

SubInACLを用いての ファイルサーバー移行

発端

- ▶ 現行ファイルサーバーの環境
 - サーバーのハード及びOS(NT4.0)はサポートが、切れて数年経過・・・
 - でも、業務に必須のシステムなので、ハードもOSも入れ替える事に・・・
 - サーバー内を確認した所、大量のファイルにローカルアカウントのアクセス権が付与されている事を発見！！

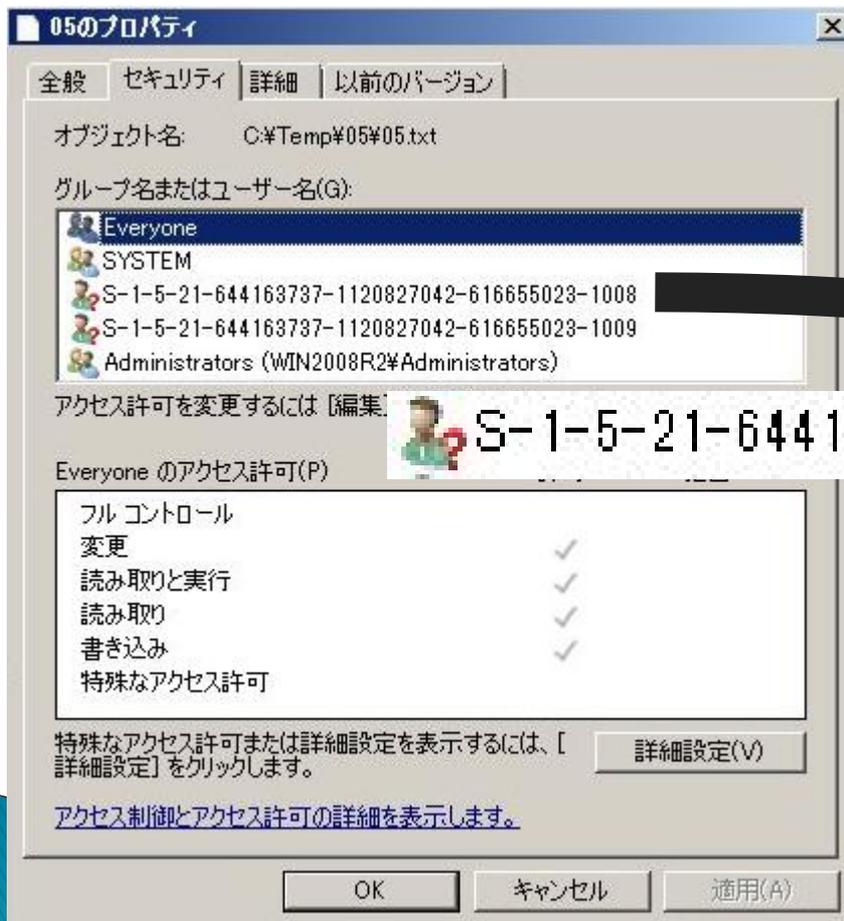
ローカルアカウントのアクセス権

▶ SID問題

- ローカルアカウントやローカルグループに付与されるSIDは常にユニークな値が割り当てされる
- そのため、通常のファイルコピーだけでは、アクセス権を維持する事はできない

例:アクセス権を維持できない

▶ xcopy(アクセス権付き)でコピー



S-1-5-21-644163737-1120827042-616655023-1008

不明なアカウントに...

当時、検討した対応策 その1



- ▶ **FSMT(File Server Migration Toolkit)**
 - **残念ながら、FSMTは仕様として、ローカルアカウント及びローカルグループに対応していないため、NG...**
 - **参考URL @IT様**
FSMTによるNTファイル・サーバ移行計画
http://www.atmarkit.co.jp/fwin2k/productreview/fsmt-02/fsmt-02_05.html

当時、検討した対応策 その2



▶ 手作業でのアクセス権付与

- アクセス権付きファイルが大量かつ
アクセス権が様々で有るため、NG...

当時、検討した対応策 その3



- ▶ **ドメインアカウントへの切り替え**
 - **設定変更箇所(作業工数)が多いため、NG...**

当時、検討した対応策 その4



▶ SubInACLにてSIDを置き換え

- ローカルアカウントの数が多く、置き換えスクリプト作成が大変のため、NG…
- しかし、ここでSubInACLが高機能で有る事に気が付く！

SubInACLとは？

▶ SubInACLの簡単な説明

- SubInACLはMicrosoftから無償提供されているツール(リソースキット扱い)
- 主な利用用途は、SIDの置き換えやファイル所有権の変更など多機能
- 注目点: Playfileというオプションスイッチを利用するとSubInACLで取得したアクセス権情報を復元できる事
- という事は・・・ アクセス権の一括取得と一括設定がSubInACLでは可能！！

