearchException	如果查询失败，则抛出此异常。
返回值	String 数组，返回符合条件的 resourceUID 数组。	
备注		

4.2.3 操作类型管理

4.2.3.1 创建操作类型

服务名称	OperationManager.createOperation	
服务说明	创建操作类型。	
参数列表	参数名称	参数说明
	operationKey	String 类型，指定操作类型关键字，如 add、update 等，关键字不能重复。如果 operationKey 为 null，抛出 IllegalArgumentException 异常。
	operationName	String 类型，指定操作类型中文名称。
	parentOperationKey	String 类型，父操作类型的关键字，如 modify 等。如果 parentOperationKey 为 null，则创建根节点。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
返回值	返回已创建的 Operation 对象。	
备注		

4.2.3.2 更新操作类型

服务名称	OperationManager.updateOperation	
服务说明	更新指定的操作类型对象。	
参数列表	参数名称	参数说明
	Operation	Operation 对象，用于更新的操作类型对象实例。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果参数指定的对象不存在，则抛出此异常，如不存在此 Operation 对象等。

返回值	boolean 类型，如果修改成功返回 true，否则返回 false。
备注	

4.2.3.3 删除操作类型

服务名称	OperationManager.deleteOperation	
服务说明	删除指定的操作类型对象。	
参数列表	参数名称	参数说明
	operationKey	String 类型，操作类型的关键字，如 add、update 等。如果 operationKey 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果参数指定的对象不存在，则抛出此异常。
返回值	boolean 类型，如果删除成功返回 true，否则返回 false。	
备注		

4.2.3.4 增加子操作类型

服务名称	OperationManager.addOperation	
服务说明	向父操作类型中增加子操作类型。父操作类型可以包含多个子操作类型，子操作类型也可有多个父操作类型。	
参数列表	参数名称	参数说明
	parentOperationKey	String 类型，父操作类型的关键字，如 modify 等。如果 parentOperationKey 为 null，抛出 IllegalArgumentException 异常。
	subOperationKey	String 类型，子操作类型的关键字，如 add、delete 等。如果 subOperationKey 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果参数指定的对象不存在，则抛出此异常。
返回值	boolean 类型，如果增加成功返回 true，否则返回 false。	
备注		

4.2.3.5 移除子操作类型

服务名称	OperationManager.removeOperation	
服务说明	从父操作类型中移除子操作类型。父操作类型可以包含多个子操作类型，子操作类型也可有多个父操作类型。	
参数列表	参数名称	参数说明
	parentOperationKey	String 类型，父操作类型的关键字，如 modify 等。如果 parentOperationKey 为 null，抛出 IllegalArgumentException 异常。
	subOperationKey	String 类型，子操作类型的关键字，如 add、delete 等。如果 subOperationKey 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。

	NoSuchElementException	如果参数指定的对象不存在，则抛出此异常。
返回值	boolean 类型，如果移除成功返回 true，否则返回 false。	
备注		

4.2.3.6 获得操作类型对象

服务名称	OperationManager.getOperation	
服务说明	获得指定的操作类型对象。	
参数列表	参数名称	参数说明
	operationKey	String 类型，操作类型的关键字，如 add、delete 等。如果 operationKey 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如通过 operationKey 无法得到相应的 Operation 对象等。
返回值	返回符合条件的 Operation 对象。	
备注		

4.2.3.7 获得子操作类型

服务名称	OperationManager.getSubOperations	
服务说明	获得指定操作类型中包含的子操作类型。一个操作类型可能有多个子操作类型。	
参数列表	参数名称	参数说明
	operationKey	String 类型，操作类型的关键字，如 add、delete 等。如果 operationKey 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果参数指定的对象不存在，则抛出此异常，。
返回值	Operation 对象数组，返回符合条件的 Operation 对象数组。	
备注		

4.2.3.8 获得父操作类型

服务名称	OperationManager.getParentOperations	
服务说明	获得指定操作类型的父操作类型。一个子操作类型可能有多个父操作类型。	
参数列表	参数名称	参数说明
	operationKey	String 类型，操作类型的关键字，如 add、delete 等。如果 operationKey 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果参数指定的对象不存在，则抛出此异常。
返回值	Operation 对象数组，返回符合条件的 Operation 对象数组。	
备注		

