
2007/10/20 Admintech.jp 第6回勉強会

誰でもここまではできる
STOPエラー調査

中西 基裕

自己紹介

- × SEやっています
- × MS製品のサポートエンジニアを8年間
 - + 全国の顧客環境のトラブルを集中対応
- × 品質保証部署を経て、
- × 現在、セキュリティソリューション部所属



はじめに

- × STOPエラー調査は例えるなら富士山登山
- × 富士山は5合目まで車・バスで行ける
つまり、半分までなら誰でも行ける
STOPエラー調査も同じなのです
- × 今日は5合目までいってみましょう♪

※調査の手引き的内容であり、
深い解析方法は内容に含みません。

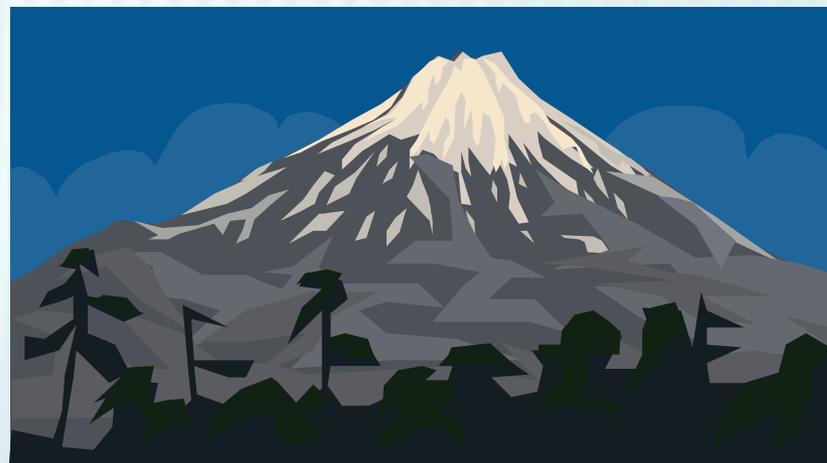


今回の流れ

- × はじめに
- × STOPエラーとダンプ取得の基本
- × さあWindbgを使おう
- × 最後に

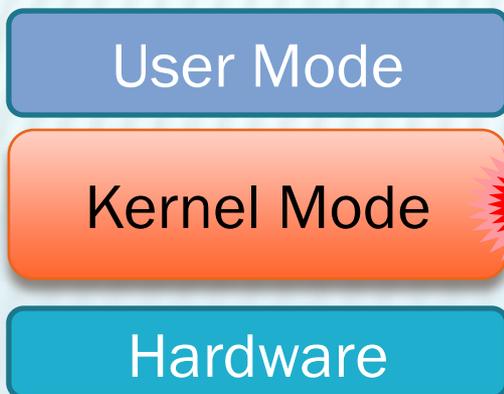
1~4合目

5合目



STOPエラーとは

- × Windows **カーネルモードのプログラムの異常により発生**する一連の処理
- × 発生後、青い画面が表示されるため、死のブルースクリーン（Blue Screen Of Death : BSOD）とも呼ばれる



```
A problem has been detected and Windows has been shut down to prevent damage to your computer.

IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

Technical information:
*** STOP: 0x0000000A (0x0227001d, 0x00000002, 0x00000000, 0x804eba3a)

Beginning dump of physical memory.
Physical memory dump complete.
Contact your system administrator or technical support group for further assistance.
```

STOP発生後に生成される情報

- × ブルー画面
- × イベントログ (SaveDumpイベント)
- × Memory.dmp



STOPエラーの原因は

- × ある書籍によると、**原因の70%は3rdパーティ製デバイスドライバの不具合**（らしい）



調査ポイント①

まず、3rdパーティ製ドライバが悪か、それ以外が悪か

ブルー画面やイベントログから調査してみる

× STOPコードは何番か？

例 STOP: 0x0000000A (引数,引数,引数,引数)

× ドライバのファイル名が表示されているか？

まずは
ここまで
登ろう

調査ポイント②

ファイル名やSTOPコード情報から
Web検索などで原因がわかる場合
が多い

それでもダメならダンプ調査

メモリダンプ (MEMORY.DMP)