SubInACLでの移行の流れ

移行元ファイルサーバー

ローカルアカウント情報の取得

Adduserやnetコマンド

NTFSアクセス権情報の取得
ネットワーク共有情報の取得

SubInACL使用

各フォルダ/ファイルを
移行先サーバーへコピー

場合により、取得した
アクセス権のファイル編集

移行先ファイルサーバー

ローカルアカウント情報の
復元

Adduserやnetコマンド

ローカルアカウントのパスワード移行は課題

ネットワーク共有の設定

NTFSアクセス権情報の復元
ネットワーク共有情報の復元

SubInACL使用

終わり

例: NTFSアクセス権情報の取得と復元

▶ NTFSアクセス権の取得

- コマンドプロンプトから以下を入力
- `subinacl /noverbose /outputlog=出力ファイルパス /subdirectories ドライブ名 or フォルダパス /display`

▶ NTFSアクセス権の復元

- コマンドプロンプトから以下を入力
- `subinacl /playfile アクセス権情報ファイルパス`

例：共有アクセス権情報の取得と復元

▶ 共有アクセス権の取得

- コマンドプロンプトから以下を入力
- `subinacl /verbose=1 /outputlog=出力ファイルパス /share ¥¥ コンピュータ名¥*`

▶ 共有アクセス権の復元

- コマンドプロンプトから以下を入力
- `subinacl /playfile アクセス権情報ファイルパス`

例: アクセス権情報を取得したファイルの中身

▶ NTFSアクセス権

```
=====
+File ¥¥Server_A¥C$¥File_Share¥Sales
=====
/control=0x0
/owner          =builtin¥administrator
/primary group  =Server_A¥なし
/audit ace count =0
/perm. ace count =12
/pace =Server_A¥group_support Type=0x0 Flags=0x9
AccessMask=0xa0000000
/pace =Server_A¥group_support Type=0x0 Flags=0x2
AccessMask=0x1200a9
/pace =Server_A¥group_sales Type=0x0 Flags=0x9
AccessMask=0x10000000
```

移行元サーバーの
コンピュータ名が
残っているので、
別名のコンピュータ名に
復元する場合は
置き換え

まとめ



- ▶ **SubInACLを利用すると、ここが便利！**
 - アクセス権の一括取得/一括設定が可能
 - OSバージョン問わずにアクセス権を付与可能
 - * WindowsNT4.0から、WindowsServer2008R2にもアクセス権を移行する事ができました
 - テキストファイルでアクセス権情報が出力されるため、編集も容易
- ▶ **SubInACLはファイルサーバー移行時に非常に頼りになるツールです**

Appendix:NTFSアクセス権移行 構文例

NTFSアクセス権の取得

subinacl /noverbose /outputlog=アクセス権情報出力ファイルパス
/subdirectories ドライブ名orフォルダパス /display

例①:ローカルのc:¥Toolフォルダ以下のアクセス権情報をローカルの
c:¥log¥acl.txtにアクセス権情報を出力する。

```
subinacl /noverbose /outputlog=c:¥log¥acl.txt  
/subdirectories c:¥tool¥*.* /display
```

NTFSアクセス権の復元

subinacl /playfile アクセス権情報入力ファイルパス

例②:ローカルのc:¥Toolフォルダ以下のアクセス権をc:¥log¥acl.txtに保
存したアクセス権情報から復元する。

```
subinacl /playfile c:¥log¥acl.txt
```

Appendix:NTFSアクセス権取得,復元パターン①

例:待ち受けサーバーが用意できる場合

参考:サーバーAのCドライブのtempフォルダ以下のアクセス権情報を取得し,そのアクセス権情報をサーバーBのc:¥log¥ntfs_acl.txtに保存し,サーバーCにアクセス権情報を復元する場合の例です。

コマンドライン①:サーバーB(待ち受け) アクセス権情報取得

```
c:¥>subinacl /noverbose /outputlog=c:¥log¥ntfs_acl.txt  
/subdirectories ¥¥サーバーA¥c¥temp¥*. * /display
```

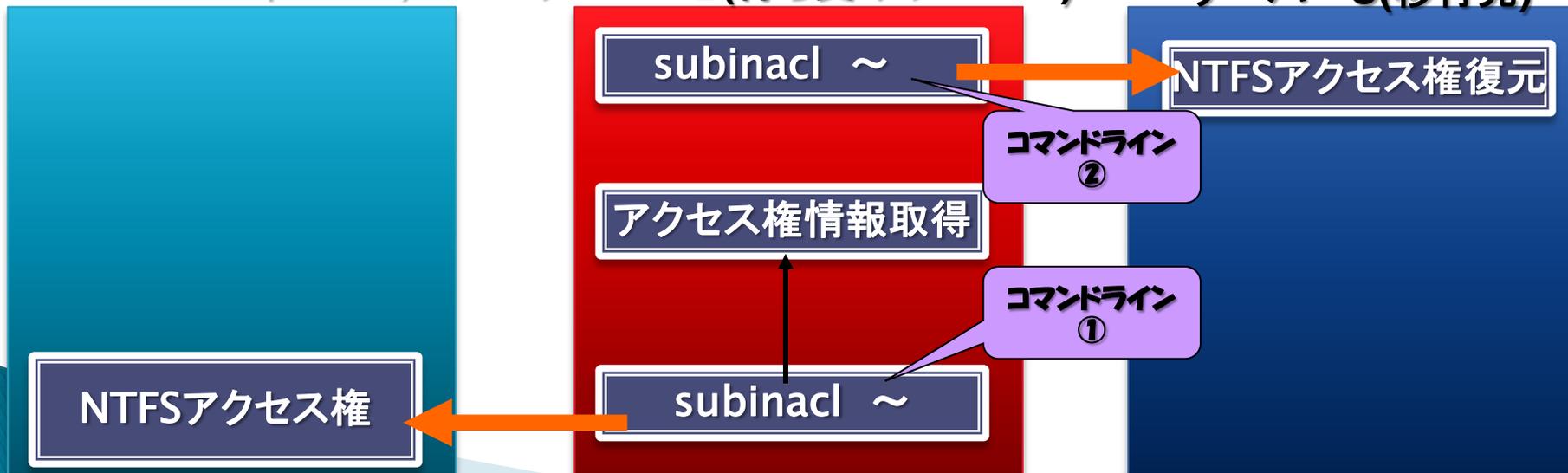
コマンドライン②:サーバーB(待ち受け) アクセス権情報復元

```
c:¥>subinacl /playfile c:¥log¥ntfs_acl.txt
```

