

windbgでやる
.NETデバッグ入門
Lv 1くまー

中 博俊

デバッグって使ってますか？

- Visual Studio

もちろんWindbgですよ。

環境を用意しましょう

- <http://www.microsoft.com/japan/whdc/DevTools/Debugging/default.mspx>

Debugging Tools for Windows を使用する

- 📦 [Windows シンボル パッケージのダウンロード](#)
各種バージョンの Windows 用シンボル パッケージ。
- 📄 [Debugging Tools for Windows 32 ビット バージョンのインストール](#)
最新の 32 ビット パッケージのダウンロード ページ。
- 📄 [Debugging Tools for Windows 64 ビット バージョンのインストール](#)
最新の 64 ビット パッケージのダウンロード ページ。
- 📄 [Debugging Tools for Windows の最新情報](#)
Debugging Tools for Windows の後続バージョンの機能に関する情報。
- 📖 [デバッグ ツールとシンボル: はじめに](#)
Debugging Tools for Windows を使用する際のヒント、およびベスト プラクティス。






環境を用意しましょう

シンボル パッケージのダウンロード リンクの表示

- + [Windows 7 および Windows Server 2008 R2](#)
- + [Windows Server 2008](#)
- + [Windows Vista](#)
- + [Windows Server 2003 および Windows XP x64 Edition](#)
- + [Windows XP](#)
- + [Windows 2000](#)

環境を用意しましょう

Debugging Tools for Windows を使用する

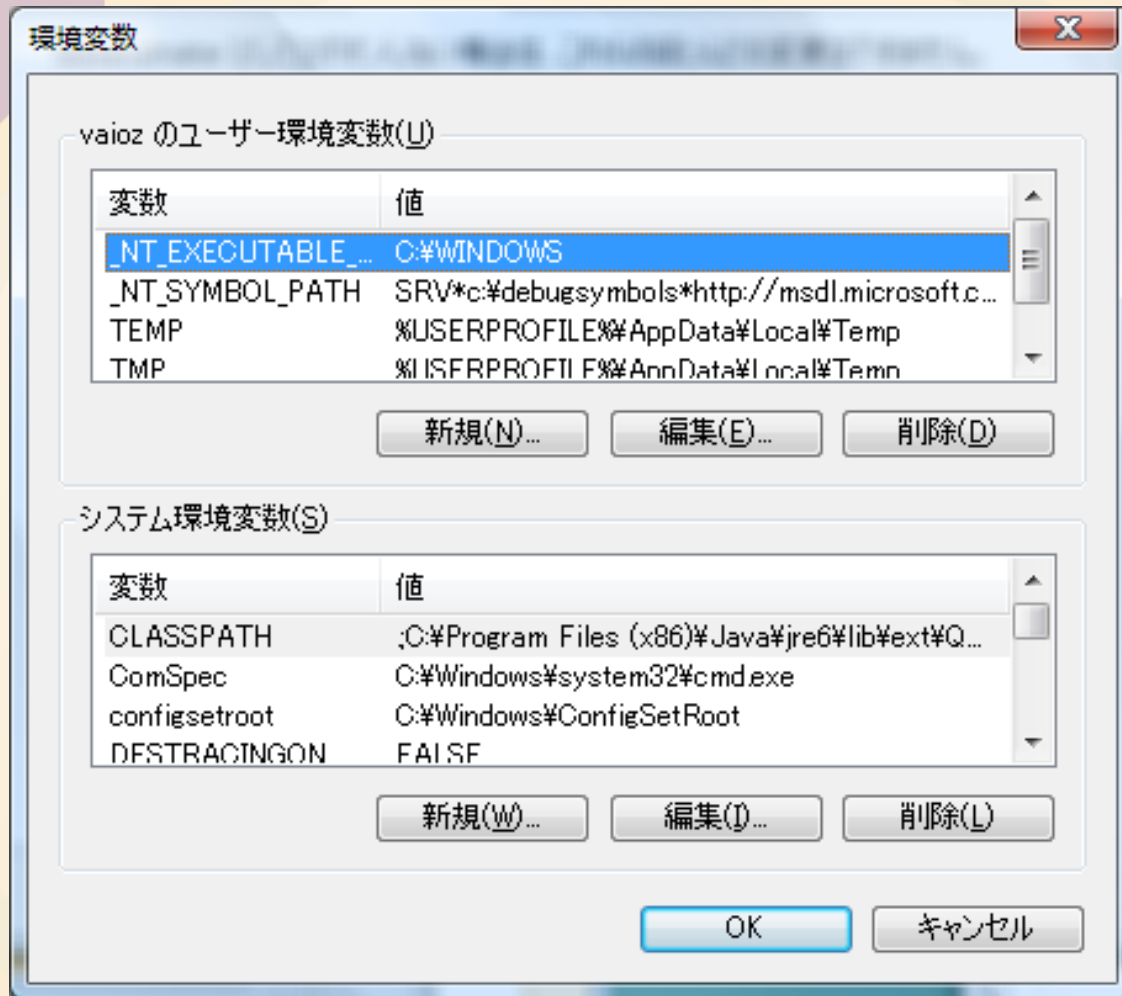
-  [Windows シンボル パッケージのダウンロード](#)
各種バージョンの Windows 用シンボル パッケージのダウンロード ページ。
-  [Debugging Tools for Windows 32 ビット バージョンのインストール](#)
最新の 32 ビット パッケージのダウンロード ページ。
-  [Debugging Tools for Windows 64 ビット バージョンのインストール](#)
最新の 64 ビット パッケージのダウンロード ページ。
-  [Debugging Tools for Windows の最新情報](#)
Debugging Tools for Windows の最新バージョンの機能に関する情報。
-  [デバッグ ツールとシンボル : はじめに](#)
Debugging Tools for Windows を使用する際のヒント、およびベスト プラクティス。

