page 1 / 5

# BackOffice 原稿(5回目) 「入門・ビギナーのためのネットワークトラブル対策」

# 奥川博司

今回は、前回に引き続き「Windows NTリソースキット」(以下 リソキ)に収録されているツールを紹介します。今回紹介する ものはプログラムの実体であるプロセスに関する情報を表示したり、指定したプロセスを終了させるツール群と、リモートマ シンのシャットダウンを行うツールです。

#### プロセスの情報の表示・終了

通常アプリケーションを実行するとそれに対応したプログラム のプロセスが起動されるようになっています(アプリケーション によっては複数のプロセスが起動されるものもあります)。現在 どのようなプロセスが起動されているかを知るにはNTに標準 で備わっている「タスクマネージャ」が利用できます。「タスク マネージャ」を起動するには、タスクバー上のなにもない箇所 で右クリックを行いポップアップメニューを表示して[タスクマ ネージャ]を選択します。([スタート]メニューの[ファイル名を 指定して実行...]よりtaskmgrを実行してもよい)

「タスクマネージャ」の[プロセス]ページを見ることで現在 稼動 しているプロセスの一覧を知ることが出来ます。例えば イン ターネットエクスプローラを起動している場合には、

「IEXPLORE.EXE」という名前のプロセスが存在しているは ずです。インターネットエクスプローラが動作がおかしくなっ てフリーズしてしまったような場合には、「IEXPLORE.EXE」 を選択して、[プロセスの終了]ボタンを押すことで強制的にその プロセスを終了させることができます<sup>\*1</sup>。(図1)

DOTO DEO EVE	400	010	010 44181	バル大川丈川里	1X/28/17
PSTORES.EXE	106	00	0:00:00	32 KB	1548 KE
	118	00	0:00:00	20 KB	290 KE
	123	00	0:00:02	1380 NB	1292 KE
EXPLOREREXE	120	00	0:02:01	2430 NB	2328 NE
	120	00	0.00.00	200 KD	1400 NE
IOMDWO.EAE	101	00	0.00.01	320 ND 1026 KD	1304 KE
internatiexe	100	00	0.00.02	1050 ND	900 KC
hook mon ovo	107	00	0.00.01	4076 KD	1700 KE
	159	00	0.00.00	4370 KD	1206 KE
MDMEVE	170	00	0.00.00	1069 KD	1740 KE
winhlp32.eve	175	00	0.00.00	28 KB	288 KE
CMDEXE	185	00	0.00.00	304 KB	428 KE
NTV/DM EXE	100	00	0.00.00	84 KB	2824 KE
MONEYEC EYE	100	ññ	0.00.00	04 10	EOE4 NE
<b>IEXPLORE EXE</b>	209	ññ	0:00:01	7108 KB	2508 KE
DDUIELDEVE	010	00	0.00.00	10 V D	1126 KP

図1.タスクマネージャでのプロセス一覧表示

UNIX では、この「プロセスを終了させる」コマンドを、kill

\*1 この機能はあくまでも強制終了ですので、あまり不用意に使用するとシステム 全体が不安定になってしまうこともあります、最終的な手段として捉えておい てください コマンドと呼んでいます。NT では、上記のようにタスクマ ネージャからkill操作が可能ですが、リソキにはローカルマシ ンでkillを行うためのコンソールプログラムおよび、リモートマ シンに対してもkillを実行するためのプログラムが用意されてい ます。

ローカルマシンにて使用するコマンドは、プロセスの一覧を見 るためのTLIST.EXEあるいは、PULIST.EXEと、プロセス を終了させるKILL.EXEがとなっています、実行画面を図2 に示します。