- × **メモリデータとデバッグ情報が記録されたファイル**
- × **STOPエラー発生後の再起動時に生成される**

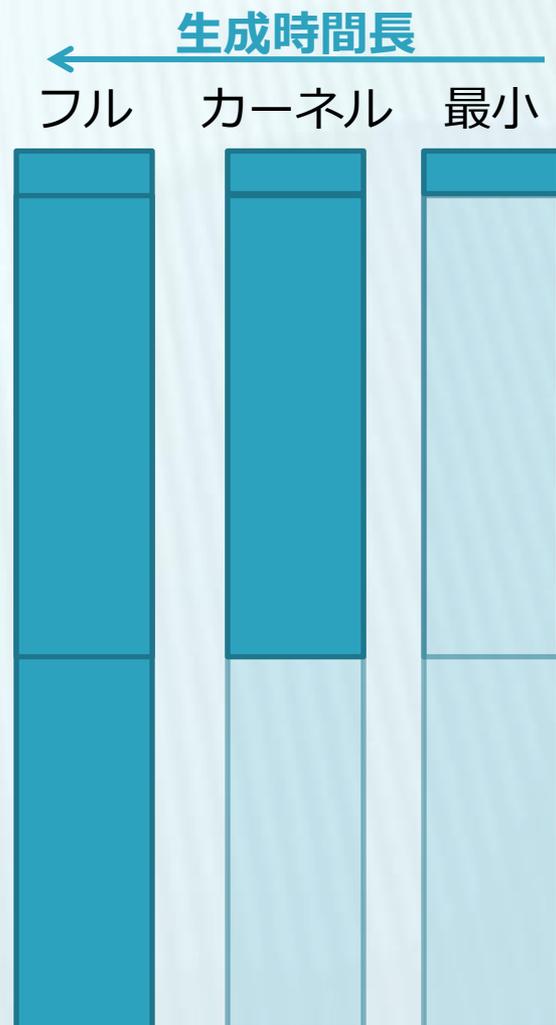
ダンプの種類

- + **フル** (物理メモリ情報すべて)
- + **カーネル** (カーネル情報のみ)
- + **最小** (最低限の情報のみ)

障害内容や許容ダウンタイムによって選ぶ

ダンプの種類を選び方

- × フルダンプ
 - + ユーザープログラムも調査対象
- × カーネルダンプ
 - + カーネルプログラムの深い調査
- × 最小ダンプ
 - + デバッグ情報のみ
 - × 詳細調査は無理
 - × 5合目までならこれで十分かも



フルダンプは2GBまで

- × フルダンプは2GBまでしか取得できない
- × 物理メモリ2GB以上のサーバーではフルダンプ取得失敗
- × どうしてもフルが必要なら、物理メモリを2GBに制限して稼働させる
 - Boot.iniで起動オプションを編集し、
/MAXMEM=2048（最大使用メモリサイズを2GB）に設定して起動