4.2.3.9 查找操作类型

服务名称	OperationManager.searchOperation	
服务说明	获得符合条件的操作列表。	
参数列表	参数名称	参数说明
	whereCase	String 类型，查询条件，不包含 where 字符串。查询条件的格式应符合 ANSI SQL 92 中 where 子句对查询条件的要求。
	pageSize	int 类型，每页显示的数目。如果为 0 表示不分页。
	pageNo	int 类型，显示第几页。
异常处理	IllegalArgumentException	如果参数为空或不符合查询条件，则抛出此异常。
	SearchException	如果查询失败，则抛出此异常。
返回值	String 数组，返回符合条件的 operationKey 数组。	
备注		

4.2.4 域管理

4.2.4.1 创建域对象

	DomainManager.createDomain	
服务说明	创建域对象。	
参数列表	参数名称	参数说明
	parentDomainUID	String 类型，传入 Domain 对象父节点唯一标识，如果 parentDomainUID 为 null，创建根节点。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果参数指定的对象不存在，则抛出此异常。
返回值	Domain 对象，返回已创建的 Domain 对象。	
备注		

4.2.4.2 修改域对象

	DomainManager.updateDomain	
服务说明	修改指定的域对象。	
参数列表	参数名称	参数说明
	domain	Domain 对象，用于更新的域对象实例。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如不存在此 Domain 对象等。
返回值	boolean 类型，如果修改成功返回 true，否则返回 false。	
备注		

4.2.4.3 删除域对象

	DomainManager.deleteDomain	
服务说明	删除指定的域对象，同时移除被删除域和域内所有对象的关系。	
参数列表	参数名称	参数说明
	domainUID	String 类型，Domain 对象唯一标识。如果 domainUID 为 null，抛出 IllegalArgumentException

		异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果参数不存在，则抛出此异常，如通过domainUID无法得到相应的Domain对象等。
返回值	boolean类型，如果删除成功返回true，否则返回false。	
备注		

4.2.4.4 获得域对象

服务名称	DomainManager.getDomain	
服务说明	获得指定的域对象。	
参数列表	参数名称	参数说明
	domainUID	String类型，Domain对象唯一标识。如果domainUID为null，抛出IllegalArgumentException异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如通过domainUID无法得到相应的Domain对象等。
返回值	返回域对象。	
备注		

4.2.4.5 查找域对象

服务名称	DomainManager.searchDomain	
服务说明	查找符合条件的域对象。	
参数列表	参数名称	参数说明
	whereCase	String 类型，查询条件，不包含where字符串。查询条件的格式应符合ANSI SQL 92中where子句对查询条件的要求。
异常处理	IllegalArgumentException	如果参数为空或不符合查询条件，则抛出此异常。
	SearchException	如果查询失败，则抛出此异常。
返回值	String数组，返回符合条件的domainUID数组。	
备注		

4.2.4.6 向域中增加对象

	DomainManager.addObject	
服务说明	增加指定对象到指定的域对象中。	
参数列表	参数名称	参数说明
	domainUID	String类型，Domain对象唯一标识。如果domainUID为null，抛出IllegalArgumentException异常。
	objcetUID	String类型，增加对象的根节点唯一标识，表明新增对象的范围，递归包含所有子对象。如果objectUID为空，抛出IllegalArgumentException异常。

	classType	String 类型，实体对象的完整类名。可以是 Actor 类、Resource 类、Operation 类、Domain 类。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如通过 objcetUID 无法得到相应的对象等。
返回值	boolean 类型，如果增加成功返回 true，否则返回 false。	
备注		

4.2.4.7 从域中移除对象

	DomainManager.removeObjcet	
服务说明	移除指定域对象中的指定对象。	
参数列表	参数名称	参数说明
	domainUID	String 类型，Domain 对象唯一标识。如果 domainUID 为 null，抛出 IllegalArgumentException 异常。
	objectUID	String 类型，被移除对象的根节点对象唯一标识，表明被移除对象的范围。如果 objectUID 为 null，抛出 IllegalArgumentException 异常。
	classType	String 类型，实体对象的完整类名。可以是 Actor 类、Resource 类、Operation 类、Domain 类。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如通过 objcetUID 无法得到相应的对象等。
返回值	boolean 类型，如果移除成功返回 true，否则返回 false。	
备注		

