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*1。(図１)

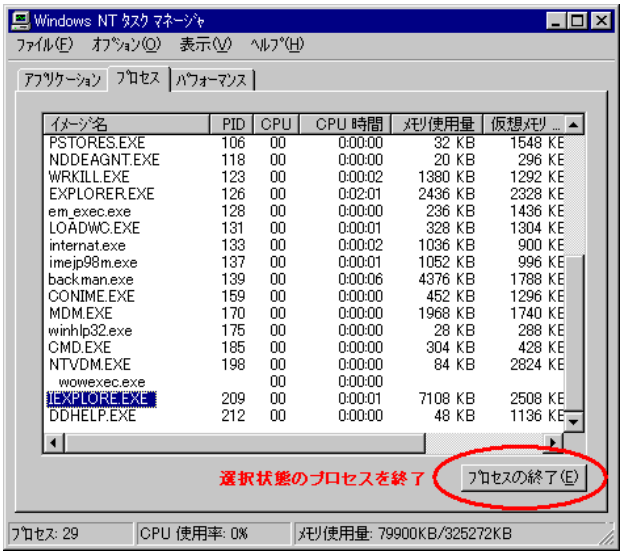

図１.タスクマネージャでのプロセス一覧表示

UNIX では、この「プロセスを終了させる」コマンドを、kill 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。