参照 KB:274568



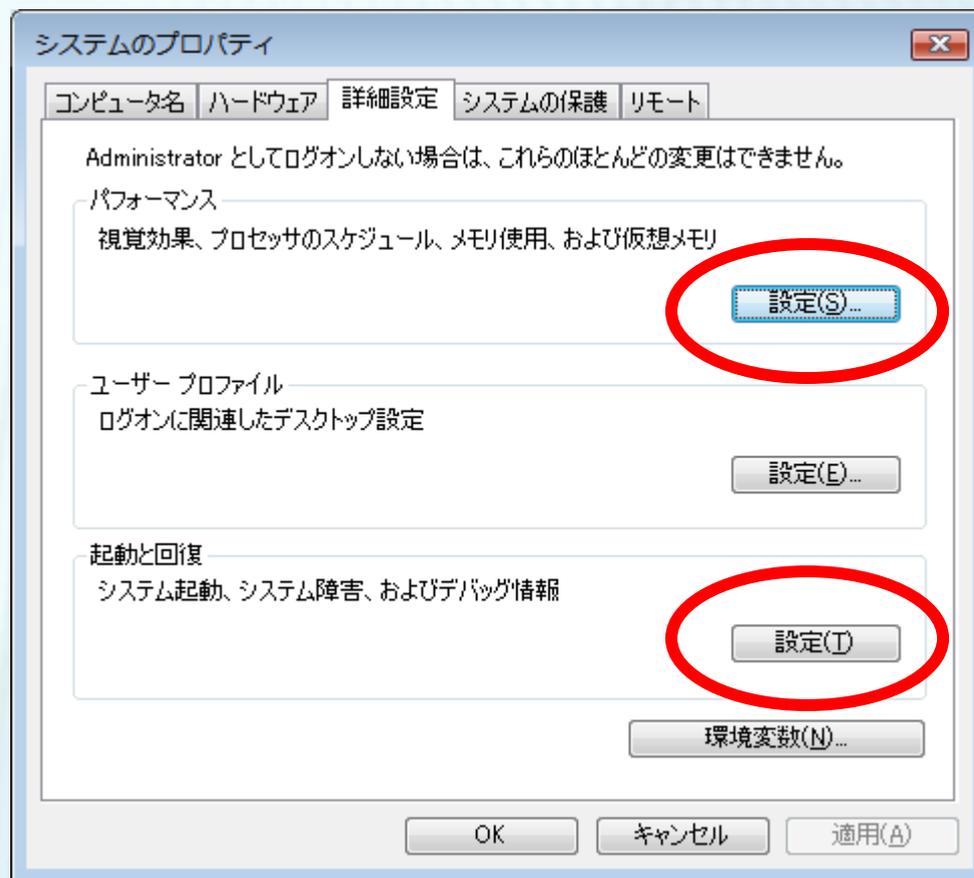
ダンプ取得設定

× システムのプロパティ

+ デバッグ情報

+ 仮想メモリ

取得の
キモ



仮想メモリサイズに注意

× 再起動前に、仮想メモリにダンプされる

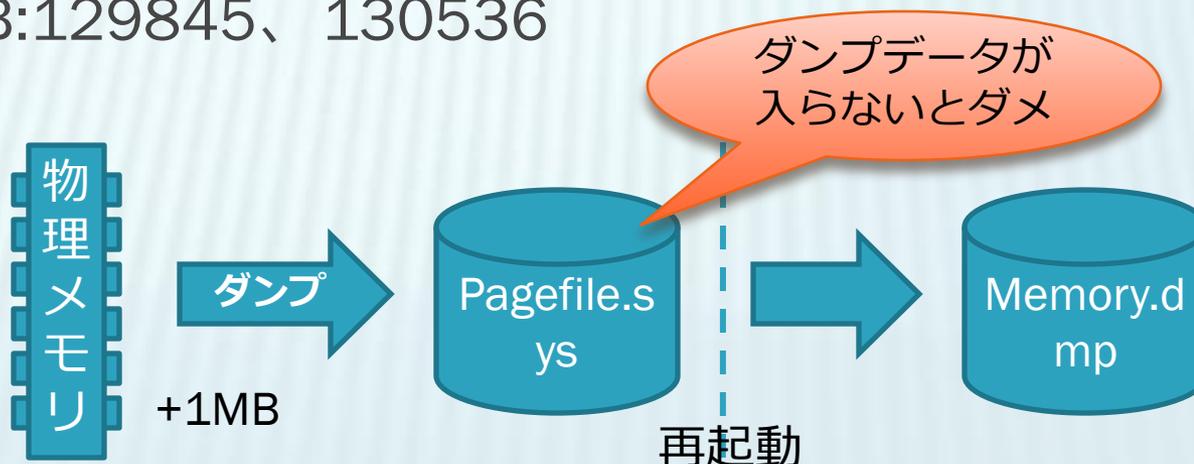
× そのため、、、

場所：**Cドライブに必ず仮想メモリを用意する**

サイズ：フルは仮想メモリの初期サイズを

物理メモリ+1MB（デバッグ情報）以上

参照 KB:129845、130536



もしダンプが取得できないなら

- × 取得設定を外している
- × 物理メモリのサイズは？
- × 仮想メモリ設定が不適切
- × Cドライブの空き領域不足
- × STOPエラー発生原因のため？
 - + I/Oまわりの問題でSTOP発生してると取れない
- × 壊れていたり、0バイトだったり
 - + dumpchk.exeで確認
 - 参照 KB:315271