C:#WINN I #system32#OML	).EXE	C
		J
C:¥>tlist		1
U System Process		Ш
2 System		Ш
24 CSRSS.EXE		Ш
34 WINLOGON FXF		-1
40 SERVICES EXE		
43 LSASS.EXE		
67 SPOOLSS.EXE		
82 RPCSS-EXE		
110 NODEACHT FYF		
126 EXPLORED EXE	Program Managar	
57 systrav.exe	i ogram manager	
128 em exec.exe		
131 LOADWC.EXE		
133 internat exe		
137 imejp98m exe		
139 backman.exe		
AU MINNIPSZ EXE	Overview of Windows NT Recourse Kit Teals	
159 CONTME.EXE	overview of windows wit Resource Kit Tools	
86 MDM.EXE		
185 CMD.EXE	C:¥WINNT¥system32¥CMD.EXE - tlist	
212 DDHELP.EXE		
45 TASKMGR-EXE	Windows NI ダルク マネージ ヤ	
198 NIVUM.EAE	Panata Vill	
165 JEXPLORE EXE	Welcome to Microsoft's Homenage - Microsoft Internet Evol	
Dier		
235 INISI EXE		
🚬 🛁 終了させた	こいプロセスの IDを指定	
U;#2KIII 100 ereeeee #185 killed		
process <del>m</del> rod killed		
C:¥>		
		<b>3</b>

#### 図 2 .TLIST、KILLの実行画面

TLIST 実行時に表示される項目は、左側から プロセスID、プ ロセス名、ウィンドウタイトルとなっています。TLIST には、 該当プロセスの詳細情報として、そのプロセスが使用している DLL の一覧やそのバージョンなどを表示する機能も備えていま す。マシンによってアプリケーションがうまく動かない場合な どに それぞれ利用されている DLL のバージョンを比較するこ とは問題を切り分けるために非常に役に立つことがあります。 特にWindows のコモンコントロールの DLL 「COMCTL32.DLL」や、Visual C++で作成したプログラム が利用していることがある MFC の DLL「MFC42.DLL」な どは多くのバージョンが存在しているため注意が必要です。(図 3)

リモートマシンに対してkillを実行可能にするためには、あらか じめリモートマシンにてRKILLSRV.EXEというサービスを 導入しておく必要があります(「Remote Kill サービスのインス

#### page 2 / 5

C:¥>tlist 142 142_telnet-eve Telnet - (/≵し)	•
U:#>tlist I42 I42:telnet.exe Telnet - (なし) owno	
CWD+ C+¥	
UmdLine: telnet VirtualSize: 26020 KB PeakVirtualSize: 30180 KB	
WorkingSetSize: 2280 KB PeakWorkingSetSize: 2300 KB	
NumberOfThreads: 1 155 Wing2924 - Midda - 0.,02020-00 Jack Engel0.00000570 States Waiting	
4.0.1381.1 shp 0x02630000 telnet.exe	
4.0.1381.77 shp 0x77f50000 ntdll.dll	
4.0.1381.81 shp Ux//e40000 USEK32.dll 4.0.1381.61 shp Dv76680000 IMM32.dll	
4.0.1381.81 shp 0x77ed0000 KERNEL32.dll	
4.0.1381.61 shp 0x77ea0000 GDI32.dll 4.0.1201.77 shp 0x77d00000 ADVARI22.dll	
4.0.1381.77 shp 0x77de0000 RPCRT4.dll	
4.0.1381.14 shp 0x77d50000 comdlg32.dll	
4.72.3609.2200 shp Ux77a80000 COMCTI32.dtl	
4.0.1381.77 shp 0x77660000 WS0CK32.dll	
4.0.1381.81 shp 0x77640000 \\S2_32.dll	
4.0.1381.28 shp 0x77630000 WS2HELP.dll	
0x10000000 BackHook.dll	
6.0.0.2523 shp 0x72cd0000 INDICULL.dii	
6.0.0.2523 shp 0x75320000 imejp98k.d	
4.U.1381.43 shp Ux//bcUUUU rpcltcl.dll	
C:¥>	
	-

図 3 .TLISTでのモジュール情報表示

トール方法」を参照)。RKILLSRV サービスが動いているマシ ンに対しては、コンソールコマンドのRKILL.EXEあるいは、 GUI版のWRKILL.EXEを使用することができます。どちら のコマンドもプロセスの一覧および、プロセスの終了という2 つの機能を併せ持ったツールとなっています。実行画面は 図4、 図5に示します。