64ビットアプリケーションは64ビットを、32ビットアプリケーションは32ビットを
基本的には両方の環境をダウンロードする

環境を用意しましょう

- 環境変数の設定
 - <http://msdl.microsoft.com/download/symbols>
- `_NT_SYMBOL_PATH`
 - `SRV*[symbolを入れるローカルフォルダ]*http://msdl.microsoft.com/download/symbols`
 - `SRV*c:¥debugsymbols*http://msdl.microsoft.com/download/symbols;c:¥windows¥symbols`
- `_NT_EXECUTABLE_IMAGE_PATH`
 - `C:¥WINDOWS`

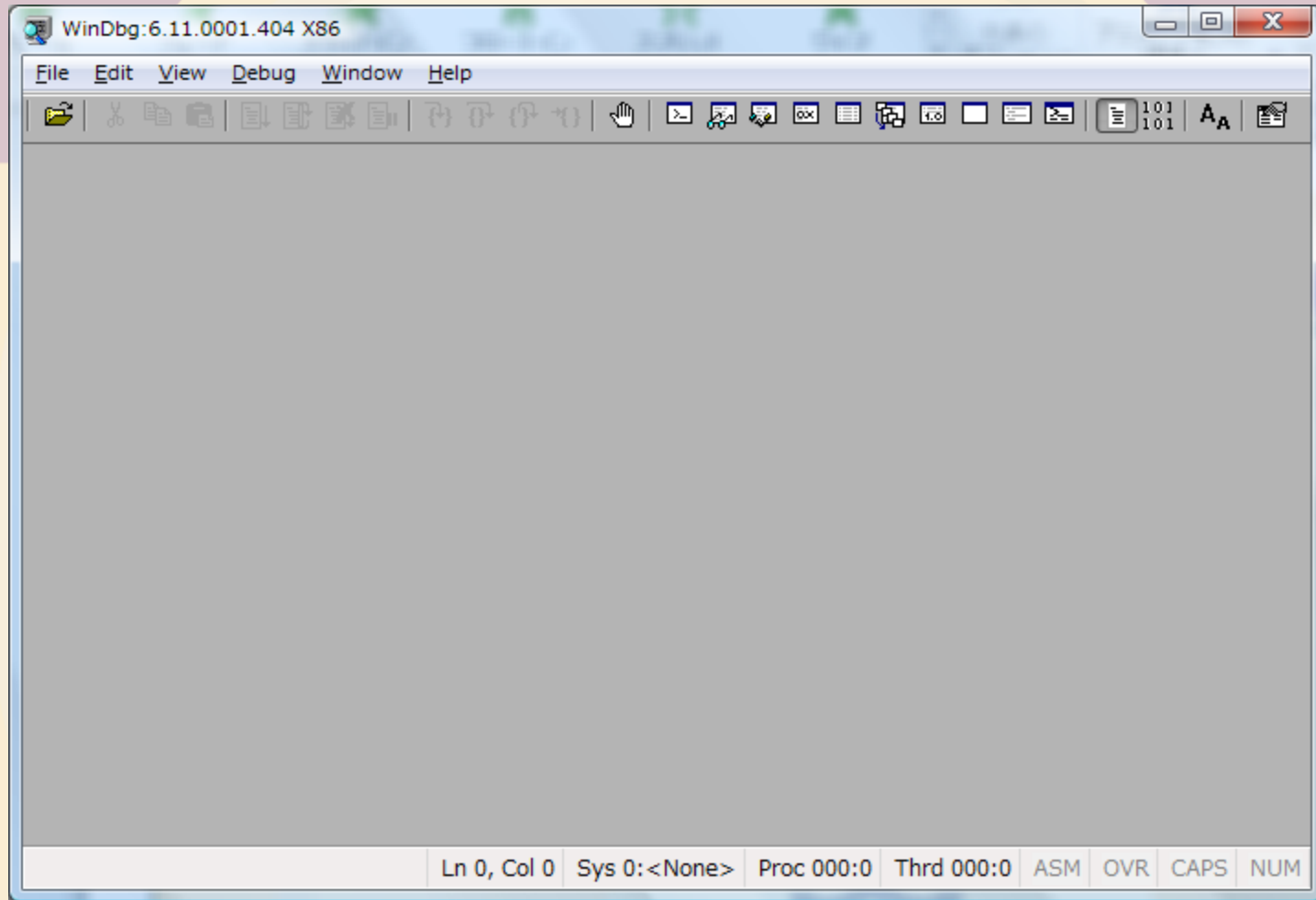
環境を用意しましょう



Visual Studio に影響しない方法

- `set _NT_SYMBOL_PATH="SRV*c:¥symbols*http://msdl.microsoft.com/download/symbols;c:¥windows¥symbols"`
- `set _NT_EXECUTABLE_IMAGE_PATH=C:¥WINDOWS`
- `cd C:¥Program Files (x86)¥Debugging Tools for Windows (x86)¥`
- `"C:¥Program Files (x86)¥Debugging Tools for Windows (x86)¥windbg.exe"`