手動でSTOPエラー発生

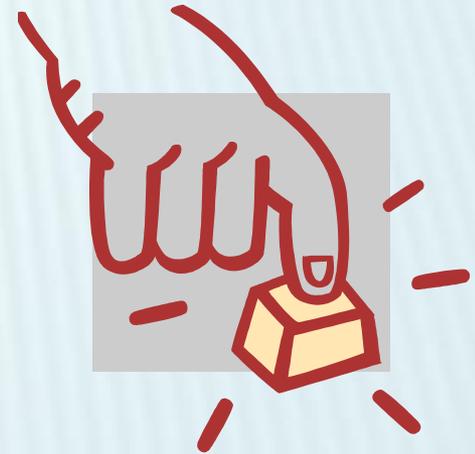
目的

- × 障害訓練（ちゃんとダンプ取れるか？）
- × **フリーズ調査**

以下のいずれかで発生

- × 特殊キー操作（レジストリ設定）
参照 KB：244139、303021
- × ツールNotmyfault（Sysinternals）

<http://download.sysinternals.com/Files/Notmyfault.zip>



Windbgでダンプ調査

- × MS社製デバッガWindbgは
さまざまなデバッグに利用可能
- × もちろん
ダンプファイルの
調査に利用できる

```
Dump C:\Windows\MEMORY-mini-BUGCODE-USB.DMP - WinDbg:6.7.0005.0
File Edit View Debug Window Help
Command - Dump C:\Windows\MEMORY-mini-BUGCODE-USB.DMP - WinDbg:6.7.0005.0
*** contain the required information. Contact the group that ***
*** provided you with these symbols if you need this command to ***
*** work. ***
*** Type referenced: nt!_KPRCB ***
*** ***
*****
MODULE_NAME: usbhub
FAULTING_MODULE: 82000000 nt
DEBUG_FLR_IMAGE_TIMESTAMP: 4549b278
DEFAULT_BUCKET_ID: WRONG_SYMBOLS
BUGCHECK_STR: 0xFE
LAST_CONTROL_TRANSFER: from 9c39f5a7 to 820d8569

STACK_TEXT:
WARNING: Stack unwind information not available. Following frames may be wrong.
87487acc 9c39f5a7 000000fe 00000008 00000006 nt!KeBugCheckEx+0x1e
87487ae8 9c39f7b9 851fc028 00000006 85f52000 usbhub+0x135a7
87487b20 9c3a4097 851fc028 00000102 0000ea60 usbhub+0x137b9
87487b4c 9c3900dc 851fc000 0000000e 851fc758 usbhub+0x18097
87487b6c 9c3a2e3c 851fc028 85f52000 00000002 usbhub+0x40dc
87487bac 9c3a1835 851fc028 00000001 851fc758 usbhub+0x16e3c
87487bcc 9c3a1ad2 851fc028 851fc758 851fc758 usbhub+0x15835
87487be8 9c39870e 851fc028 851fc758 00000007 usbhub+0x15ad2
87487c04 9c3a1bea 00000003 851fc758 00000007 usbhub+0xc70e
87487c20 9c3b28c1 851fc028 851fc758 851fc028 usbhub+0x15bea
87487c3c 9c3ac054 851fc028 851fc758 851fc028 usbhub+0x268-1
kd>
```

Windbgの準備

1. Debugging Tools for Windows をダウンロード

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

2. インストール

3. シンボル格納フォルダを作成

例 : C:¥Symbols

4. シンボル格納フォルダのパスを指定

設定場所 : Fileメニュー-Symbol File Path

例 :

SRV*C:¥Symbols*http://msdl.microsoft.com/download/symbols

参照 KB:311503

シンボルファイル

- × アドレスの番地からファンクション名（関数名）を解決するための情報が保存されている
- × 詳細な調査に使用する
- × ファンクション名から処理内容を推測するのに使える

