Windowsユーザのための Sambaの使い方

ややこしや、ややこしや ---- SambaでACLを使うとき

日本 samba ユーザ会

代表幹事　太田俊哉

staff@samba.gr.jp
http://www.samba.gr.jp/

日本 samba ユーザ会

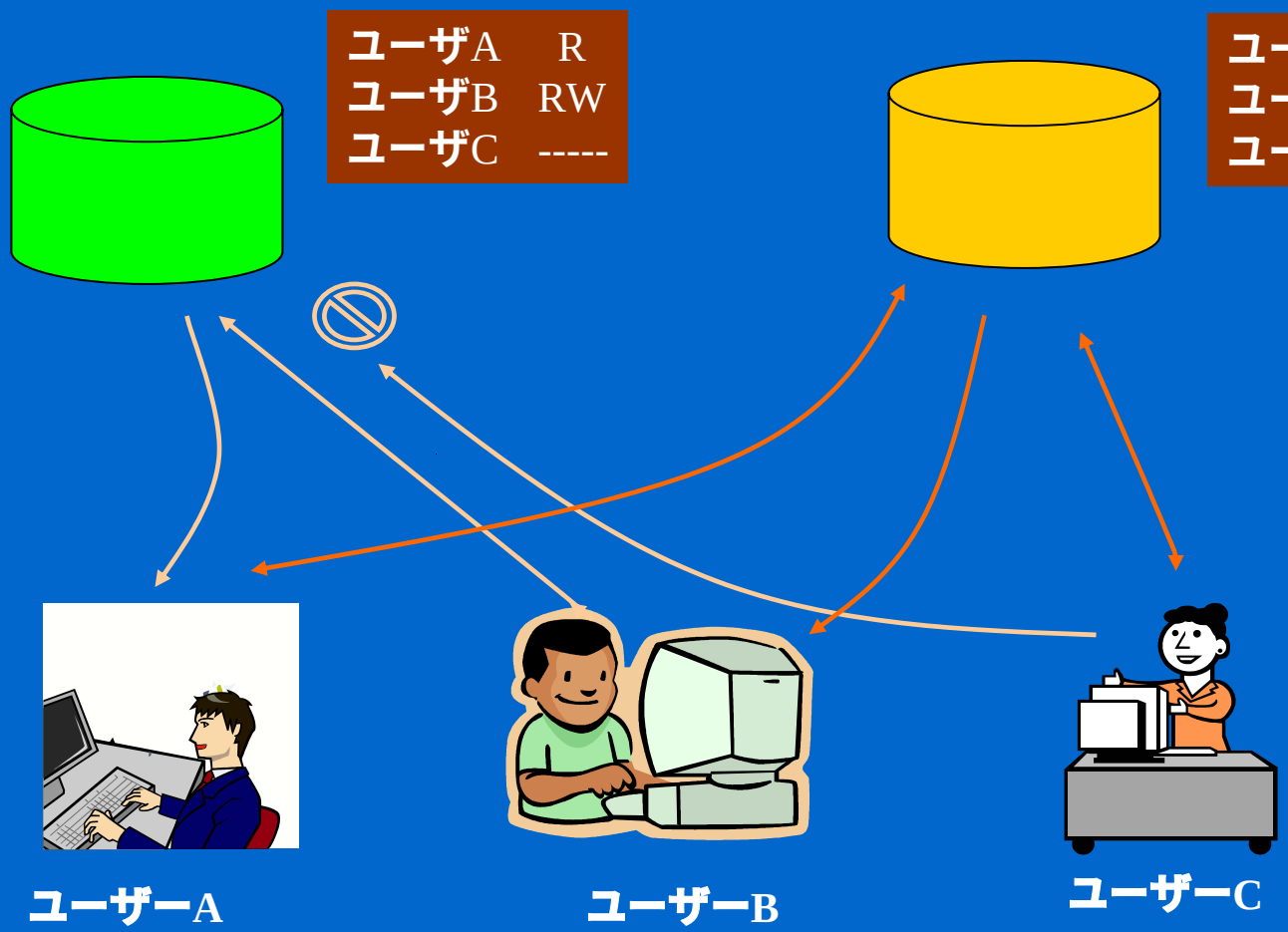
今日のお話

- WindowsとUNIX（Linux）では、アクセス制御に大きな違いがある
- Sambaを使う場合、両方のアクセス制御について理解しておく必要がある
- SambaをWindows互換と思うと、思いもよらぬ所ではまる