4.2.4.8 获得域中对象

	DomainManager.getObjects	
服务说明	获得指定的域对象中的指定对象。	
参数列表	参数名称	参数说明
	domainUID	String 类型，Domain 对象唯一标识。如果 domainUID 为 null，抛出 IllegalArgumentException 异常。
	classType	String 类型，实体对象的完整类名。可以是 Actor 类、Resource 类、Operation 类、Domain 类。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如通过 domainUID 无法得到相应的 Domain 对象等。
返回值	String 数组，返回符合条件的 objectUID 数组。	
备注		

4.2.4.9 获得对象所属的域对象

	DomainManager.getDomains

服务说明	获得指定对象所属的域对象。	
参数列表	参数名称	参数说明
	objectUID	String 类型，指定对象唯一标识。如果 objectUID 为 null，抛出 IllegalArgumentException 异常。
	classType	String 类型，实体对象的完整类名。可以是 Actor 类、Resource 类、Operation 类、Domain 类。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如通过 domainUID 无法得到相应的 Domain 对象等。
返回值	Domain 对象数组，返回符合条件的 Domain 对象数组。	
备注		

4.2.5 分配权限

4.2.5.1 直接授权

	AccessGrant.grantPermission	
服务说明	直接为 Actor 对象授权，授予 Actor 对象以指定操作类型访问指定资源的权限。	
参数列表	参数名称	参数说明
	actorUID	String 类型，指定执行者唯一标识。如果 actorUID 为 null，抛出 IllegalArgumentException 异常。
	resourceUID	String 类型，指定资源唯一标识。如果 resourceUID 为 null，抛出 IllegalArgumentException 异常。
	operationKey	String 类型，指定操作类型关键字，比如：add、update 等。如果要授予负权限，在 operationKey 前面加减号表示。如果 operationKey 为空，抛出 IllegalArgumentException 异常。
	isInherit	boolean 类型，是否允许权限继承。
异常处理	AccessManagerException	如果无法正常返回结果，则抛出此异常，如权限分配错误等。
	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如通过 actorUID 无法得到相应的 Actor 对象等。
返回值	boolean 类型，如果授权成功返回 true，否则返回 false。	
备注		

4.2.5.2 批量授权

	AccessGrant.grantPermissions	
服务说明	批量为 Actor 对象授权。	
参数列表	参数名称	参数说明
	actorUIDs	String 数组，指定执行者唯一标识数组，不包含其子节点。

	resourceUIDs	String 数组，指定资源对象唯一标识的数组，不包含其子节点。
	operationKeys	String 数组，指定的操作类型数组。如果要授予负权限，在 operationKey 前面加减号表示。
	isInherit	boolean 类型，是否允许权限继承。
异常处理	AccessManagerException	如果无法正常返回结果，则抛出此异常，如权限分配错误等。
	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。如果 actorUIDs、resourceUIDs、operationKeys 数组为 null，抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常。
返回值	boolean 类型，如果批量授权成功返回 true，否则返回 false。	
备注		

4.2.5.3 权限回收

	AccessGrant.revokePermision	
服务说明	回收 Actor 对象对资源对象的操作权限。如果 cascade 为 true，级联回收 Actor 对象再授权及相关联的权限，否则只回收 Actor 对此资源的权限。	
参数列表	参数名称	参数说明
	actorUID	String 类型，指定操作者唯一标识。如果 actorUID 为 null，抛出 IllegalArgumentException 异常。
	resourceUID	String 类型，指定资源唯一标识。如果 resourceUID 为 null，抛出 IllegalArgumentException 异常。
	operationKey	String 类型，指定操作类型关键字，比如：add、update 等。如果要回收负权限，在 operationKey 前面加减号表示。如果 operationKey 为 null，抛出 IllegalArgumentException 异常。
	cascade	boolean 类型，是否级联回收 Actor 对象再授权及相关联的权限，缺省为 false。
异常处理	AccessManagerException	如果无法正常返回结果，则抛出此异常。
	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常。
返回值	boolean 类型，如果回收权限成功返回 true，否则返回 false。	
备注		

4.2.5.4 新建权限过滤

	AccessGrant.createPermisionFilter	
服务说明	新建对资源对象的权限过滤。	
参数列表	参数名称	参数说明
	resourceUID	String 类型，指定资源唯一标识。如果 resourceUID 为 null，抛出 IllegalArgumentException

