中山大学信息科学与技术学院　王雯琴　丘海明

借用权限的实现与考虑

为满足不同情况下，对同一对象有不同访问权限的需求，本文探讨AS/400计算机系统提供的一种临时授权方法——借用权限的实现、应用、及其使用考虑。

在AS/400系统上，用户访问某一对象或完成某一任务的能力是受其操作系统OS/400控制的，OS/400控制是基于用户对对象或任务的权限(即访问对象或完成任务的能力)，它使用两类权限:特殊权限（Special Authority）和特定权限(Specific Authority)，其中特殊权限与用户描述相关，控制系统操作拥有系统范围内的作用域，完成一定任务不需要附加对象权限;特定权限与对象相关，控制用户如何访问对象(在用户特殊权限被允许完成任务的情况下)。一旦给用户颁发了某种权限，用户将永久性地拥有此权限，除非用命令撤消所授予的权限。

借用权限的实现及应用

有时对某个对象或应用，根据具体情况在不同环境下用户需要不同权限，例如，当使用应用程序提供的功能时，允许用户改变文件中的记录；而当使用决策工具（例如SQL）时，仅允许用户查看其内容，不允许改变记录。要解决这种问题可授予用户对文件有*USE权限，对文件维护程序使用借用权限，允许用户改变文件中的记录。当对象使用程序拥有者的权限时称为借用权限(Adopted Authority)。借用权限给用户临时的使用程序中所需的对象，它借用程序拥有者的权限给程序的使用者，类型为*PGM、*SRVPGM、*SQLPKG的对象可以使用借用权限功能。

1. 借用权限的实现

确保程序带USRPRF（*OWNER）属性。在程序创建时，命令CRTXXXPGM应使用USRPRF(*OWNER)参数，若程序已创建好可用CHGPGM或CHGSRVPGM命令保证其属性为USRPRF（*OWNER)。这样凡是对程序有执行权限的用户，在程序运行期间可借用程序拥有者的权限作为自己的附加权限。

2. 借用权限应用

假设USER1对文件FILE1有*USE权限，仅可查看文件数据，USER2对文件FILE1有*CHANGE权限，可对文件数据进行任何检索或更新操作，若USER2创建程序PGM1来维护文件FILE1，且程序带USRPRF(*OWNER)属性，授予USER1对程序有*USE 权限(包括*OBJOPR和*EXECUTE)，那么USER1在程序执行时使用程序逻辑控制存取(例如，只允许对文件进行某种

类型的更新）的方法更新文件，这样USER1借用了程序拥有者USER2对文件FILE1的*CHANGE权限。

借用权限应用考虑

1. 借用权限是借用程序拥有者的特权和对对象的特定权限。程序拥有者仅可借用对象拥有者或对象的私有权限，不能借用对象的*PUBLIC权限。如果程序拥有者的用户描述是一个组文件的成员，那么这个组的权限不能被借用。

2. 只要使用借用权限的程序仍然在程序堆栈中，借用权限就活动。例如，程序PGMA用CALL命令调用程序PGMB，程序堆栈如下：

在CAII 命令之前的调用堆栈	在CAII 命令之后的调用堆栈
QCMD	PGMA
QCMD	PGMA
	PGMB

因为在程序PGMB被调用之后，程序PGMA仍然在调用堆栈中，程序PGMB可使用PGMA的借用权限。程序的USRADPAUT属性决定系统是否使用堆栈中早期程序的借用权限，将USRADPAUT设为*NO时，就可防止程序从调用它的程序中继承任何借用的权限。看下面的例子：

调用堆栈　　程序执行期间的权限

PGM1

Owner:APP_OWNER　　User plus APP_OWNER

User Profile:*OWNER

PGM2

Owner:QSECOFR　　User plus APP_OWNER

User Profile:*OWNER　　plus QSECOFR

PGM3

Owner:QPGMR　　User plus APP_OWNER

User Profile:*OWNER

plus QSECOFR

PGM4

Owner:APP_OWNER

User plus APP_OWNER

User Profile:*OWNER

Use Adopted AUT:*NO

当程序创建时，缺省带USRADPAUT（*YES）属性，CHGPGM或CHGSRVPGM命令可将USRADPAUT参数置为*NO 。如果程序PGMA使用TFRCTL命令调用程序PGMB，程序堆栈如下：