🖗 Remote Kill	_ 🗆 ×	
¥¥Remote Server : ¥¥PRONT		
🕀 🕀 0 - System Process		
📄 🝈 209 – Explorer.exe		
🦾 🝈 220 – msime97m.e×e		
🚯 217 – loadwo.e.xe		
🔕 224 — Internat.exe		
🚯 175 – regedit.EXE		
🔄 🖓 104 – CMD.EXE		
🛄 🕼 191 – conime.exe		
🛶 🚯 240 - notepad.exe		
🛞 250 – iexplore.exe		
Exit Kill Selected Process Refresh Proce	ess List	

図 5.WRKILLの実行画面

マシンの挙動がおかしくなった場合など、これらのプログラム を用いて稼動しているプロセスを確認していくことで原因とな っているプログラムの追及などに役に立てることができると思 います。

🖧 C#WINNT¥system32¥CMD.EXE	]
C:¥≻rkill /view ¥¥pront	]
System Process 0 System 2 smss.exe 21 csrss.exe 28 winlogon.exe 35 services.exe 41 spoolss.exe 68 ovspmd.exe 77 pmd.exe 112 ovtrapd.exe 143 ovactiond.exe 146 Ilssrv.exe 83 RpcSs.exe 90 snmptrap.exe 93 snmptrap.exe 109 snmpdm.exe 124 wpaagt.exe 129 tcpsvcs.exe 95 pstores.exe 125 wins.exe 59 rkillsrv.exe 222 lsass.exe 44 nddeagnt.exe 74 Explorer.exe 209 msime97m.exe 220 loadwc.exe 217 Internat.exe 224 regedit.EXE 175 CMD.EXE 104 conime.exe 191 notepad.exe 240 iexplore.exe 250	
操作は正常終了しました。	
C:¥≻rkill /kill ¥¥pront 250 Process 250 killed !	
操作は正常終了しました。	
C:¥>_	·

図 4.RKILLの実行画面

#### 表 1.プロセス関係のツール一覧

18	こうロビス国际のう ル 見
ローカ	ルマシンにて使用するコマンド
TLIST.EXE	稼動中のプロセス一覧を表示
KILL.EXE	指定したプロセスを終了
ローカルおよびリ	モートマシンに対して使用可能なコマンド
PULIST.EXE	稼動中のプロセス一覧を表示(ローカルマシ ンに対して実行した場合はプロセスの所有 者情報も表示)
リモートマシン(R	KILLSRV サービスが動いているマシン)に 対して使用するコマンド
WRKILL.EXE	GUI 版のRemote Kill プログラム
RKILL.EXE	コマンドライン版Remote Kill プログラム

Remote Kill サービスのインストール方法

通常 サービスをインストールするために、oemsetup.infとい うファイルが用意されているのですが、RKILLSRV.EXE で はそのファイルが用意されていないためリソキに含まれる INSTSRV.EXE というサービスのインストーラを用いて手動

でインストールを行います。(図6)

サービスのインストール

1. リモートマシンの任意のディレクトリにRKILLSRV.EXE をコピーします。

2. コマンドプロンプトにて下記のコマンドを実行します。(この例では、"Remote Kill Service"という名前のサービスとして「c:\ntreskit\rkillsrv.exe」ファイルをインストールしています)

instsrv "Remote Kill Service" c:\ntreskit\rkillsrv.exe 3. [サービス]コントロールパネルを開いて "Remote Kill Service"を選択し、[開始]ボタンを押します。

サービスの削除

1. [サービス]コントロールパネルにて、削除したいサービスを 停止します。

2. コマンドプロンプトにて下記のコマンドを実行します。 inetsrv "Remote Kill Service" remove

## SHUTDOWN.EXE リモートシャットダウン

リモートマシンのシャットダウンを行うコマンドラインツール です。プロセスの終了だけでは手におえない場合など再起動せ ざるを得ない場合があります、このコマンドを使用することで 離れた場所にあるWindows NT マシンのシャットダウンやリ プートを行うことが可能となります。