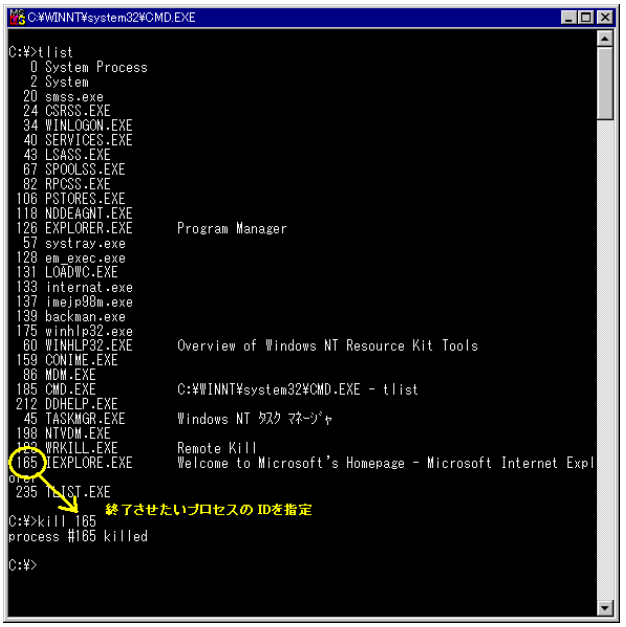

図２.TLIST、KILLの実行画面

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

*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

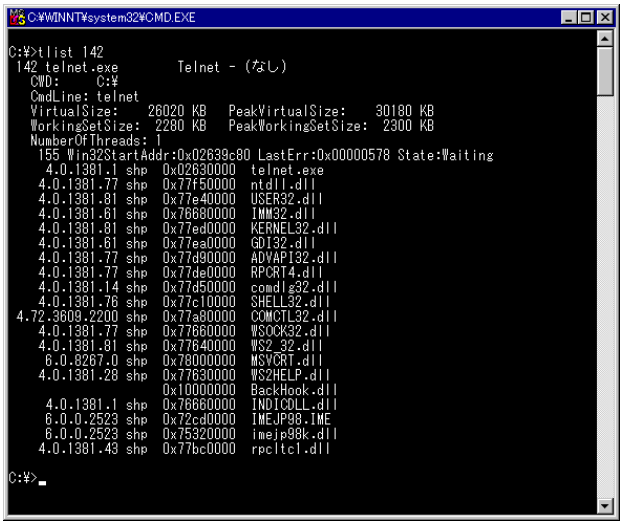

図３.TLISTでのモジュール情報表示

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。

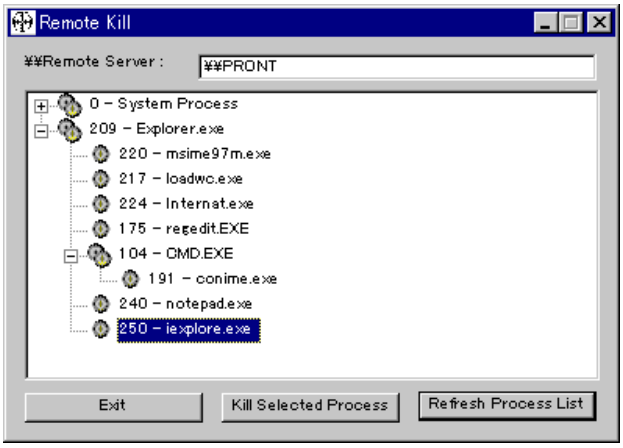

図５.WRKILLの実行画面

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。

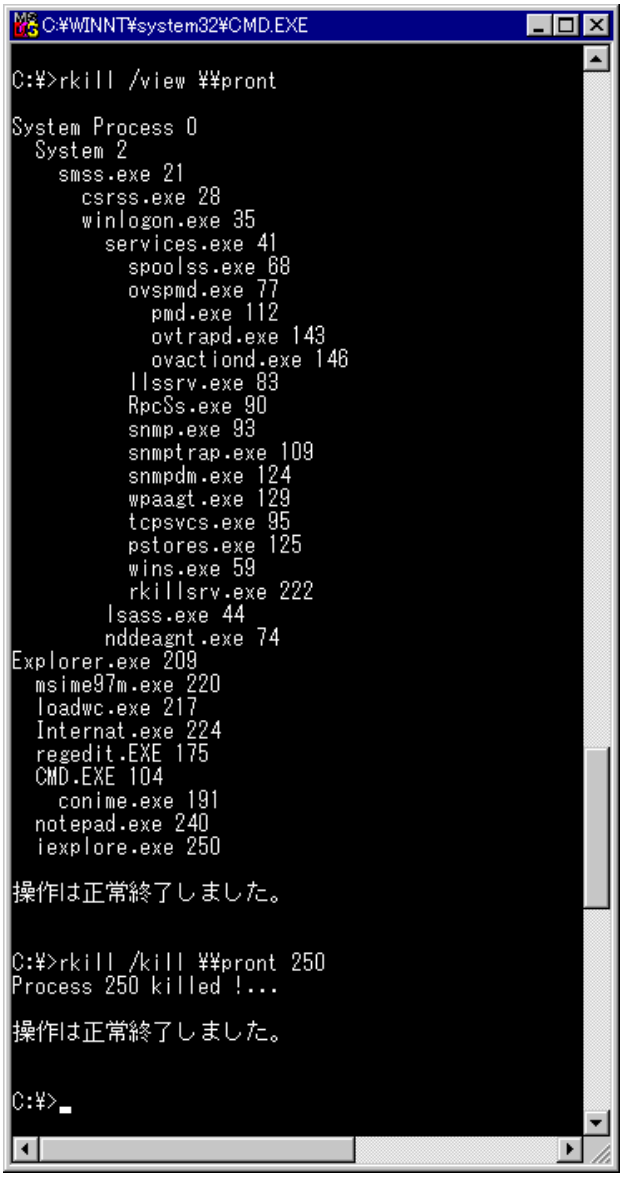

図４.RKILLの実行画面

表１.プロセス関係のツール一覧

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(RKILLSRV 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ブ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[*2]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ブ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

[*2] 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

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ブル対策などについて言及したいと考えております。

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。

◇ 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

◇ プロセスの終了

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

◇ プロセスの一覧およびその所有者を表示

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

◇ サービスのインストール・アンインストール

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] [/l] [/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。

/l　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ブートを行う。

/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