		异常。
	operationKey	String 类型，指定操作类型关键字，比如：add、update 等。如果 operationKey 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常。
返回值	boolean 类型，如果新建权限过滤成功返回 true，否则返回 false。	
备注		

4.2.5.5 删除权限过滤

	AccessGrant.deletePermisionFilter	
服务说明	删除对资源对象的权限过滤。	
参数列表	参数名称	参数说明
	resourceUID	String 类型，指定资源唯一标识。如果 resourceUID 为 null，抛出 IllegalArgumentException 异常。
	operationKey	String 类型，指定操作类型关键字，比如：add、update 等。如果 operationKey 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常。
返回值	boolean 类型，如果删除权限过滤成功返回 true，否则返回 false。	
备注		

4.2.5.6 获得权限过滤

	AccessGrant.getPermisionFilters	
服务说明	获取指定资源对象的权限过滤。	
参数列表	参数名称	参数说明
	resourceUID	String 类型，指定资源唯一标识。如果 resourceUID 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常。
返回值	String 数组，返回符合条件的 operationKey 数组。	
备注		

4.2.5.7 新建权限等效

	AccessGrant.createPermisionEquivalent	
服务说明	新建两个 Actor 对象的权限等效关系。将使权限等效 Actor 对象获得被等效 Actor 对象在 rootResourceUID 下的所有权限，用 actorUID 指定权限等效 Actor 对象，用 equivalentedActorUID 指定被等效 Actor 对象，此权限在指定的起止时间内有效。	
参数列表	参数名称	参数说明

	actorUID	String 类型，指定权限等效 Actor 对象。如果 actorUID 为空，抛出 IllegalArgumentException 异常。
	equivalentedActorUID	String 类型，指定被权限等效的 Actor 对象。如果 equivalentedActorUID 为空，抛出 IllegalArgumentException 异常。
	rootResourceUID	String 类型，指定权限等效的资源范围，递归包含子节点。
	startDate	Date 类型，格式：yyyy-mm-dd HH:mm:ss，起始时间，如果 startDate 为空，按当前日期计算。
	endDate	Date 类型，格式：yyyy-mm-dd HH:mm:ss，结束时间，如果 endDate 为空，则永久等效。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常。
返回值	boolean 类型，如果新建权限等效成功返回 true，否则返回 false。	
备注		

4.2.5.8 删除权限等效

	AccessGrant.deletePermisionEquivalent	
服务说明	删除两个 Actor 对象的权限等效关系，使权限等效对象不再拥有被权限等效对象在 rootResourceUID 下的权限。	
参数列表	参数名称	参数说明
	actorUID	String 类型，权限等效 Actor 对象。如果 actorUID 为空，抛出 IllegalArgumentException 异常。
	equivalentedActorUID	String 类型，被权限等效的 Actor 对象，如果 equivalentedActorUID 为空，抛出 IllegalArgumentException 异常。
	rootResourceUID	String 类型，指定权限等效的资源范围，递归包含子节点。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常。
返回值	boolean 类型，如果删除权限等效成功返回 true，否则返回 false。	
备注		

4.2.5.9 获取权限等效的对象

	AccessGrant.getPermisionEquivalent	
服务说明	获取指定 Actor 对象的权限等效对象，指定的 Actor 对象为被权限等效对象。	
参数列表	参数名称	参数说明
	actorUID	String 类型，指定被权限等效 Actor 对象唯一标识。如果 actorUID 为空，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常。

返回值	String 二维数组，第一维 actorUID 是权限等效的对象唯一标识，第二维是设置权限等效资源节点唯一标识。
备注	

4.2.5.10 获取被权限等效的对象

	AccessGrant.getPermisionEquivalented	
服务说明	获取指定 Actor 对象的被权限等效对象，指定的 Actor 对象为权限等效对象。	
参数列表	参数名称	参数说明
	equivalentedActorUID	String 类型，指定权限等效的 Actor 对象。如果 actorUID 为空，抛出 IllegalArgumentExceptio n 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常。
返回值	String 二维数组，第一维 actorUID 是被权限等效的对象唯一标识，第二维是设置权限等效资源节点唯一标识。	
备注		