まずはwindbgを起動してみよう

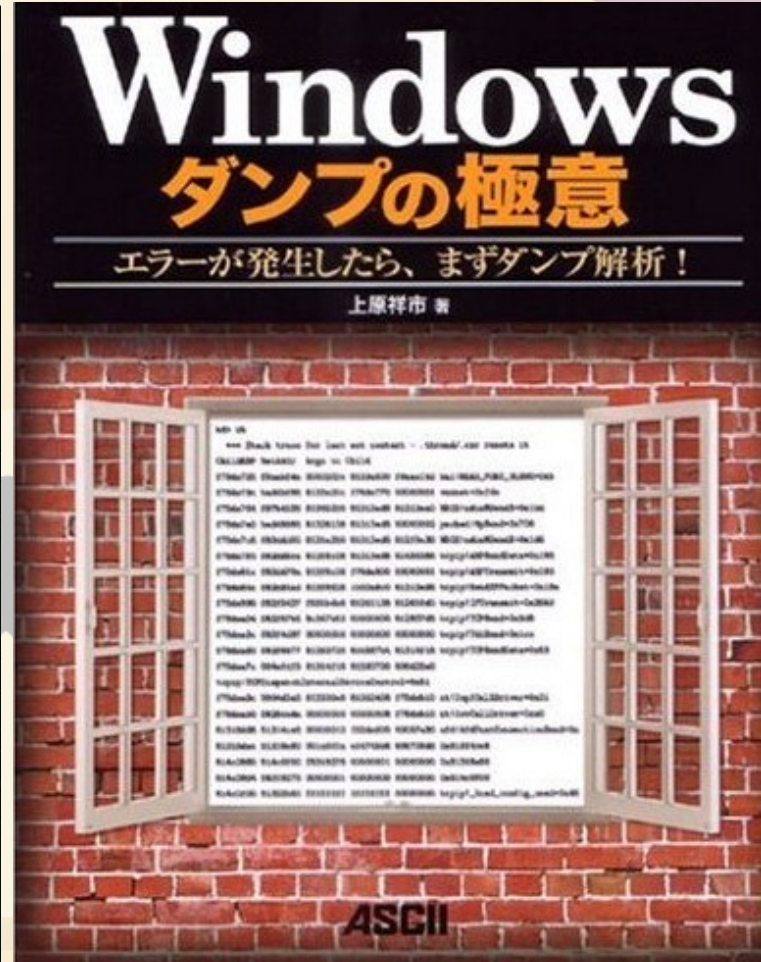
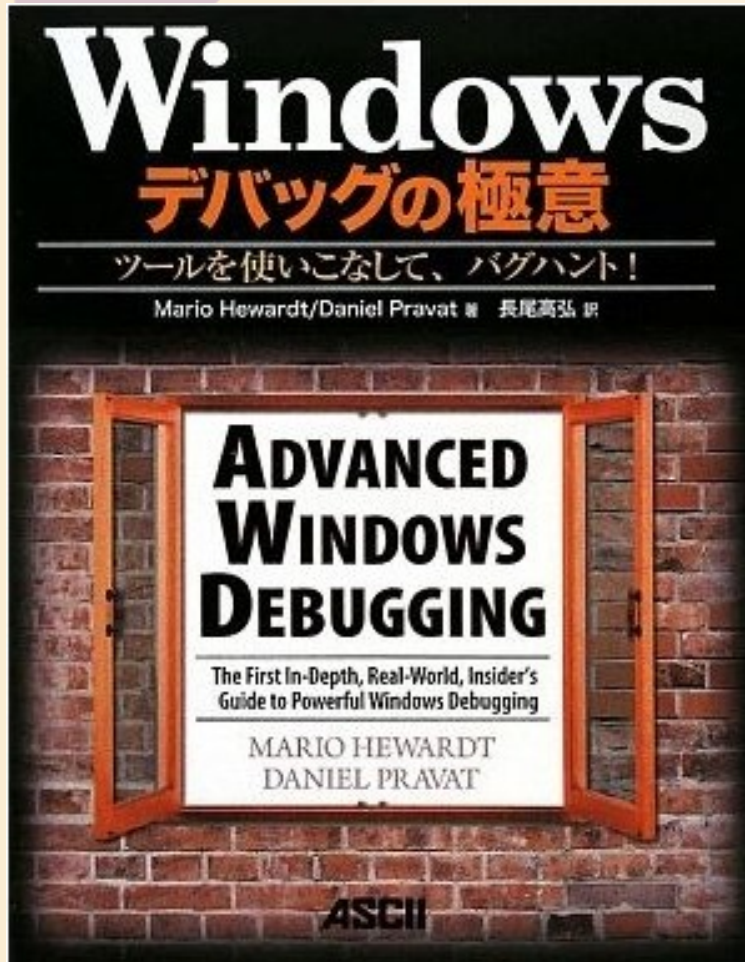


```
"C:\Users\vaioz\AppData\Local\Temporary Projects\ConsoleApplication1\bin\x86\Debug\ConsoleApplication1.exe" - WinDbg:6.11.0001.404 X86
File Edit View Debug Window Help
Command
CommandLine: "C:\Users\vaioz\AppData\Local\Temporary Projects\ConsoleApplication1\bin\x86\Debug\ConsoleApplication1.exe"
Symbol search path is: SRV*c:\debugsymbols*http://msdl.microsoft.com/download/symbols;c:\windows\symbols
Executable search path is: C:\WINDOWS
ModLoad: 013c0000 013c8000 ConsoleApplication1.exe
ModLoad: 774d0000 77630000 ntdll.dll
ModLoad: 737f0000 73838000 C:\Windows\SysWOW64\mscoree.dll
ModLoad: 75d20000 75e30000 C:\Windows\syswow64\KERNEL32.dll
(2c90.290c): Break instruction exception - code 80000003 (first chance)
eax=00000000 ebx=00000000 ecx=7b850000 edx=00000000 esi=ffffffe edi=774f4c52
eip=774e0004 esp=0037f560 ebp=0037f590 iopl=0         nv up ei pl zr na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000246
*** ERROR: Symbol file could not be found. Defaulted to export symbols for ntdll.dll -
ntdll!DbgBreakPoint:
774e0004 cc             int     3
0:000> g
ModLoad: 76160000 76226000 C:\Windows\syswow64\ADVAPI32.dll
ModLoad: 76fa0000 77090000 C:\Windows\syswow64\RPCRT4.dll
ModLoad: 754b0000 75510000 C:\Windows\syswow64\Secur32.dll
ModLoad: 73750000 73794000 C:\Windows\Microsoft.NET\Framework\v4.0.20506\mscoreei.dll
ModLoad: 73690000 7374d000 C:\Windows\SysWOW64\MSVCR100.dll
ModLoad: 75820000 75878000 C:\Windows\syswow64\SHLWAPI.dll
