WinDBG Cheatsheet
by katahiromz
2022-03-27

*** General ***

`!help`	Show help	ヘルプを表示。
`.hh (keyword)`	Open help file	ヘルプファイルを開く。
`dt (type-name)`	Dump type	型（構造体など）を確認。
`r`	Show CPU registers	CPU レジスタを確認。
`ln`	List Nearest Symbols	現在の実行位置付近のシンボル。
`k`	Show call stack (without parameters)	呼び出し履歴を表示 (引数なし)。
`kb`	Show call stack (displays the first 3 parameters)	呼び出し履歴を表示 (引数あり)。
`.tlist`	List Process IDs	プロセス ID 一覧。
`.process (address)`	Attach the process by process address	プロセスをアタッチする。
`u (address)`	Unass*mble Address	アドレス位置を逆汗。
`uf (function-name)`	Unass*mble Function	関数を逆汗。
`LM`	List loaded Modules	モジュールの一覧。
`x (Module!symbol)`	Examine symbols (wildcard OK)	モジュール内のシンボルを確認。
`.reload /user`	Reload user symbols only	ユーザモードのシンボルのみ。カーネルシンボルは無視。

*** Execution ***

`bp (function-name)`	Set Breakpoint on function	ブレイクポイントを関数先頭に置く。
`bp (address)`	Set Breakpoint on address	ブレイクポイントをアドレスに置く。
`g`	Go	ブレイクポイントか例外まで一気に実行。
`t`	Step Into (Trace)	実行位置を一歩進める。
`gu`	Step Out (Go Out)	関数から脱出するまで実行。
`p`	Step Over	実行位置を一まとまりだけ進める。
`pa (address)`	Step to Address	実行位置を指定アドレスまで進める。
`.restart`	Restart process	プロセスを再起動。
`bl`	List breakpoints	ブレイクポイント一覧。

*** Memory ***

`d (address)`	Dump memory	メモリブロックを吐く。
`dw (address)`	Dump memory as WORDs	2 バイトずつメモリを吐く。
`dc (address)`	Dump memory as DWORDs	4 バイトずつメモリを吐く。
`du (address)`	Dump memory as Unicode string	Unicode 文字列としてメモリを吐く。

*** Kernel Debugging ***

`!process 0 0`	Show all the processes	プロセス一覧。
`!process 0 0 (exe-name)`	Show Process by name (wildcard OK)	EXE ファイル名でプロセスを列挙。
`!process -1 0`	Show current process	現在のプロセス情報を表示。

*** Misc ***

`!gle`	Show `GetLastError()` value	最後のエラーコードの値を表示する。