具体的に利用方法のひとつとしては、長期稼動をさせることに よって若干不安定になるサーバがある場合など、スケジュール 実行を行うat コマンド<sup>\*2</sup>と このshutdown コマンドを組合わせ ることで週に一回 日曜の深夜などに自動的にリプートを行うと いった用途が考えられます。

#### このコマンドの使用方法は、

shutdown \\Computer

として、シャットダウンを行いたいコンピュータ名を指定する だけです。オプションには強制シャットダウンを行う指定や、 シャットダウンが実際に実行されるまでのタイムアウト値の設 定などがありますので詳しくはコマンドリファレンスを参照し てください。

同様の機能をもった GUI 版のツールである SHUTGUI.EXE というツールも存在しています。

注.うまく機能しない場合は、下記の情報なども参照してみてく ださい。

マイクロソフトのサポート技術情報「 J041981:[NT]リモート

シャットダウンに失敗する」http://www.microsoft.com/ mscorp/worldwide/japan/support/kb/articles/j041/9/81. htm

# さいごに

今回 紹介したツールはシャットダウンを行うといったような強 力な機能のため当然、管理者権限が必要となりますが慎重にシ ステムを構成することで役に立てることができると思います。 さて、ちょっとネットワークと離れた話題となってしまってお りますので次回はネットワークモニタを用いたトラプル対策な どについて言及したいと考えております。

<sup>\*2</sup> リソキには、atコマンドの GUI版である WINAT.EXE というツールも用意されて います

page 4 / 5

リソキの情報がどこから収集すればよい? リソースキットに収録されているツールは便利なものが色々あ るのですがその使用方法についてちゃんと日本語で解説された ものは残念ながら見かけたことがありません。しかしながら有 志の方によって リソキの話題を取り扱った Web サイトやメー リングリストが運営されています。リソキ関連情報を探すため の最初の一歩となり得るWeb サイトを2つほどご紹介しておき ます。



永江さん。「初心者による、リソースキット・プロジェクト!」 http://www.netwave.or.jp/~jun-n/

リソースキットの入手方法に関する情報や、リソキのツールを 利用したユーザアカウント登録方法やタイムサーバの設定方法 などでは具体的な使い方が詳しく紹介されています。

吉川さん。「Resource Kit Project(Supplement Two)」 http://www.iza.kamakura.kanagawa.jp/reskit.html リソースキットの新しいバージョンであるSupplement Two にて追加になっているツールにも言及されているリソキ収録 ツールの紹介や、リソキ関連情報を取り扱うNT-Reskit-Mailing Listの運営されています。

		1 0
🖉 WindowsNT S	erver 4.0 Resourc	eKit Supplement Two – Microsoft Internet Explorer 📃 🗖 🗙
ファイル(E)	編集(E) 表示()	ク 移動(G) お気に入り(A) ヘルプ(B) 🥂 🦉
- -		
] 4 . 4 . (		🗴 💽 🎯    / T D A 💽 http://www.iza.kamakura.kanagawa.jp/reskit.ntmi
		▲
Dean	waa Kit	Drain at (Supplement Two)
Resou	Irce Kit	Project (Supplement Two)
El dr. Att	AD.	
和文 初 1 日	180	Hac NI-Committeez ResourceNit FreeBSD
	トップページ	このページは永江純さんのWindowsNT Server Resource Kit Projectを
	たい 175年 日 ED	影ながら(?)支援するページです。
	and codiac	私は管理者でないため善殺、WindowsNT Workstationを使用するのですが
	音楽活動	そのResource Kitlに関する情報がなかったので自分でやってしまおう
Fi	reeBSDとの格闘	と思ったものです。WindowsNT 4.0 Workstation Resource Kitlま
_		ASCII社よりMicrosoft Pressで1/6/円+祝で売っています。 注意・インフトーラーが付属していますがPartのこれを使用したいでください
Rec	WindowsNT ourceKit Project	これでPerlをインストールしようとすると悲惨な結果になることが多いです。
1.000	Surgerin Tropper	
	NT-Committee2	WindowsNT World1998年9月号にて紹介されました。
	リンク集	これから力をいれようと思っています。
	63484	なお、 <u>yoshikawa@iza.kamakura.kanagawa.ip</u> にメールをくださった方には
	<u>H C.4671</u>	このコンテンツの進行状況を随時お伝えします。
	メーリングリスト	このページはWindows NT 4.0 Workstation Besource Kit(日本語版)のための
		ものでしたが、この度、
		Windows NT 4.0 Server Resource Kit Supplement Two (日本版はなし)に
		145長することにいたしました。現在はFまで145長作業が済んでいます(2度い・・)
		最新情報
		11月24日発売のWindows NT PRESS #4(技術評論社)に
		私の原稿が掲載されています。たた・・ → 部譲値かありまして、 それらけへ後 正理主と てまとめていくつもいです
		連動企画(?)としてNT-Reskit-Mailing Listが運営されています。
		<u>メーリングリストのページ</u> をごらんください。
		数字ABCDEEGHIJKLMNOPQRSTUVWXYZ
4		
24 <sup>1</sup>		<u> </u>
2		