ACLとは(1)

- ACL (Access Control List)
  - IEEEで定義。IEEE1003.6→IEEE1003.1eとIEEE1003.2cに
  - その後、2つとも廃止になり、IEEE1003.1とIEEE1003.2を参照するようになっている。
  - http://ieeexplore.ieee.org/Xplore/DynWel.jsp で状況が分かる
- 個々のユーザがアクセス可能な権限のリスト。個別ユーザごとに細かく制御するときに使う。

ACLとは(2)

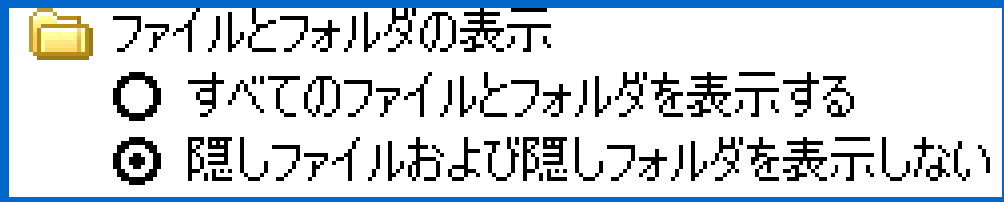


おさらい：UNIXの基本アクセス制御

- ユーザ（所有者）、グループ、その他（ugo）
  - R(ead),w(rite)、x(eXecute)で制御
- 複数のグループに所属することも可能
- setuid/setgid
- stickyビット
- ディレクトリに対しては意味が変わる
- 固有の拡張属性もある(FreeBSD)
  - man 2 chflags

おさらい：DOSの基本アクセス制御

- RO、System、Hidden、Archive
- アプリケーションが使わないと意味がない



- FAT/VFAT/NTFSで利用可能
- ディレクトリに対するアクセス権は少し違う
- Using Sambaの8章
  - File Permissions and Attributes on MS-DOS and Unix

おさらい：NTの基本アクセス制御

- ACLを採用
- かなり複雑な設定が可能
  - フルコントロール/変更/読み取りと実行/読み取り/書き込み/特殊なアクセス許可　が基本
- 許可と拒否
  - 既定値：拒否（暗黙の拒否）
  - ACL設定で許可
- 所有権
- 継承

UNIXのACL

- POSIXで規定
- いくつかのOSで実装
  - Solaris,HP-UX,FreeBSD(5.x),Linux
- 基本はあくまでも昔ながらのアクセス制御
- それを各ユーザ単位で設定できるようにした
- setfacl/getfaclコマンド

FreeBSDの場合

- 5系列で利用可能
- /etc/fstabにオプション acls が必要
  - 設定しないと動かない

Linuxの場合

- 2.4系列(一部)、2.6系列で利用可能
  - Kernel がACLを使えるようにコンパイルされていることが必要
  - ディストリビューションによって異なるので確認が必要
- /etc/fstabにオプション acl が必要
  - 設定しないと動かない
  - acls ではない
- ext3/xfs/jfsで利用可能

設定例

- [tmp]# setfacl -m g:group2:rw acltest
- [tmp]# getfacl acltest
- # file: acltest
- # owner: root
- # group: root
- user::rw-
- user:lduser1:r--
- user:lduser2:rw-
- group::r--
- group:group2:rw-
- mask::rw-
- other::r--

Sambaを使うときのACLの処理(1)