サーバーA(移行元)

サーバーB(待ち受けサーバー)

サーバーC(移行先)



Appendix:共有アクセス権移行 構文例

共有アクセス権の取得

```
subinacl /verbose=1 /outputlog=アクセス権情報出力ログパス  
/share ¥¥コンピュータ名¥*
```

例①:ローカルのコンピュータ(ServerA) の共有のアクセス権情報をローカルの
c:¥log¥share.txtにアクセス権情報を出力する。

```
subinacl /verbose=1 /outputlog=c:¥log¥share.txt /share  
¥¥ServerA¥ *
```

共有アクセス権の復元

```
subinacl /playfile アクセス権情報保存ログパス
```

例②:ローカルのコンピュータ(ServerA) の共有のアクセス権情報をc:¥logに保存
したアクセス権情報から復元する。

```
subinacl /playfile c:¥log¥share.txt
```

Appendix:NTFSアクセス権取得,復元パターン②

例:移行元サーバー,移行先サーバーでコンピュータ名やIPアドレスが違い,
ネットワークで接続されている場合,移行元サーバーがWindowsNT4.0の場合

参考:サーバーAのCドライブtempフォルダ以下のアクセス権情報を取得し,そのアクセス権情報をサーバーBのc:\logフォルダ保存し,サーバーBにアクセス権情報を復元する場合です。

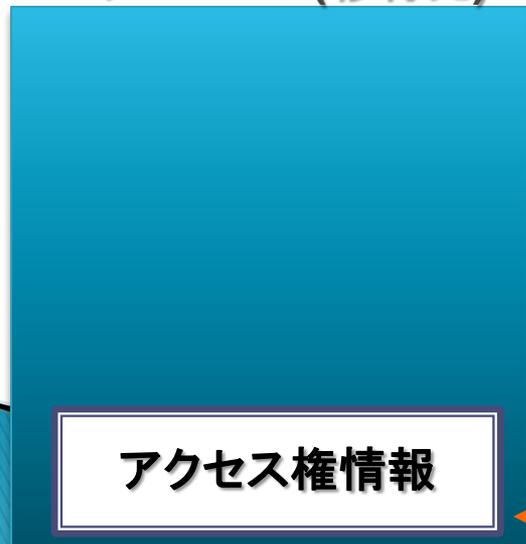
コマンドライン①:サーバーA(移行元) アクセス権情報取得

```
c:¥>subinacl /noverbose /outputlog=c:¥log¥ntfs_acl.txt  
/subdirectories ¥¥サーバーA¥c$¥temp¥*. * /display
```

コマンドライン②:サーバーB(移行先) アクセス権情報復元

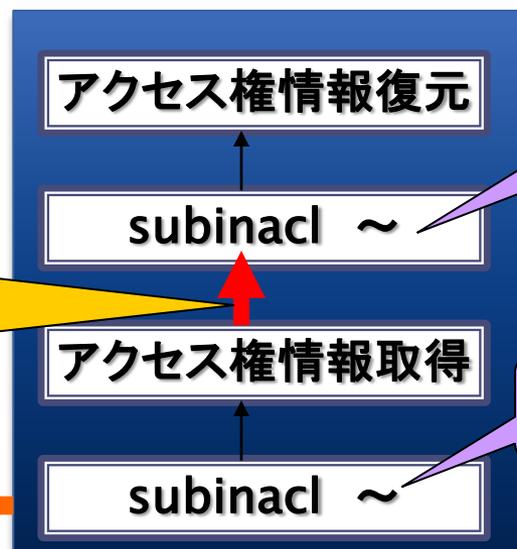
```
c:¥>subinacl /playfile c:¥log¥ntfs_acl.txt
```

サーバーA(移行元)



取得したアクセス権情報のテキストファイルを一部整形する必要があります。スライド7参照

サーバーB(移行先)



コマンドライン②

コマンドライン①