

# ACL 確認ツールコマンドライン仕様

2017/09/11

株式会社鉄飛テクノロジー

## 変更履歴

- 2017/09/11 /groupformat オプションを追加。
- 2017/08/28 /strictinheritcheck オプションを追加。
- 2016/07/25 AclDump.exe(GUI 版)のコマンドラインオプションを追加。
- 2015/08/11 /outfilenameutf8 オプションを追加しました。
- 2014/07/29 /ignoreownerace オプションを追加しました。
- 2013/11/27 /showdir オプションを追加しました。  
/hideinherited /hideinheritedace の設定にかかわらずフォルダ名は全部出力します。
- 2013/06/27 /showtop オプションを追加しました。本オプションを指定した場合、/hideinherited /hideinheritedace の設定にかかわらずに対象トップフォルダの情報を出力します。
- 2013/01/31 /targethost オプションを追加しました。
- 2012/03/14 進捗ファイル指定のオプション名に誤りがあり訂正しました。( /progress が正しく、 /progressfile は誤りでした)
- 2010/09/03 出力ファイル名指定コマンド文法の記載に誤植があり、「/out」を「/outfilename」に訂正しました。
- 2010/12/14 Ver.1.0.4 長いパス名（260文字を越えるような）のファイルでアクセス権の取得に失敗する問題に対処しました。

- 2010/09/03 出力ファイル名指定コマンド文法の記載に誤植があり、「/out」を「/outfilename」に訂正しました。
- 2010/12/14 Ver.1.0.4 長いパス名（260文字を越えるような）のファイルでアクセス権の取得に失敗する問題に対処しました。

## 文法

ACLDump のコマンドラインインタフェースは ACLDumpConsole.exe です。ACLDump.exe(GUI 版)については、本文書末尾をごらんください。

```
ACLDumpConsole <対象フォルダ> [<対象フォルダ 2>...] [/r <階層数>]
[/showfiles] [/hideinherited] [/hideinheritedace] [/strictinheritcheck]
[/showtop] [/ignoreownerace] [/showdir]
[/outfilename <出力ファイル名(SJIS)>]
[/outfilenameutf8 <出力ファイル名(UTF8)>]
[/progress <進捗ファイル名>]
[/targethost <ホスト名>]
[/rule <パーミッション名定義ファイル>]
[/groupformat <グループ名/ユーザー名フォーマット>]
```

/outfilename と /outfilenameutf8 は、いずれか片方のみ指定可能です。

両方省略した場合には標準出力になります。

## コマンドラインオプション

### 基本オプション

#### /showfiles

ファイルも出力（処理）対象にする。  
デフォルトではフォルダのみ出力します。

#### /hideinherited

親フォルダから継承したままのアクセス制御リスト（ACL）のファイル/フォルダは出力しない。

#### /hideinheritedace

親フォルダから継承していないアクセス制御エントリ（ACE）だけを出力する。

#### /strictinheritcheck

親フォルダから継承したとマークされている ACE のみで構成されている ACL であっても、親フォルダの ACL と各エントリを比較して、完全一致しない場合には当該 ACL を全部出力する。

/showtop も自動的にオンになります。

#### [ 詳しい説明 ]

Windows の ACL は ACE で構成されており、各 ACE は、親フォルダから継承したエントリに「inherited」フラグを立てるようになっています。

そのため、ACL Dump では、この inherited フラグをみて、親フォルダから継承された ACL を判別しています。

しかしながらこの方式には限界があり、「/strictinheritcheck オプション（親フォルダと子フォルダのアクセス権差異チェックを厳密に行う）」の機能を設けております。

アクセス権の変更時に、適応先に「サブフォルダ・ファイル」が含まれている場合、Windows エクスプローラは、親フォルダから順にサブフォルダおよびサブフォルダ内のファイルに対して再帰的に ACL を更新する処理を行います。

この処理は順次実行されるため、フォルダ内のサブフォルダ・ファイルが多数である場合には、全ファイルのアクセス権の更新に数分～数十分の長時間を要します。長時間の処理中にプロセスが異常終了したり、強制終了させられた場合には、処理が途中停止してしまい、処理が及ばなかったサブフォルダ・ファイルのアクセス権は、そのまま放置されて親フォルダと不一致となりますが、当該フォルダの ACL だけをみるともともと親フォルダから継承していたことになっているため、ACL Dump の基本方式でその違いを検出できません。

なお、このオプションを有効にすると、継承マークを頼らずに各エントリを比較するためその分処理スピードは遅くなります。

#### /showtop

スキャン対象のトップフォルダ（最上位フォルダ）について、無条件に ACL を出力します。

/hideinherited、/hideinheritedace が指定されても出力されます。

### `/outfile` <出力ファイル名>

結果をファイルに書き出します。(ファイル名は SJIS で渡します)