- Sambaを使う場合、Windowsのアクセス権とUNIXのアクセス権の調停が必要
- DOSのアクセス権とUNIXのアクセス権のマッピングは比較的容易
- NTのACLのマッピングは、UNIX上にACL機能があったとしても
  完全互換にはならない
- sambaを使うときの鬼門の一つ

Sambaを使うときのACLの処理(2)

- nt acl support = yes
  - これがないと動かない
  - share毎に設定可能
- マッピングのルールを憶える
- DOSのアクセス権との関係を憶える
- 問題となる現象を押さえる

DOSのアクセス権の処理(1)

- R,S,H,AをUNIXのアクセス権に割り振る
- Windowsから見た場合、ほとんど違和感がない
  - DOSのR
    - UNIXのRとW
  - DOSのS,H,A
    - UNIXのugoのX
    - Map [archive|system|hidden]
    - u rwX g rwX o rwX

DOSのアクセス権の処理(2)

- ログインユーザ以外の属性
  - create mask,force create mask
- ディレクトリの属性
  - これはできない(制限事項)
- ファイルの削除
  - DOS(Windows)では、Rが付いていると削除不可
  - UNIXでは、ディレクトリにwがない場合に削除不可

実際に削除してみる(1)

- DドライブがVFAT、ZドライブがSamba
  - D:¥>attrib rotest.txt
  - A　　R　　D:¥rotest.txt

  属性が付いていることを確認

  - D:¥>del rotest.txt
  - D:¥rotest.txt
  - アクセスが拒否されました。

  消去できない

  - D:¥>z:
  - Z:¥test>attrib rotest.txt
  - A　　R　　Z:¥test¥rotest.txt

  Samba上で同じことをすると

  - Z:¥test>del rotest.txt

  削除できる

  - Z:¥test>

実際に削除してみる(2)

- wを落して削除してみました

```
 Z:¥test のディレクトリ

2005/03/21  16:59    <DIR>          .
2005/03/21  16:41    <DIR>          ..
2005/03/21  16:45                 8 rotest.txt
               1 個のファイル                 8 バイト
               2 個のディレクトリ    1,552,875,520 バイトの空き領域

Z:¥test>del rotest.txt

Z:¥test>dir

 Z:¥test のディレクトリ

2005/03/21  16:59    <DIR>          .
2005/03/21  16:41    <DIR>          ..
2005/03/21  16:45                 8 rotest.txt
               1 個のファイル                 8 バイト
               2 個のディレクトリ    1,552,875,520 バイトの空き領域
```

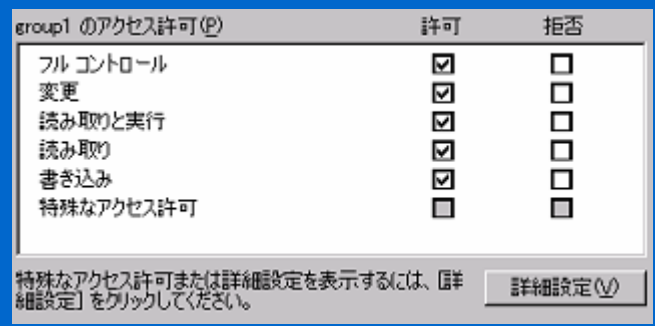
消えてません

NTのACLの処理(1)

- 特殊なアクセス権をそのまま移行するのは無理
- DOSレベルのアクセス権程度をマッピングできると思えばだいたいあっている
  - フルコントロール
    - たとえばユーザの rwx
  - 読み取りと実行＋読み取り
    - たとえばユーザの r-x

NTのACLの処理(2)

- NTのACLはSamba上ではこうなる
  - 変更
    - フルコントロールに変更される
  - 読み取りと実行
    - 読み取りと実行＋読み取り
  - 読み取り
    - 読み取り(r--)
  - 書き込み
    - 読み取り＋書き込み(rw-)



NTのACLの処理(３)

セキュリティの画面でACLをセットするとSambaでは....
(ファイルの場合)