在TFRCTL 命令之前的调用堆栈	在TFRCTL命令之后的调用堆栈
QCMD	QCMD
PGMA	PGMB

程序PGMB不能使用PGMA 的借用权限，因为PGMA不再在程序堆栈中。

3. 当用户、用户所属组或*PUBLIC对某个对象请求操作的权限不够时，系统才检查借用权限。系统可以使用用户调用的原始程序的借用权限。为了提供好的性能和减少私有权限搜索次数，检查借用权限的过程先查看程序拥有者是否有*ALLOBJ 特权或是被检查对象的拥有者，这个过程重复对堆栈中每个有借用权限的程序进行检查。如果没找到足够的权限，系统再查看程序拥有者是否对被检查对象有私有权限，这个过程重复对堆栈中每个有借用权限的程序进行检查。

4. 提交作业请求不能借用提交作业的程序的权限。因为当一个新的作业开始时，对这个作业新的程序堆栈建立，直到第一个程序被加到程序堆栈中借用权限才生效，借用权限不能获得访问任何在作业开始路由之前已经加到作业结构中的对象，例如，*OUTQ、 *JOBD等。

5. 如果程序使用CRTXXXPGM命令，带参数REPLACE（*YES）创建，那么程序的新的拷贝与被代替程序有相同的USRPRF、USRADPAUT 和AUT值，在CRTXXXPGM命令中指定的USRPRF和AUT值被忽略。

6. 仅当用户拥有程序或有*ALLOBJ 和*SECADM特权时，才能改变参数USRPRF的值。只有有*ALLOBJ和*SECADM 特权的用户才能转换一个有借用权限的对象的拥有者和完成恢复，除此之外任何人恢复一个有借用权限的程序，这个程序的拥有者、私有权限和*PUBLIC权限均被撤消。

7. 如果有借用权限的程序运行中断，借用权限的使用停止，这些功能不能使用借用权限：

① System Requst

② Attention key 包括TFRGRPJOB

③中断消息处理程序 ④ Debug 功能。

8. 查看借用权限信息的三个命令：DSPPGM 和

DSPSR VPGM 可显示程序是否有借用权限和能否使用堆栈中前面程序的借用权限，DSPPGMADP 可显示借用用户描述的特权和私有权限的对象。

9. 与借用权限相关的系统值

（1）系统值 QALWOBJRST 决定安权性敏感的对象是否允许恢复到系统上，它的可能值如下表:

QALWOBJRST 的值	功能描述
※ ALL	任何对象可以恢复到系统上，只要用户有适当的权限
※ NONE	安全性敏感的对象，例如，系统态程序或有借用权限的程序不允许恢复到系统上
※ ALWSYS	系统态程序允许恢复
※ ALWPGMADP	有借用权限的程序允许恢复

该系统值提供了一种保护系统方法，以防装入程序引起问题。对正常操作应考虑将其值设为 *NONE，在完成这样一些活动，例如，安装特许程序、应用 PTFs 及恢复系统时应保证该值为 *ALL，如果要定期恢复程序到系统上，需将此值设为 *ALWPGMADP，否则有借用权限的程序不能恢复到系统上。

（2）系统值 QUSEADPAUT 决定哪些用户可创建带 USRADPAUT(*YES）属性的程序，可能的值如下表:

QUSEADPAUT 的值	功能描述
权限表名称	如果用户对权限表有权限，可创建带 USRAD PAUT（*YES）属性的程序或服务程序，否则所创建程序带 USRADPAUT(*NO)属性
※ NONE	所有用户可创建、改变和更新 USRADPAUT（*YES）属性的程序或服务程序，如果用户对程序或服务程序有必要的权限

建议对生产机，建立一个权限表带有 *PUBLIC（*EXCLUDE）属性，然后指定权限表作为该系统值的值。防止权限表之外的用户建立带有借用权限属性的程序。■

参考文献

1 IBM,Security Reference ,1997.