4.3 数据权限

数据权限根据不同的业务需求，可以划分为行数据权限、数据范围权限、表权限、字段权限。其中行数据权限、数据范围权限可归为行权限，表权限、字段权限可归为列权限。为了对数据资源进行授权和控制，将数据映射为Resource，对数据的操作映射为Operation，整个授权过程与普通的Resource对象相同。

由此根据数据类型的不同，会产生相应的Resource对象：

1. DataRowResource，行数据资源，资源类型名称是dataRowResource，记录行数据的基本信息，由于数据动态产生，只有在数据产生时生成DateRowResource对象。
2. DataScopeResource，数据范围资源，资源类型名称是dataScopeResource，记录符合特定条件的行数据集合，由于包含多条动态数据，DateScopeResource对象只记录产生数据集合的条件，并不包含实体数据。
3. TableResource，表资源，资源类型名称是tableResource，映射数据库表对象。
4. TableColumnResource，字段资源，资源类型名称是tableColumnResource，映射数据库表列字段。

以上四种资源类型的基本属性如下：

4.3.1 DataRowResource

基本属性列表：

	DataRowResource	
属性列表	属性名称	属性说明
	rowUID	String 类型，对应数据记录的唯一标识。
	resourceName	String 类型，资源名称。
	dataCreater	String 类型，数据记录创建者。
	dataCreateDate	Date 类型，数据记录创建时间。
备注		

4.3.2 DataScopeResource

基本属性列表：

	DataScopeResource	
属性列表	属性名称	属性说明
	dataScope	String 类型，数据范围的查找条件，SQL 语句（格式应符合 ANSI SQL 92 的要求）。
	tableName	String 类型，数据表名称。
备注		

4.3.3 TableResource

描述：表数据资源。

基本属性列表：

	TableResource	
属性列表	属性名称	属性说明
	tableName	String 类型，表名称。
备注		

4.3.4 TableColumnResource

描述：字段数据资源。

基本属性列表：

	TableColumnResource	
属性列表	属性名称	属性说明
	tableName	String 类型，表名称。
	tableColumnName	String 类型，列名称。
备注		

4.3.5 获得 Actor 对象能以指定操作访问的行数据资源

服务名称	AccessControl.getDataRowResources	
服务说明	获得指定 Actor 对象能以指定的操作类型访问的行数据资源。	
参数列表	参数名称	参数说明
	actorUID	String 类型，指定操作者唯一标识。如果 actorUID 为 null，抛出 IllegalArgumentException 异常。
	operationKey	String 类型，指定操作类型关键字，如 add、update 等。如果 operationKey 为 null，抛出 IllegalArgumentException 异常。
	rootResourceUID	String 类型，数据资源的查找范围唯一标识，如果 rootResourceUID 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如通过 actorUID 无法得到相应的 Actor 对象等。
返回值	String 数组，返回符合条件的 rowUID 数组。	
备注		

4.3.6 获得 Actor 对象能以指定操作类型访问的数据范围资源

服务名称	AccessControl.getDataScopeResources	
服务说明	获得指定 Actor 对象能以指定操作类型访问的数据范围资源。	
参数列表	参数名称	参数说明
	actorUID	String 类型，指定操作者唯一标识。如果 actorUID 为 null，抛出 IllegalArgumentException 异常。
	operationKey	String 类型，指定操作类型关键字，比如：add、update 等。如果 operationKey 为空，抛出 IllegalArgumentException 异常。
	rootResourceUID	String 类型，数据资源的查找范围唯一标识，如果 rootResourceUID 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如通过 actorUID 无法得到相应的 Actor 对象等。
返回值	String 数组，返回符合条件的 rowUID 数组。	
备注		

4.3.7 获得 Actor 对象能以指定操作类型访问的数据范围资源 SQL

服务名称	AccessControl.getDataScopeResourceSQL	
服务说明	获得指定 Actor 对象能以指定操作类型访问的数据资源范围的 SQL 语句。	
参数列表	参数名称	参数说明
	actorUID	String 类型，指定操作者唯一标识。如果 actorUID 为 null，抛出 IllegalArgumentException 异常。
	operationKey	String 类型，指定操作类型关键字，比如：add、update 等。如果 operationKey 为空，抛出 IllegalArgumentException 异常。
	rootResourceUID	String 类型，数据资源的查找范围唯一标识，如果 rootResourceUID 为 null，抛出 IllegalArgumentException 异常。
异常处理	IllegalArgumentException	如果参数非法或参数类型不正确，则抛出此异常。
	NoSuchElementException	如果对象不存在，则抛出此异常，如通过 actorUID 无法得到相应的 Actor 对象等。
返回值	String 类型，返回符合条件的 SQL 语句。	
备注		