ModLoad: 75900000 75990000 C:\Windows\syswow64\GDI32.dll
ModLoad: 75b20000 75bf0000 C:\Windows\syswow64\USER32.dll
ModLoad: 75bf0000 75c9a000 C:\Windows\syswow64\msvcrt.dll
ModLoad: 757c0000 75820000 C:\Windows\SysWOW64\IMM32.DLL
ModLoad: 75510000 755d8000 C:\Windows\syswow64\MSCTF.dll
ModLoad: 75cb0000 75cb9000 C:\Windows\syswow64\LPK.DLL
ModLoad: 76e60000 76edd000 C:\Windows\syswow64\USP10.dll
ModLoad: 745f0000 7478e000 C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.6001.18000_none_5cdbaa5a083979cc\com
ModLoad: 6a9a0000 6af30000 C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
ModLoad: 73e30000 73ecb000 C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4053_none_d08d7da0442a985d\MSVCR80.dll
ModLoad: 75ca0000 75ca7000 C:\Windows\syswow64\PSAPI.DLL
ModLoad: 76260000 76d70000 C:\Windows\syswow64\shell32.dll
ModLoad: 755e0000 75724000 C:\Windows\syswow64\ole32.dll
ModLoad: 60340000 60348000 C:\Windows\Microsoft.NET\Framework\v2.0.50727\culture.dll
ModLoad: 5e020000 5eb17000 C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\c068708e16abf0be77a21b9f29817d83\mscorlib.ni.dll
ModLoad: 6db90000 6dbe8000 image6db90000
ModLoad: 027d0000 02828000 image027d0000
ModLoad: 6db90000 6dbe8000 C:\Windows\assembly\GAC_MSIL\mscorlib.resources\2.0.0.0_ja_b77a5c561934e089\mscorlib.resources.dll
ModLoad: 707d0000 7082b000 C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorlib.dll
*BUSY* Debuggee is running...
Ln 12, Col 29 Sys 0:<Local> Proc 000:2c90 Thrd 000:290c ASM OVR CAPS NUM
```