Windowsに関するシンボルの入手先

- × シンボルサーバー（普通はサーバーを使う）
- × WHDCサイト（オフライン時の調査に）

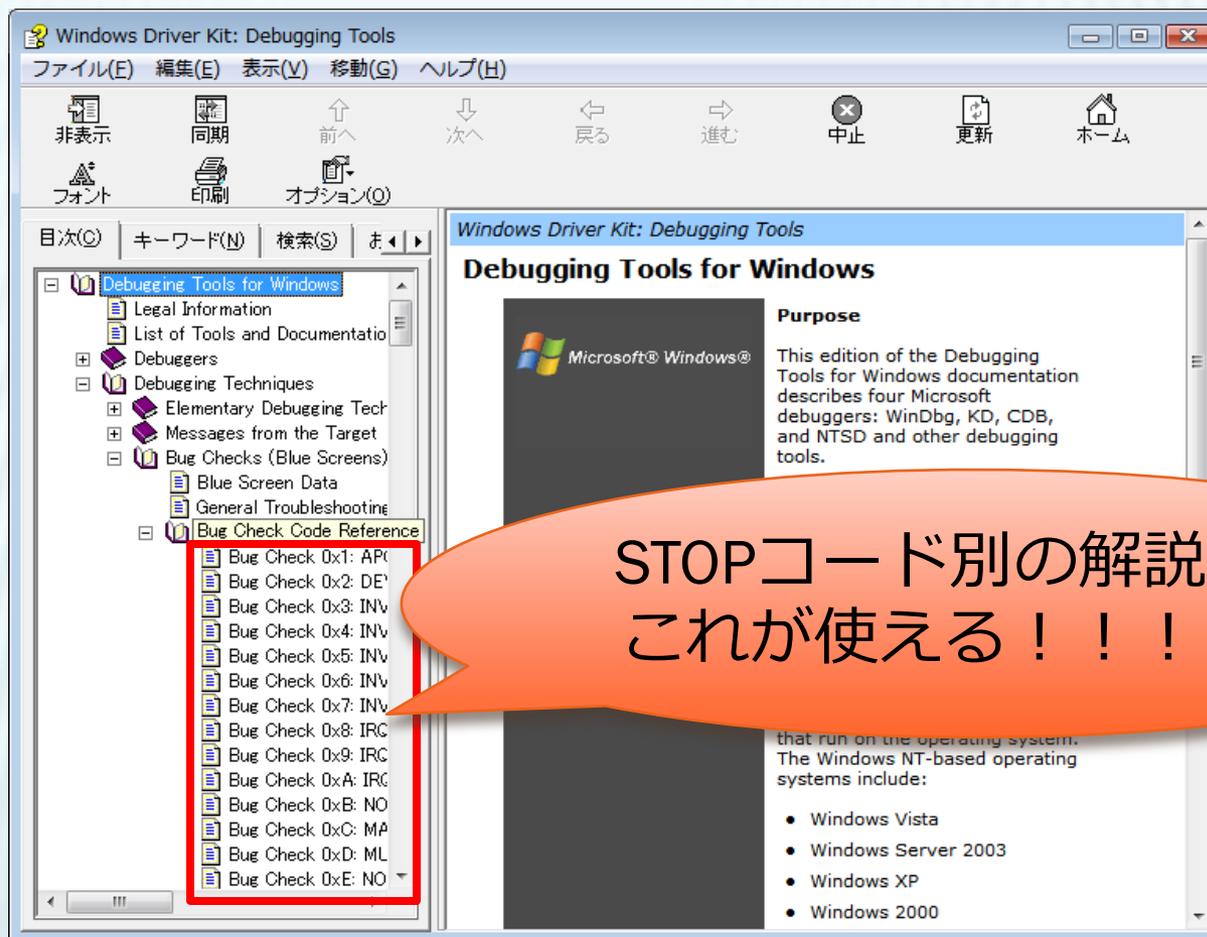
<http://www.microsoft.com/japan/whdc/devtools/debugging/symbolpkg.msp>

Windbgによるダンプの確認

- × Windbgの起動（Vistaでは管理者権限で？）
- × Fileメニュー-Open Crash Dumpでダンプファイルを開く
- × 表示内容「Probably caused by」（原因と思われるファイル名）を確認
- × !analyzeコマンドで詳細分析結果表示
 - + STOPコード詳細
 - + スタックトレースに実行されていた関数名
- × !m vコマンドでドライバのバージョンや会社名など表示
- × STOPコードについてヘルプ情報を確認

強力なDebugging Help

× Debugging Tools for Windowsのヘルプ



STOPコード別の解説あり
これが使える！！！！！！

まとめ

- × あきらめるな！見ればわかる！（かもw）
 - + 3rdベンダドライバが原因？
- × ちゃんとダンプを取得する設定にしよう
 - + 仮想メモリ設定
 - + 空き領域
- × Windbgを入れて活用しよう
 - + ヘルプの活用
 - + ドライバ情報の取得



最後に

頂上を目指すには

- × アドレス空間
 - × スレッド、プロセス
 - × ミューテックス、セマフォ
 - × Win32API
 - × アセンブラ
- ...etc



最後に

セキュリティに関する注意！

- × **フルダンプには個人情報が含まれている可能性ががあります**
 - + 個人情報を扱うシステムのS/Cならもちろん...
 - + 個人PCなら“お気に入り”などプライバシーが...
etc
- × **ダンプファイルの持ち出しには注意が必要**



参考資料 (1/2)

- × 書籍：インサイド Windows 第4版
+ 第14章クラッシュダンプ解析
- × Windows Hang and Crash Dump Analysis Mark
Russinovich

Webcast

<http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?culture=en-US&EventID=1032298076&CountryCode=US>

PPT

http://download.microsoft.com/download/0/1/3/01381C25-72DA-4AA9-B792-43E02A243C71/SVR422R_Russinovich.ppt

参考資料 (2/2)

- × 各KBへはここから
 - + マイクロソフトサポート技術情報検索
<http://support.microsoft.com/search/>

STOPコードの情報を検索する場合、
例えば、コードが0x0000000Aなら0を取った
0x000Aや0x0Aも検索すること

おわり

ご静聴

ありがとうございました