# 权限管理：

1. 信息权限(此块权限是判断用户是否有权限调用相关接口操作该信息)

栏目权限是否作用于信息

* 1. ~~信息内容的投稿权限~~(由于信息并未产生,不存在此处的权限判断,因此投稿权限只存在于栏目中)
  2. 信息内容的修改权限
  3. 信息内容的查看权限
  4. ~~信息内容的删除权限-~~--信息没有这个设置

1. 信息列表查看权限—进了栏目能看到哪些信息列表—栏目设置-信息机构开关
2. 栏目模块的权限(此块权限是判断用户是否有权限调用相关接口操作栏目)
   1. 栏目模块的投稿权限—是否有权限添加该栏目下的信息内容

添加信息—栏目设置是否开放投稿（只对前端有效）

* 1. 栏目模块的修改权限—是否有权限修改该栏目下的信息内容
  2. 栏目模块的查看权限—是否看得到这个栏目信息列表or在信息模块左边菜单是否显示
  3. 栏目模块的删除权限—是否有权限删除该栏目下的信息内容

综上,权限判断主要分2块内容:1.判断用户是否有权限调用接口(权限判断函数) 2.该用户有权限看到哪些东西(权限 sql)

## 权限的配置源：

* 1. 信息内容权限
     1. 信息内容相关的可浏览或可查看或可删除
     2. 信息的白名单
     3. 信息的黑名单
  2. 信息列表权限
     1. 栏目中设置的信息机构开关
     2. 信息列表的可查看权限
  3. 栏目的权限
     1. 栏目的部门和角色
     2. 栏目的白名单
     3. 栏目的黑名单

我的信息：

1. 我的id和我的机构id
2. 根据两个id从机构人员表中找出我的部门以及部门角色的集合

## 权限判断函数—此函数好像用不到缓存数据

将我的权限(我的部门以及部门角色的集合)和对应的权限集合(例如:栏目可浏览部门、角色用户组+栏目可浏览白名单+栏目可浏览黑名单 或者 栏目可修改部门、角色用户组+栏目可修改白名单+栏目可修改黑名单等)作对比,如果我的id 出现在黑名单中,则没权限,如果我的 id出现在白名单中,或 我的权限出现在用户组中,则有权限(写一个函数,返回布尔值, true 则有权限, false 则无权限)

## 列表的浏览权限（权限 sql）

首先把每个人的部门,部门角色缓存下来(指的是我的所有部门和所有部门角色)

获取我的所有部门和所有部门角色见最后的方法

随后可以用来做权限判断

将缓存的部门集合或部门角色集合拿出,将其中的逗号替换为竖线,形成正则表达式

以可浏览部门来举例:

可浏览部门 REGEXP (部门1|部门2|部门3)

1. ~~浏览部门：（栏目浏览部门pids+信息浏览部门pids）包含 我的部门~~

~~参照：~~[~~http://blog.csdn.net/hechurui/article/details/49278493~~](http://blog.csdn.net/hechurui/article/details/49278493)~~。~~

~~如果我的部门有多个，就要把这个语句分解成多个，用或者关系（OR）合并~~

1. ~~浏览部门角色：部门角色包含多个部门角色，将其中一个分解成浏览部门和浏览角色。我包含一个部门角色为例：把我的部门角色分解成我的部门和我的角色，~~

~~（浏览部门pids 包含 我的部门and浏览角色pids 包含 我的角色）~~

~~其他依次类推，用or连接起来~~

1. ~~浏览白名单~~

~~白名单 包含 我的id~~

1. ~~浏览黑名单~~

~~黑名单 不包含 我的id~~

1. ~~信息机构开关(1仅自己可见 2子部门可见 3父部门可见 0全部可见 默认0)~~

~~我的权限中的部分符合信息机构开关中的设置~~

~~综上，最后将所有的条件用or连接，生成列表浏览权限的sql~~

~~步骤——~~

~~1.通过人员id，获取部门角色，分割出部门id和角色id，把部门id拿去机构表里查出pids，将每个pid和角色id组合（这句话好像有问题），得到部门角色权限组~~

~~2.pids 和部门id组成部门权限组~~

~~3.peopleid用于黑白名单查询~~

~~4.遍历组合where语句: (seegroupid like 部门角色权限1 or seegroupid like部门角色权限2 or ..or seegroupid like 部门权限1+"," or seegroupid like 部门权限2+",") or seewhitelist like peopleid and seeblacklist not like peopleid~~