わんくま同盟 福岡勉強会 #10

Unmanagedなことは



今回は
マネージドアプリケーション
だけが対象です。

- SOSのロード

- .load

- C:¥WINDOWS¥microsoft.net¥Framework64¥v2.0.50727¥sos.dll

- .load

- c:¥windows¥Microsoft.NET¥Framework¥v2.0.50727¥SOS.dll

- .NET1.1アプリケーションの場合には以下

- .loadby sos mscorwks

ヒープを見てみましょう

- !dumpheap -stat

MT	Count	TotalSize	Class Name
5e2650e4	335	14740	System.Int16[]
5e2641d0	1733	87132	System.Object[]
5e290a00	717	168600	System.String
5e293470	70	177180	System.Byte[]

MT=MethodTable

Count=インスタンス数

TotalSize=利用バイト

Class Name=クラス



```
0:006> !dumpheap -stat
```

```
total 9000 objects
```

```
Statistics:
```

MT	Count	TotalSize	Class Name
6cdfbfd0	1	12	System.Drawing.GraphicsUnit
6a2a6438	1	12	System.Collections.Generic.ObjectEqualityComparer`1[[System.IntPtr,
6a2a6198	1	12	System.Collections.Generic.GenericEqualityComparer`1[[System.Int16,
6a2a190c	1	12	System.Collections.Generic.GenericEqualityComparer`1[[System.String,
6a2a0bbc	1	12	System.Security.Permissions.ReflectionPermission
6a29f8c4	1	12	System.Resources.FastResourceComparer
6a29eadc	1	12	System.Boolean
6a29e5c8	1	12	System.DefaultBinder

Method
Table

存在数

使用メ
モリ

クラス名




```
!dumpheap -type TestObj
```

Address	MT	Size
02747fb4	00146c3c	20

total 1 objects

インスタ
ンスアド
レス

Method
Table

使用メ
モリ

オブジェクトをのぞいてみよう

```
0:005> !DumpObj 2747fb4
```

```
Name: WindowsFormsApplication1.TestObj
```

```
MethodTable: 00146c3c
```

```
EEClass: 00540c60
```

```
Size: 20(0x14) bytes
```

```
(C:\Users\naka9\Documents\Visual Studio
```

```
2008\Projects\WindowsFormsApplication1\WindowsFormsApplication1\bin\x86\De
```

```
Fields:
```

MT	Field	Offset	Type	VT	Attr	Value	Name
6a2988c0	4000006	4	System.String	0	instance	00000000	a
6a29ab0c	4000007	c	System.Int32	1	instance	0	b
6a29aa5c	4000008	8	System.Int32[]	0	instance	02747fc8	c



メモリのダンプで中身を見る

- dd 2747fb4+c l1

DumpDWORD

ベースアドレス

オフセット

Length

- 0:005> dd 2747fb4+4 l1

- 02747fb8 00000000

- 0:005> dd 2747fb4+8 l1

- 02747fbc 02747fc8

- 0:005> dd 2747fb4+c l1

- 02747fc0 00000000

Int[]
だからメモ
リの番地が
入っている

配列をダンプする

```
0:005> !do 02747fc8
Name: System.Int32[]
MethodTable: 6a29aa5c
EEClass: 6a05b4d4
Size: 20(0x14) bytes
Array: Rank 1, Number of elements 2, Type Int32
Element Type: System.Int32
```

```
0:005> !da 02747fc8
Name: System.Int32[]
MethodTable: 6a29aa5c
EEClass: 6a05b4d4
Size: 20(0x14) bytes
Array: Rank 1, Number of elements 2, Type Int32
Element Methodtable: 6a29ab0c
[0] 02747fd0
[1] 02747fd4
```

配列の基
本情報

!da
!dumparray



被参照をチェックする

```
0:005> !gcroot 258a808
```

Note: Roots found on stacks may be false positives. Run "!help gcroot" for more info.

```
Scan Thread 0 OSThread 2918
```

```
ESP:16ed38:Root:02552208(System.Windows.Forms.Application+ThreadContext)->
```

```
025517a0(WindowsFormsApplication1.Form1)->
```

```
025518f0(System.Collections.Generic.List`1[[WindowsFormsApplication1.TestObj, WindowsFormsApplication1]])->
```

```
0258a830(System.Object[])->
```

```
0258a808(WindowsFormsApplication1.TestObj)
```

```
Scan Thread 2 OSThread e98
```



例外のデバッグ

- Debug -> Event Filters
- CLR exception – enabled – handled
- に設定する
 - sxe clr
- Gで実行する
- 例外が起きるアクションをする

(2900.288c): CLR exception - code e0434f4d (first chance)

First chance exceptions are reported before any exception handling.

