Access Control List & umask

小林 稔幸

2001 年 6 月 13 日

1 Access Control List(アクセス制御リスト)

UNIX 標準のファイルシステムの場合、アクセス権を設定する対象は「ユーザ・グループ・その他」の 3 種類のみとなっています。

仮に koba というユーザが toshi, toshiyuki という 2 つのユーザにファイルのアクセス権を与えたい場合を想定します。従来の UNIX ファイルパーミッション機能の場合、システム管理者に依頼を行って koba, toshiyuki, kobayashi の 3 ユーザのみが所属するグループを作成する必要があります。その後アクセス権を与えるファイルのグループを新しく作成したグループに変更してパーミッションを設定する必要があります。

Access Control List(以下 ACL) を用いると、通常の UNIX ファイルモードに加えて特定のユーザのパーミッションを設定することができます。

現在、 AIX 及び HP-UX で ACL を用いることができます。ここでは、 AIX Access Control List について説明します。

1.1 AIX Access Control List

AIX ACL には以下のフィールドがあります。

```
attributes:
base permissions
 owner: rw-
 group: rw-
 others: r--
extended permissions
 enabled
 specify r-- u:toshi,toshiyuki
 deny -w- u:ushiwakamaru
 permit rw- g:kobayashi
```

1 行目の attributes では、ファイル・ディレクトリの属性を指定します。指定できる属性は SETUID, SETGID, SVTX の 3 つです。カンマで区切って複数指定することもできます。

2 行目から 4 行目の base permissions では、ファイル・ディレクトリの基本パーミッションを設定します。この部分の設定は UNIX 標準のファイルモードと一致している必要があります。

5 行目以降の extended permissions では、拡張パーミッションを指定します。ここで個別のユーザやグループに対してアクセス権を設定できます。6 行目でこの機能を使用する (enabled) か使用しない (disabled) かを設定します。それ以降の行では、次のような形式で設定を記述します。

```
operation access-types user-and-group-info
```

operation で指定できるのは、 permit(許可), deny(不許可), specify(設定) の 3 つです。これらはそれぞれ、 chmod の +, -, = に相当するものです。次にユーザやグループに対して設定するアクセス権を記述し、最後にそのユーザ名・グループ名を指定します。 u: ではじまるステータスはユーザ名、 g: ではじまるステータスはグループ名です。

ただし、同じユーザに対して permit 及び deny の両方でアクセス権の設定が行なわれていた場合、 ACL は安全性を重視して deny で指定されている内容を重視します。

2 umask(user file-creation mode mask)

umask は、 UNIX 系 OS 上で、新しく作成するファイル・ディレクトリのパーミッションを決定する際に用いられる 8 進数の値です。 umask は新しくファイルを作成する際のデフォルトのパーミッションを設定するための数字です。多くの UNIX では、新しいファイルを作成すると最初のパーミッションが 644 もしくは 666 になっており、新しいプログラムを作成した際は 755 もしくは 777 になっています。このモードはカーネル内部で open システムコールで指定したモードを umask の値でマスクしたものです。例えば、システムコールの指定したモードが 666 で umask が 022 の場合、デフォルトで使用されるパーミッションモードは 644 となります。

0666	システムコールのパーミッションモード
(0022)	umask
0600	デフォルトで使用されるパーミッションモード

umask の値はシステムによって異なりますが、.cshrc や.profile, /etc/profile などで設定することができます。