セットするアクセス許可	設定されるアクセス許可	UNIX上の権利
フォルダのスキャン/ファイルの実行	属性の読み取り アクセス許可の読み取り	x
フォルダの一覧/データの読み取り	標準の'読み取り'	r
属性の読み取り	標準の'読み取り'	r
拡張属性の読み取り	標準の'読み取り'	r
ファイルの作成/データの書き込み フォルダの作成/データの追加 属性の書き込み 拡張属性の書き込み	特殊なアクセス権 ファイルの作成/データの書き込み フォルダの作成/データの追加 属性の書き込み アクセス許可の読み取り	w
削除/アクセス許可の読み取り アクセス許可の変更	何も設定されない	

NTのACLの処理(４)

同じことをディレクトリでやってみると

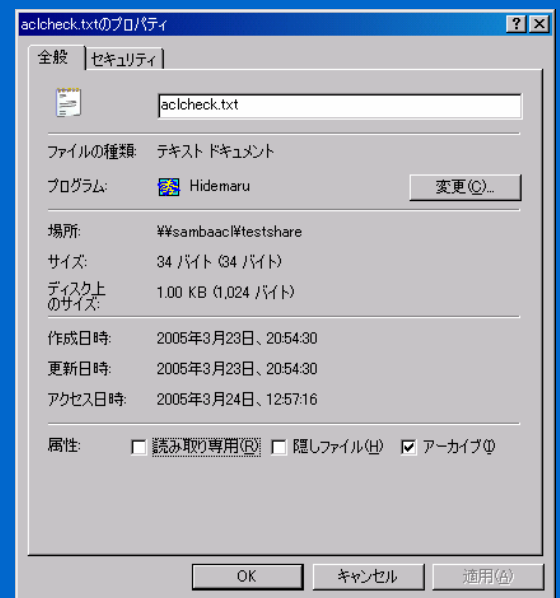
セットするアクセス許可	設定されるアクセス許可	UNIX上の権利
フォルダのスキャン/ファイルの実行	属性の読み取り アクセス許可の読み取り	x
フォルダの一覧/データの読み取り	標準の'読み取り'	r
属性の読み取り	標準の'読み取り'	r
拡張属性の読み取り	標準の'読み取り'	r
ファイルの作成/データの書き込み フォルダの作成/データの追加 属性の書き込み 拡張属性の書き込み	特殊なアクセス権 ファイルの作成/データの書き込み フォルダの作成/データの追加 属性の書き込み アクセス許可の読み取り	w
サブフォルダとファイルの削除 削除/アクセス許可の読み取り アクセス許可の変更	何も設定されない	

DOSのアクセス権との共存(1)

- 基本的にはDOSのアクセス権とNTのACLのand動作
  - Hidden,system,archive
    - Xビットにマップ(おさらい:DOSのアクセス権)
    - NTのアクセス権をいじるとSamba上では変更されてしまうことに注意

DOSのアクセス権との共存(2)

- readonly
  - 全般の画面でセットすると、NTのACLは
    - 読み取りと実行+読み取り　に変更される
    - 一旦プロパティを閉じないと反映しないので注意



トラブルになる例(1)

- LinuxのファイルシステムでのACLのエントリ数は有限
  - jfs　8191個
  - ext3　32個
  - xfs　24個

- さらに、ugoの分が3つ減らされる
  - Windowsで沢山のACEを使っていた場合に問題になる
- Windowsからの移行時に要注意

トラブルになる例(2)

- Administrator ≠ root
  - UNIXではrootは特権ユーザ
    - 何でも出来る
  - Windowsでは、Administratorも1ユーザ

ユーザがAdministratorを外しちゃうと……

- これも、Windowsからの移行時に問題となる

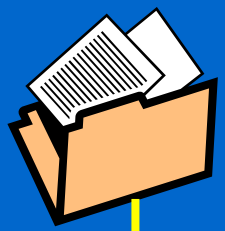
トラブルになる例 (3a)