### `/outfileutf8` <出力ファイル名>

結果をファイルに書き出します。(ファイル名は UTF8 で渡します)

### `/progress` <進捗ファイル名>

進捗状況を別ファイルに書き出します。

### `/targethost` <ホスト名>

ユーザ名/グループ名のデコード時、指定されたホストに問い合わせを行います。

### `/rule` <パーミッション定義フィールド>

通常は編集不要です。

F=フルコントロール、C=変更 などの (「F」「C」などの) 記号を定義できます。通常は使わないオプションです。

### `/ignoreownerace`

「このフォルダ/このファイルのみ」のフルコントロール許可の ACE を無視 (出力省略) します。

### `/groupformat` <グループ名/ユーザー名フォーマット>

出力結果のグループ名/ユーザー名の文字列フォーマットを以下の変数を用

いて設定できます。既定値は `$(domain)¥$(group)` です

変数	意味
<code>\$(name)</code>	グループ名もしくはユーザー名
<code>\$(domain)</code>	ドメイン名もしくはコンピュータ名
<code>\$(displayname)</code>	表示名 (ActiveDirectory やユーザー管理に設定されている。未設定の場合があります。)
<code>\$(name_or_displayname)</code>	表示名が空白 (or 未設定) の場合には代わりに <code>\$(group)</code> を出力

例)

```
/groupformat $(domain)¥$(name)
```

```
TEPPI¥tanaka
```

```
TEPPI¥suzuki
```

```
/groupformat “$(domain)¥$(name) ($(displayname))”
```

```
TEPPI¥tanaka (田中太郎)
```

```
TEPPI¥suzuki ()
```

```
/groupformat $(domain)¥$(name_or_displayname)
```

```
TEPPI¥田中太郎
```

```
TEPPI¥suzuki
```

## 基本的な使い方例示

例 1) T:¥work フォルダ以下 2 階層をチェックする

階層数を省略した場合、2 階層までスキャンします

```
> ACLDumpConsole T:¥work
```

例 2) T:\work フォルダ以下 3 階層をチェックする

```
> ACLDumpConsole /r 3 T:\work
```

例 3) T:\work フォルダ以下 4 階層と T:\publi 以下 2 階層と C:\temp 以下 2 階層をチェックする

スキャン対象フォルダ毎に階層数を指定します

```
> ACLDumpConsole /r 4 T:\work /r 2 T:\public
```

例 4) フォルダだけでなくファイルも表示する、ただし、親フォルダから継承した ACL だけのファイルは出力しない

```
> ACLDumpConsole /r 4 T:\work /showfiles /hideinherited
```

例 4') 上記において、最上位フォルダ(T:\Work)は親フォルダから継承しただけであっても無条件に出力する

```
> ACLDumpConsole /r 4 T:\work /showfiles /hideinherited /showtop
```

例 5) 親フォルダから継承していない ACE (アクセス制御エントリ) のみを出力する

```
> ACLDumpConsole /r 4 T:\work T:\public /hideinheritedace
```

例 5') 上記において、最上位フォルダ(T:\Work)は親フォルダから継承し

ただけであっても無条件に出力する

```
> ACLDumpConsole /r 4 T:\work /hideinheritedace /showtop
```

例 5'') 「このフォルダのみ」の ACE を無視し、残りの ACE によって、親フォルダから継承していない ACL の判定および、親フォルダから継承していない ACE の判定を行う

CREATOR OWNER にフルコントロールの権限が与えられているフォルダ以下にファイル・フォルダを作成すると、そのフォルダは、作成者に対して「このフォルダのみ」を適用範囲とする、フルコントロールの ACE を持つようになります。

```
> ACLDumpConsole /r 4 T:\work T:\public /ignoreownerace /hideinheritedace
```

このようにすることで、「このフォルダのみ」「このファイルのみ」のフルコントロールアクセス権を無視するようにします。/ignoreownerace はかならず/hideinherited または /hideinheritedace と併用してください。(単体では動作に影響を与えません)

Windows Vista/2008 以降のファイルサーバでは「CREATOR OWNER」に対して「フルコントロール」アクセス権が定義されているフォルダにサブフォルダ・ファイルを作成すると、そのサブフォルダ・ファイルの ACE も親フォルダから継承した ACE として認識できますが、Windows2003/XP 以前のファイルサーバでは「このフォルダのみ」の「フルコントロール」ACE が継承なしで付加されてしまうため、これを無視するために当オプションがあります。