This exception may be expected and handled.

eax=0032e9dc ebx=e0434f4d ecx=00000001 edx=00000000

esi=0032ea64 edi=006479a0

eip=7583b727 esp=0032e9dc ebp=0032ea2c iopl=0 nv up ei pl nz

na po nc

cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b

efl=00000202

*** ERROR: Symbol file could not be found. Defaulted to export

symbols for C:\Windows\system32\KERNELBASE.dll -

KERNELBASE!RaiseException+0x58:

7583b727 c9

leave



スタック情報を確認する(メソッドコール)

```
0:000> !CLRStack
```

```
OS Thread Id: 0x288c (0)
```

```
ESP      EIP
```

```
0032eab4 7583b727 [HelperMethodFrame: 0032eab4]
```

```
0032eb58 004204a9 WindowsFormsApplication1.Form1.button2_Click(System.Object, System.E
```

```
0032eb90 686d4170 System.Windows.Forms.Control.OnClick(System.EventArgs)
```

```
0032eba8 686cf55a System.Windows.Forms.Button.OnClick(System.EventArgs)
```

```
0032ebb8 68c66f34 System.Windows.Forms.Button.OnMouseUp(System.Windows.Forms.Mous
```

```
0032ebd4 68c37723 System.Windows.Forms.Control.WmMouseUp(System.Windows.Forms.Me
```

```
0032ec60 68f69fb2 System.Windows.Forms.Control.WndProc(System.Windows.Forms.Message
```

```
0032ec64 68f68781 [InlinedCallFrame: 0032ec64]
```

```
~~~~省略~~~~
```

```
0032f22c 6ab31b6c [GCFrame: 0032f22c]
```



スタック情報を確認する(スタックオブジェクト)

```
0:000> !DumpStackObjects
```

```
OS Thread Id: 0x288c (0)
```

```
ESP/REG Object Name
```

```
0032ea48 026e0b14 System.NotImplementedException
```

```
0032ea94 026e0b14 System.NotImplementedException
```

```
0032eaa4 026bf27c System.Windows.Forms.Button
```

```
0032eaa8 026bff2c System.EventHandler
```

```
0032eaac 026deb5c System.Windows.Forms.MouseEventArgs
```

```
0032ead8 026e0b14 System.NotImplementedException
```

```
0032eae0 026bff2c System.EventHandler
```

```
0032eae8 026deb5c System.Windows.Forms.MouseEventArgs
```

```
0032eb3c 026e0b14 System.NotImplementedException
```

```
0032eb58 026e0b14 System.NotImplementedException
```

```
0032eb5c 026bf27c System.Windows.Forms.Button
```

```
0032eb60 026a17a0 WindowsFormsApplication1.Form1
```

```
0032eb70 026bff2c System.EventHandler
```

```
0032eb74 026deb5c System.Windows.Forms.MouseEventArgs
```

```
0032eb78 026deb5c System.Windows.Forms.MouseEventArgs
```

```
0032eb7c 026bff2c System.EventHandler
```

```
0032eb80 026bf27c System.Windows.Forms.Button
```


- http://www.shoeisha.com/mag/windev/pdf/870507/windev0507_178_Debug.pdf
- 例外の調べ方
- http://keicode.com/note/debug_exception_test1.php
- SOSの日本語ヘルプ
- <http://msdn.microsoft.com/ja-jp/library/bb190764.aspx>

- Mini dumpファイルの解析のための方法
- <http://voneinem-windbg.blogspot.com/2007/10/failed-to-load-data-access-dll.html>