- ファイルの所有権に関するトラブル
  - プライマリグループと所属するグループが複数ある
  - 特定のディレクトリ内のファイルを更新する場合

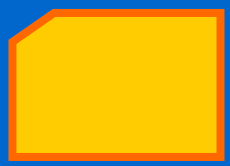
    

    更新後、他人がアクセス不可になる場合がある
  - 話がややこしいので図解

トラブルになる例 (3b)



ディレクトリ acltest
owner: root
group: users
access: rwxr-x---
acl:group1:rwx



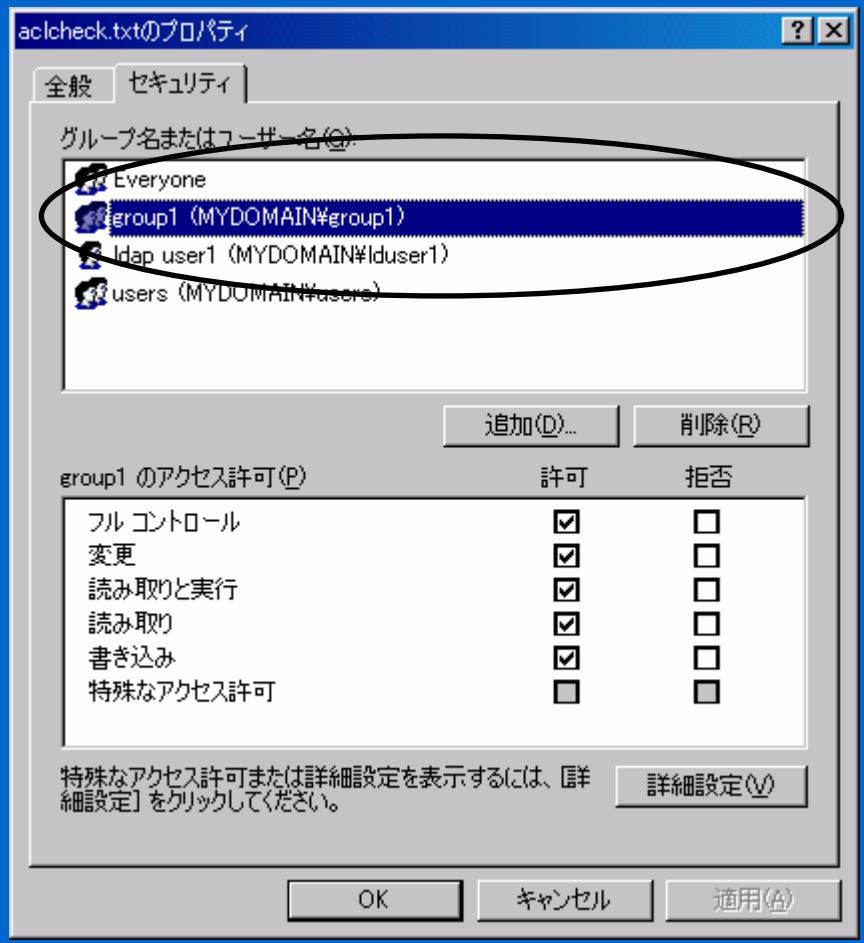
ファイル aclcheck.txt
owner: lduser1
group: users
acl: group1:rwx

変更処理

ユーザ ribbon
group(P): users
group(S): group1

ユーザ lduse1
group(P): users
group(S): group1

トラブルになる例 (3c)