## 例 6) 標準出力の代わりに出力ファイル名を指定する

```
> ACLDumpConsole /r 4 T:¥work /outfilename C:¥temp¥test.txt
```

## 例 7) 進捗状況をファイル出力する

フォルダ/ファイルのスキャン 1000 件ごとに進捗状況をファイルに書き出します。

```
> ACLDumpConsole /r 500 T:¥ /progress progress.txt
```

このように進捗状況ファイルのファイル名を指定すると、そのファイルに 1000 件スキャンごとの進捗状況が報告されます。(巨大ファイルサーバの処理において、どの程度処理が進んだかを確認することができます。)

## 例 8) ファイルサーバ上のローカルユーザ名を表示する

通常、ツールを実行するマシンと同一ドメインのユーザのユーザ名はデコードされますが、リモートファイルサーバ上のローカルユーザ名を表示するには、/targethost ファイルサーバ名 をオプションとして加えてください。

```
> ACLDumpConsole /r 500 ¥¥broccoli¥docs¥ /progress progress.txt  
/targethost broccoli
```

## 出力の読み方

下記の順でタブ区切りテキストとして、各行に出力されます。

1. パス
2. 種別

- ・フォルダの場合 F
- ・ファイルの場合 T

### 3. No.

ACL を構成する ACE (エントリ) の連番です。同一ファイルの中では、1 番から順に振られます。なお、親フォルダから ACL を継承せず置換しているときは、特別に 0 番のエントリが出力されます。

### 4. 許可/拒否

許可のエントリと、拒否のエントリの別を表示します。

### 5. ユーザ/グループ

ユーザ/グループを示す SID をデコードして、ユーザ名/グループ名として表示します。デコードできない場合は SID のまま表示されます。

### 6. アクセス権

アクセスマスクを表現します。代表的なアクセスマスクとして、次の 4 種類は事前定義されています。

F : フルコントロール  
C : 変更  
R : 読取  
"" : なし

それ以外は「特殊なアクセスマスク」として扱われ、次のビット名をカンマ区切りで列挙します。

```
{symbol:"read", mask:"$1"},
```

```
{symbol:"read-attr", mask:"$80"},
{symbol:"read-xa", mask:"$8"},
{symbol:"exec", mask:"$20"},
{symbol:"write", mask:"$2"},
{symbol:"append", mask:"$4"},
{symbol:"write-attr", mask:"$100"},
{symbol:"write-xa", mask:"$10"},
{symbol:"del-child", mask:"$40"},
{symbol:"delete", mask:"$10000"},
{symbol:"read-acl", mask:"$20000"},
{symbol:"write-acl", mask:"$40000"},
{symbol:"take-own", mask:"$80000"}
```

なお、この定義は `dumprule.txt` の形式で定義ファイルを記述し、`/rule` オプションでパーミッション定義ファイルを読み込ませることで変更することが可能です。

## 7. フラグ (適用先)

このフォルダのみ	
このフォルダ、サブフォルダおよびファイル	(OI)(CI)
このフォルダとサブフォルダ	(CI)
このフォルダとファイル	(OI)
サブフォルダとファイルのみ	(OI)(CI)(IO)
サブフォルダのみ	(CI)(IO)
ファイルのみ	(OI)(IO)

## 8. 継承タイプ

親フォルダから継承したままの ACL のエントリ (ACE)	""
親フォルダから継承した ACL に追加されたエントリ (ACE)	+ (プラス)
親フォルダから継承せずに置換した ACL のエントリ (ACE)	- (マイナス)
親フォルダから継承せずに置換した ACL の 0 番目に出 力されるダミー ACE です	. (ピリオド)

権限不足などアクセス権読み取りに失敗した場合に 出力されるダミー ACE です	?
/strictinheritcheck オプションが指定されて、継承 ACL のチェックを厳格に行う場合、 親フォルダから継承しているはずなのに、 親フォルダと異なる ACE を持つ、すなわち <b>継承関係に 矛盾が発見された ACL のエントリ (ACE)</b>	X
/showdir オプションが指定された場合、 親フォルダから継承した ACL を持つフォルダについて /hideinherited,/hideinheritedace が指定されているに もかかわらず、強制的にフォルダ名を出力します。その 際のダミー ACE です	*