page 5 / 5

#### プロセス情報の表示

TLIST.EXE tlist [/t] { pid | pattern } /t プロセスの親子関係によってツリー表示 pid 指定した pid のモジュール情報を表示 pattern 指定したパターンと一致するプロセス名、あるいは ウィンドウタイトルを持つプロセスのモジュール情報を表示

#### <u> プロセスの終了</u>

KILL.EXE
kill [/f] { pid | pattern }
/f プロセスの強制終了
pid 指定した pid のプロセスを終了
pattern 指定したパターンと一致するプロセス名、あるいは
ウィンドウタイトルを持つプロセスを終了

#### <u>プロセスの一覧およびその所有者を表示</u>

PULIST.EXE pulist [\\Server] [\\Server...] \\Server指定したリモートマシンでのプロセス一覧を表示 オプションなしで実行した場合はローカルマシンでのプロセス 一覧およびそのプロセスの所有者名を表示

#### リモートマシンのプロセス表示・終了

RKILL.EXE rkill { /view | /token } \\servername rkill /kill \\servername \\pid /view \\servername で稼動しているプロセス一覧を表示 /token \\servername に対して所有しているリモートセキュリ ティトークンの表示

# <u>サービスのインストール・アンインストール</u>

INSTSRV <servicename> { <exe\_file> | remove } [-a < account name>] [-p <account password>] servicename インストール(あるいは削除)したいサービス名 exe\_file サービスのEXEファイルがあるフルパスを指定 remove サービスの削除 -a <account name> サービスを実行するアカウントを指定 -p <account password> サービスを実行するアカウントのパ スワードを指定

## リモートマシンのシャットダウン

shutdown [\\computer\_name] [/1] [/a] [/r] [/t:xx] ["msg"] [/y] [/c] [/?]

\\computer\_name シャットダウンしたいリモートコン ピュータの名前を指定。 未指定の場合であっても他のオプションによって開始され

- る場合は、ローカルマシンの名前が使用されます。
- /1 ローカルマシンのシャットダウンを行う。
- /a シャットダウンの中止。タイムアウト待機中のみ有効。こ
- のオプションを指定した場合、他のオプションは無視されます。 /r シャットダウン後にリプートを行う。
- /t:xx 実際にシャットダウンを開始するまでのタイムアウト(秒)を設定。デフォルトは20秒。

"msg" シャットダウンが行われることを示すダイアログに表 示する127文字以内のメッセージを設定します。

- /y 以後の質問に対してあらかじめyesを指定します。
- /c 稼動中のアプリケーションを強制終了します。
  注. /c オプションを指定した場合、動作中のアプリケーションはデータが変更されていてもファイル保存を促すダイアログを表示しないため、保存していないデータは破棄されてしまいます。
- /? コマンドラインオプションの説明を表示します。

#### 参考文献

Microsoft Windows NT 4.0 Server ネットワーキングガイド アスキー出版局 Windows NT ヘルプファイル

#### 参考 URL

「Windows NT Resource Kit 」 http://www.netwave.or.jp/~jun-n/ 「Windows NT Server 4.0 ResourceKit Supplement Two 」 http://www.iza. kamakura.kanagawa.jp/reskit.html