问题：为什么在struts2的拦截器中都要使用roleID，mid，pid去查询一遍数据库，而为什么不从Session中获取mid的值和注解上定义的mid的值进行比较呢？

回答：此时不安全，如果盗用账户，登录系统（一定有Session），即可以操作每一个执行的方法。但是由于挂失后，即使将数据库中的账户、权限更改了，存放的数据发生变化，但是账户已经被盗，黑客的session中已经具有此权限。来不及了。所以 还是操作每一个功能之前先查询权限，这样查询才能保证数据安全。

系统权限控制，在项目上线的时候添加

项目经理要求：**在每个方法上添加注解，并指定该方法能访问的功能权限**

例如：ElecSystemDDLAction类的save方法，应该添加

@Limit(mid="ec" pid="ea")