4.4 异常约定

访问控制服务应包含以下异常：

异常名称	异常描述
AccessControlServiceException	访问控制服务的根异常。

SearchException	查询类异常，通过whereCase进行查找会产生此异常。
AccessControlException	权限访问异常，如果权限计算错误等会抛出此异常。
AccessManagerException	管理控制异常。
IllegalArgumentException	非法参数异常，如果传入参数类型不正确则抛出异常。
NoSuchElementException	指定的对象不存在，则抛出此异常。

上述异常类的关系如图2所示：

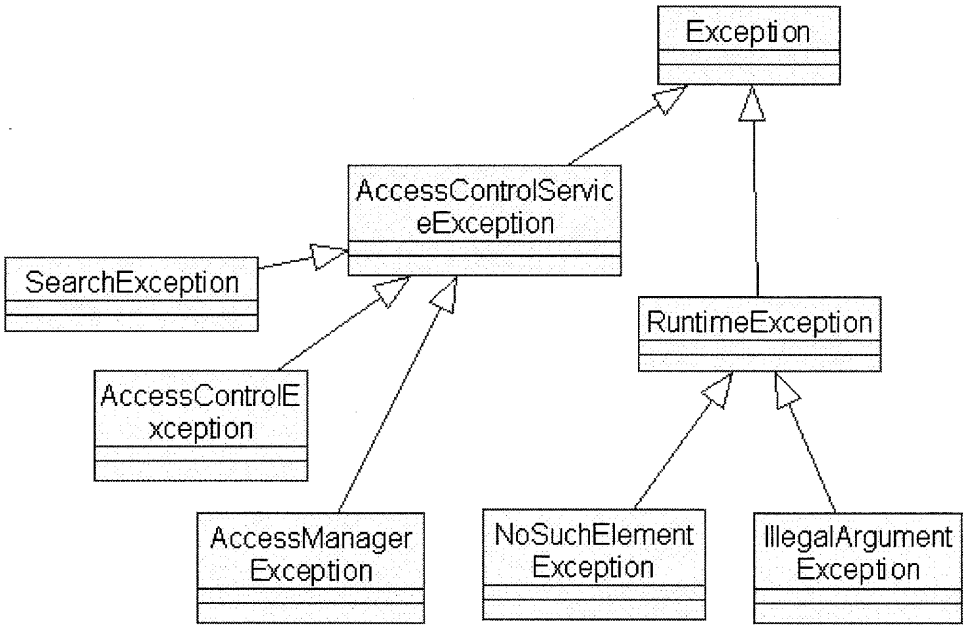

图2　访问控制服务异常关系示意图

5　访问控制要求

5.1　日志

要求能够记录用户访问日志，包括用户登陆、用户操作等；授权日志，包括权限的授予、权限变更等；系统日志，包括访问异常、权限操作异常等。可以根据访问者的权限提供日志的查询、删除功能，日志纪录可以是log文件、数据库、xml等。

5.2　审计

通过对用户访问日志和权限日志进行分析，检查某一时间顺序的用户访问过程和授权过程，对其中出现的资源访问、权限授予、权限变更、权限策略等进行检查，形成审计结果。

5.3　统计

对指定条件下的访问纪录或者权限纪录进行统计，获得统计信息，如获得访问者对指定资源对象的访问次数；访问者的对指定资源的权限变更纪录等。可以通过列表方式或者图表方式进行展示。

参考文献

[1].《信息安全技术》，2005 - 北京:科学出版社
[2].《电子政务总体设计与技术实现》，2003 - 北京：电子工业出版社
[3].《网络与信息安全》，2004年4月
[4].《Proposed NIST Standard for role-based access control》，2001年8月
[5].《Role-Based Access Control》，2003年
[6]. OASIS eXtensible Access Control Markup Language (XACML) TC
[7]. NIST, Role Based Access Control, ANSI INCITS 359-2004