## (参考) No=0 のエントリの意義

親フォルダから ACL を継承せず、置換しているファイル/フォルダを目立たせるために、あえて出力しています。

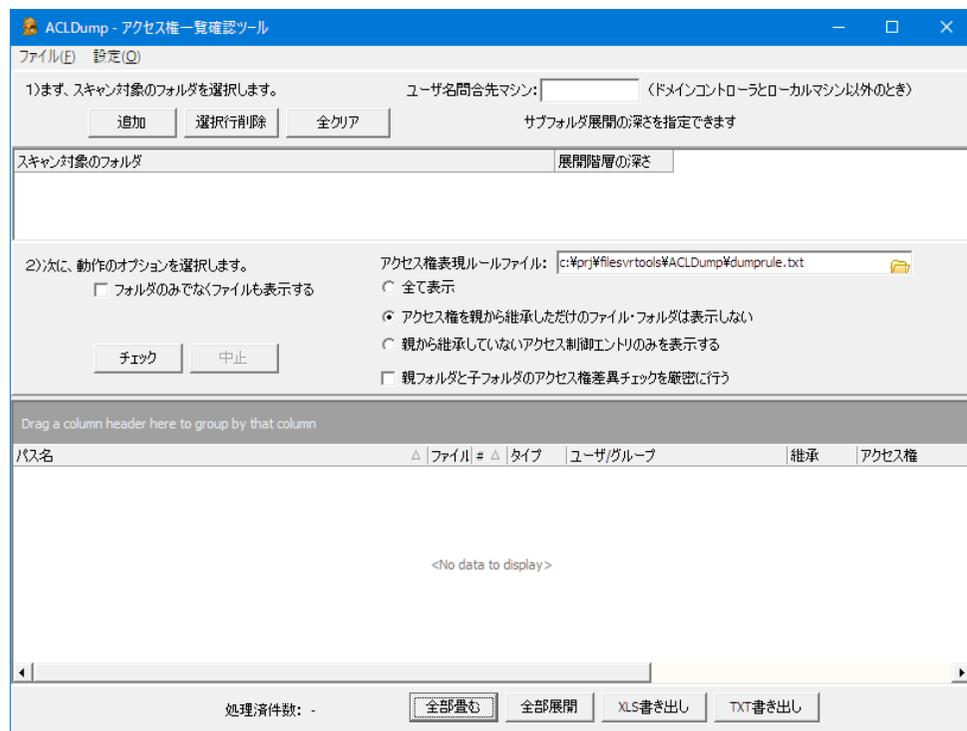
将来的に、ACLDump またはシリーズ製品で ACL 書き換え機能を実装するときに、「ダミーエントリがあったら、ACL をクリアする (継承を切る)。+-のエントリがあったらエントリ (ACE) を追加する」という扱いにすることを想定しています。

親フォルダから継承せずに ACL を置換している場合、特別に 0 番目のエントリが出力されます。

t:¥ okd F	0	—	—	.	.	.
t:¥ okd F	1	許可	SYSTEM F	(OD)(CI)	.	.
t:¥ okd F	2	許可	TEPPI¥okd	C	(OD)(CI)	.

## ACLDump.exe(GUI版)の画面と、ACLDumpConsole オプションの対応

ACLDump(GUI版)プログラムの画面で選択するオプションと  
ACLDumpConsole オプションの対応は下記の通りです。



GUI 画面要素	対応する ACLDumpConsole オプション
ユーザ名問い合わせマシン	/targethost <ホスト名>
展開階層の深さ	/r <階層深さ>
フォルダのみでなくファイルも表示する	/showfiles
アクセス権表現ルールファイル	/rule <パーミッション名定義ファイル>
すべて表示	
アクセス権を親から継承しただけのファイル/フォルダは表示しない	/hideinherited
親から継承していないアクセス制御エントリのみを表示する	/hideinheriteddace
親フォルダと子フォルダのアクセス権差異チェックを厳密に行う	/strictinheritcheck

して保存したものです。コマンドラインオプションで指定することで、最初からフィルタを適用可能です。

## ACLDump.exe(GUI版)のコマンドラインオプション

```
ACLDump <対象フォルダ> [<対象フォルダ 2>...] [/r <階層数>]
[showfiles]
[hideinherited | hideinheritedace | showall] [/strictinheritcheck]
[rule <パーミッション名定義ファイル>] [targethost <ホスト名>]
[filter <filter 定義ファイル名>]
```

原則として ACLDumpConsole のコマンドラインオプションに準じます。  
次は ACLDump 特有です。

- 出力対象：

/showall	すべて表示
/hideinherited	アクセス権を親から継承しただけのファイル・フォルダは表示しない。
/hideinheritedace	親から継承していないアクセス制御エントリのみを表示する。
/strictinheritcheck	親フォルダと子フォルダのアクセス権差異チェックを厳密に行う

- グリッドのフィルタ条件

/filter <filter 定義ファイル名>	filter 定義ファイルとは、結果表示グリッドにフィルタを適用した状態で「Customize」ボタンでフィルタ絞り込み状態を *.flt ファイルと
--------------------------	---