~~注：因为seegroupid的格式是 部门id\_角色id,部门id\_角色id,部门id,~~

~~所以如果要搜索某个部门权限时，需要用【部门权限+","】这种方式，避免和【部门id\_角色id】冲突~~

下面的是老文档内容

1. ~~栏目的投稿权限~~
2. ~~从栏目中取出投稿权限，~~

~~包含四个部分：部门（可能有多个，多个用逗号隔开）、部门角色（可能有多个，多个用逗号隔开）、白名单、黑名单~~

1. ~~根据我的机构id和员工id，从机构员工表中取出员工的我的部门（可能有多个，多个用逗号隔开）和我的部门角色（可能有多个，多个用逗号隔开）。~~
2. ~~根据我的部门判断是否有投稿权限，记为权利A：~~

~~（栏目浏览部门pids+信息浏览部门pids）包含 我的部门~~

~~如果我的部门有多个，就要把这个语句分解成多个，用或者关系（OR）合并~~

1. ~~根据我的部门角色判断是否有投稿权限，记为权利B：~~

~~部门角色包含多个部门角色，将其中一个分解成浏览部门和浏览角色。我包含一个部门角色为例：把我的部门角色分解成我的部门和我的角色，~~

~~（浏览部门pids 包含 我的部门and浏览角色pids 包含 我的角色）~~

~~其他依次类推，用or连接起来~~

1. ~~根据我的id从白名单中判断是否有权限，记为权利C：~~

~~白名单 包含 我的id~~

1. ~~根据我的id从黑名单中判断被剔除，记为权利D：~~

~~黑名单 包含 我的id~~

~~最后的权利计算方式是：!D and (B or C or D),可以通过程序或sql语句来判断权限。如果是通过sql语句，就是把权利的sql语句并入整个条件的where部分。在三栏目的列表权限中，没有选择，只能用sql语句。  
栏目的投稿权限缓存到5、zjxx\_classpower（栏目权限表）中的seewhere字段~~

## 刷新人员菜单权限：参数userid、orgid(机构id)

1. 根据userid、orgid(机构id)查询机构人员表，获取人员机构信息，获取其中所属部门的 orgids，角色表ID集合rids，人员私有的功能权限personnelmenuids。
2. 对orgids 拆分、去重，得到peopleoorgids（人员所属机构、部门id合集）
3. 对rids 拆分（机构id|角色id,部门id|角色id） ，for循环获取每一个rids的子集（部门|角色），在根据子集的部门id和角色id分别查询pids （分别查询机构表和角色表）组成orgpids和rolepids；根据获取的orgpids（部门）和rolepids(角色)，组成sql(select menuids from zjxx\_adminrorg where orgid in ("+orgpids+") and rid in ("+rolepids+")")获取rolemenuids；
4. 获取peopleorgids中所有机构部门的公共菜单 orgmenuids，select publicadminmenuids from zjxx\_orgnization\_functioninfo where id in (peopleorgids);得到 orgmenuids；
5. 对personnelmenuids 、orgmenuids和rolemenuids组合去重

## 刷新人员权限：参数userid、orgid(机构id) 缓存人员权限信息

根据userid、orgid(机构id)查询机构人员表，获取人员机构信息，获取其中所属部门的 orgids，角色表ID集合rids。

**获取人员所属部门集合orgidlist的sql语句：**

SELECT

left(GROUP\_CONCAT(zjxx\_orgnization.pids SEPARATOR ''), length(GROUP\_CONCAT(zjxx\_orgnization.pids SEPARATOR ''))-1) AS orgidlist

FROM

zjxx\_orgnization

WHERE

(

SELECT

locate(

id,

(

SELECT

orgids

FROM

zjxx\_frontorg

WHERE

zjxx\_frontorg.orgid =

“orgid”

AND zjxx\_frontorg.peid =

“Peid”

)

)

)

关键sql：GROUP\_CONCAT—多行汇总成一列，locate-B包含A

问题：得到的orgidlist并没有去重，mysql没有字符串去重函数，需要自定义函数去重。

**获取人员所属部门角色集合逻辑：**

A|B,C|D 拆分A|B，在拆分A,B。分别获取A的pids和B的pids，交叉组合。循环这个方法，获取**所属部门角色集合**