group1が利用できる
ACLが付いている

これをribbonが変更
しようとした

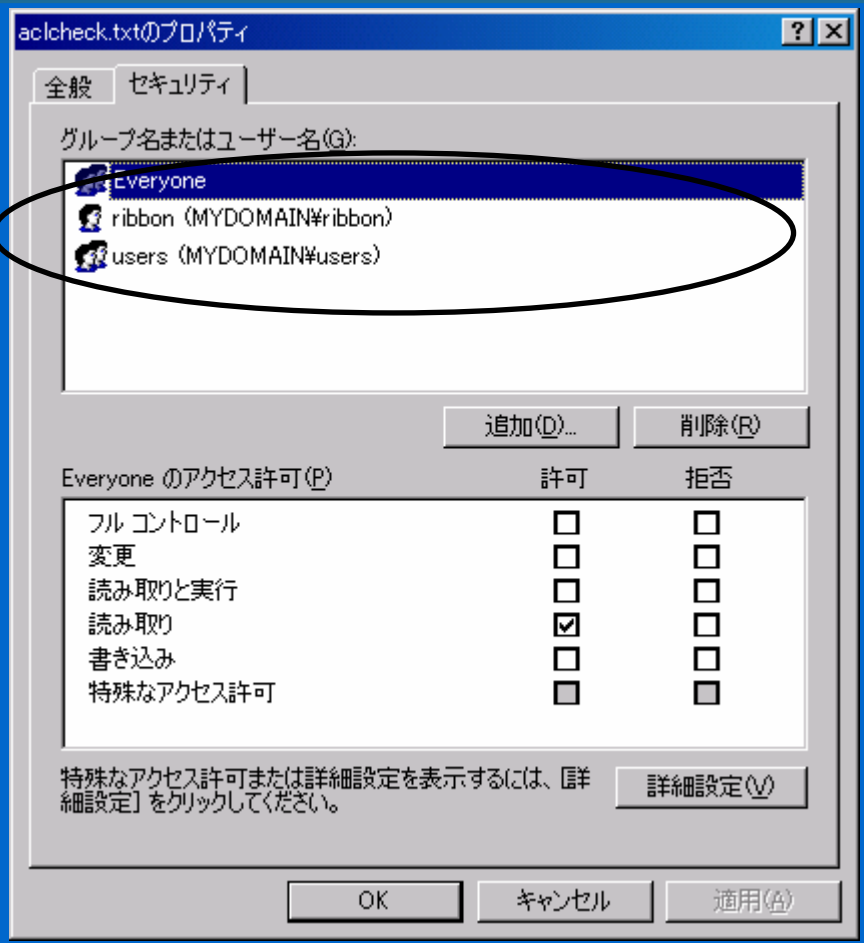
トラブルになる例 (3d)

ファイル aclcheck.txt
owner: lduser1
group: users
acl:group1:rwx

ファイルを更新するとき、バックアップを作り、新規ファイルを作成する形で行なう。

ファイル aclcheck.txt
owner: ribbon
group: users
acl: none!

トラブルになる例 (3e)



group1のACLがなくなってしまう

トラブルになる例 (3f)

- この場合、プライマリグループにwがないと (group1でアクセス制御している場合) lduser1はファイルに書けなくなる。
- 対処法
  - 複数のユーザが変更する場合、プライマリグループを同一にしておく。
- 書込み権が付いてしまう逆の例もありえる
  - 読み出しだけだったファイルが書き込み可能に

トラブルになる例(4)

- グループが所有者
  - Windowsではあたりまえ
    - Administratorsなど(複数の管理者)
  - UNIXにはない概念
- 移行の時の対処法
  - force unknown acl user = yes
  - winbind
  - 再マッピング

まとめ

- ACLを利用したWindows環境をSambaに移行するときが一番の難所です
- Windowsで出来たことが全部はできないことをまず理解しましょう
- あくまでもUNIXベースで動作していることを念頭におきましょう
- いい解決方法があったら samba-jp ML で共有しましょう

参考情報

- Linux Extended Attributes and ACLs
  - http://acl.bestbits.at/
- ディレクトリに対する制限
  - http://www.samba.gr.jp/project/kb/J0/1/05.html
- アクセス制御を利用する
  - http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/ja-jp/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/ja-jp/acl_con_use.asp
- にほんごであそぼ
  - http://www.nhk.or.jp/kids/program/index.html