



パーミッション ACLの基礎知識

セミナー資料制作:

株式会社プロフェッショナル・ネットワークス
プロネット教育研究所
長川 維斗子(ながかわ いとこ)
<http://www.pronets.co.jp/>



本日の講師:

株式会社オープンソース総合研究所
テクニカルトレーニングセンター
三島 匡史(みしま ただし)
<http://www.osri.co.jp/>



1



ACLが101新試験で追加される

■101新試験出題範囲

(日本語版配信予定時期 2007年初旬)

<http://www.lpi.or.jp/exam/200607/101ObjectiveJ.html>

「1.104.5 ファイルへのアクセス制御のために
パーミッションを使用する」の

「主要な知識範囲」において、

「ACLに関する基礎的な知識」が追加される。



2





ACLとは

ACL(Access Control Lists)

Linuxカーネル2.6で組み込まれている
Linuxカーネル2.4向けのパッチもある

POSIX(Portable Operating System Interface)規格

<http://wt.xpilot.org/publications/posix.1e/>



ACLの利点

従来のファイルパーミッション概念を拡張

《従来》ファイルの所有者1名、所有グループ1グループ、
その他に対してrwxのパーミッションを割り当てる

+

《ACL》上記以外の複数のユーザや複数のグループに対しても
パーミッションを割り当てることができる

たとえば・・・

会社の来年度採用内定者名簿ファイルに対して、人事部全員と、各部門の部長以上には読み書きを許可、各部門の課長以上には読み込みのみ許可、その他の社員には読み込めないように設定する。



ACL利用時の問題点

アプリケーションがACLをサポートしている必要がある

基本的なコマンド(cp,mv,ls等)や
SambaはACLをサポート

tarコマンドではACLはバックアップできない
(starコマンドでACLをバックアップできる)



ACLとファイルシステム

ACLをサポートするファイルシステム

ReiserFS、Ext2、Ext3、JFS、XFS

使用上の留意点

ReiserFS、Ext2、Ext3・・・管理者側で設定が必要

/etc/fstabにaclオプションを追加し、リマウントする。

例) /etc/fstabの記述

```
/dev/hda3 /share ext3 defaults,acl 1 2
```

リマウントする

```
mount -o remount /dev/hda3
```

JFS、XFS・・・・・・・・・・管理者側で設定は不要

/etc/fstabにaclオプションは無いが、ACLがサポートされる。



ACLのエントリタイプ

タイプ	書式
所有者	user::rwx
名前付きユーザ	user:ユーザ名:rwx
所有者グループ	group::rwx
名前付きグループ	group:グループ名:rwx
マスク	mask::rwx
その他	other::rwx

青字 … 「最小ACL」(従来のパーミッションと対応するエントリタイプ)
 赤字 … 「拡張ACL」(ACLで拡張されたエントリタイプ)
 「名前付きユーザ」と「名前付きグループ」は任意の個数追加できる



ACLの設定例

所有者rootにrwx、所有者グループrootにr-x、その他に許可無しのパーミッションを割り当てたファイルaclfileがある。このaclfileに、拡張ACLとして、名前付きユーザtarouにrwx、名前付きグループsalesにrwxを追加する例を考えよう。

タイプ	書式
所有者	user::rwx
名前付きユーザ	user:tarou:rwx
所有者グループ	group::r-x
名前付きグループ	group:sales:rwx
マスク	mask::rwx
その他	other::---



ACL関連コマンド

getfacl ファイル・ディレクトリのACLを表示
getfacl aclfile

参考

ls -l の実行例

```
-rwxrwx---+ 1 root root 0 Jan 26 14:32 aclfile
```

拡張ACLが設定されているとパーミッションの右横に+マークが表示される



ACL関連コマンド

setfacl ファイル・ディレクトリのACLを設定
アクセスACLの追加・変更例(1)

```
setfacl -m user:taro:rwx,group:sales:rwx aclfile
```

maskは、指定しないと自動的に名前付きユーザのパーミッションに対応する値rwxが生成され、付加される

アクセスACLの追加・変更例(2)

```
setfacl -m mask::r-x aclfile
```

mask値r-xによってwがマスクされ、例(1)のtaroとsalesの実際に有効なパーミッションはr-xとなる
(「getfacl aclfile」で「#effective:r-x」と表示されるのが実際に有効なパーミッション)



ACL関連コマンド

setfacl 続き

デフォルトACLの追加・変更例

```
setfacl -d -m user:taro:r-x acldir
```

デフォルトACLはディレクトリにしか設定できない

デフォルトACLを設定することにより、そのディレクトリ下にディレクトリやファイルを作成する際、ACLを継承する

ACLの部分的な削除例

```
setfacl -x user:taro: aclfile
```

すべての拡張ACLの削除(最小ACLは保持)例

```
setfacl -b aclfile
```



ACL学習のヒント

manコマンドで確認してみよう

```
getfacl setfacl acl
```

(本セミナーで取り上げなかったオプションもある。)

余裕があれば試してみよう

```
chmod
```

(本セミナーでは、時間の都合で説明を割愛する。

ただし、拡張ACLが設定されているファイルにchmodを実行すると影響がある。興味がある方は実験してみてください。)

ACLの詳細情報

<http://acl.bestbits.at/>