

Windowsの内部を知る

st.lain@わんくま同盟



自己紹介

- ・ ハンドル名はst. lainです
 - 以下略
- ・ エセ名古屋人です
 - 名古屋駅地下で迷子になります
- ・ ぶつ～の言語を触ってます
 - VC++ (MFC中心), C#, JScript等
- ・ 一日に「ほげ」と何回打つか知りません

アジェンダ

1. 内部を知る必要があるの？
2. Windowsアーキテクチャの概要
3. ユーザーモードとカーネルモード
4. などなど…

適当に掻き摘んでいきます！

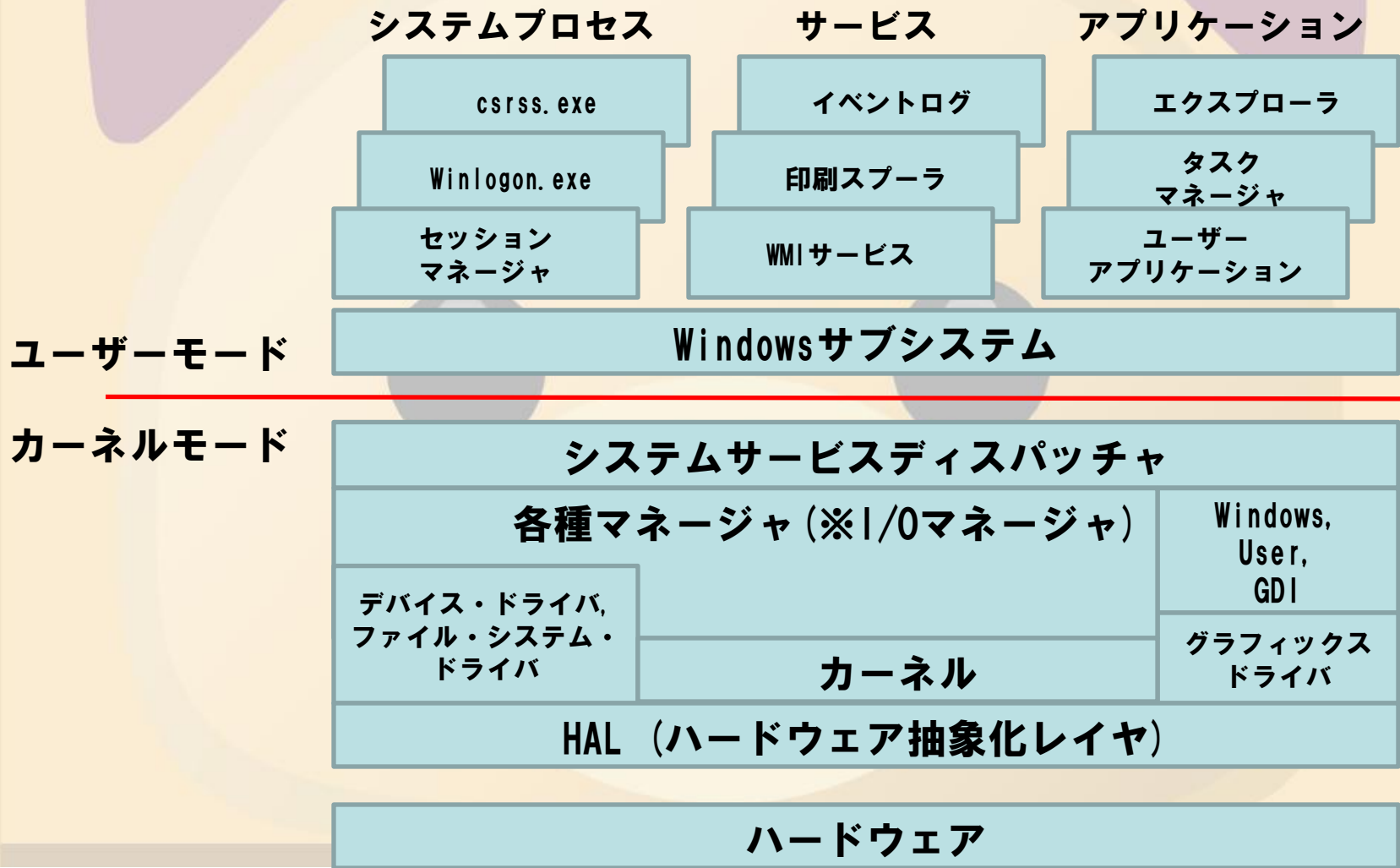
内部を知る必要があるの？

- ・ 知る必要がないかもしれませんが
 - Windows使ってて普通は困ることないですよ

でもっっっ・・・

- ・ こんな困ったところありませんか？
 - プロセス動かしてないのに、あっごい重いの
 - 何もしてないのにリブートかかっちゃった
 - 同上、青画面 (BSOD) が表示されちゃった

Windowsアーキテクチャの概要



ユーザーモードとカーネルモード

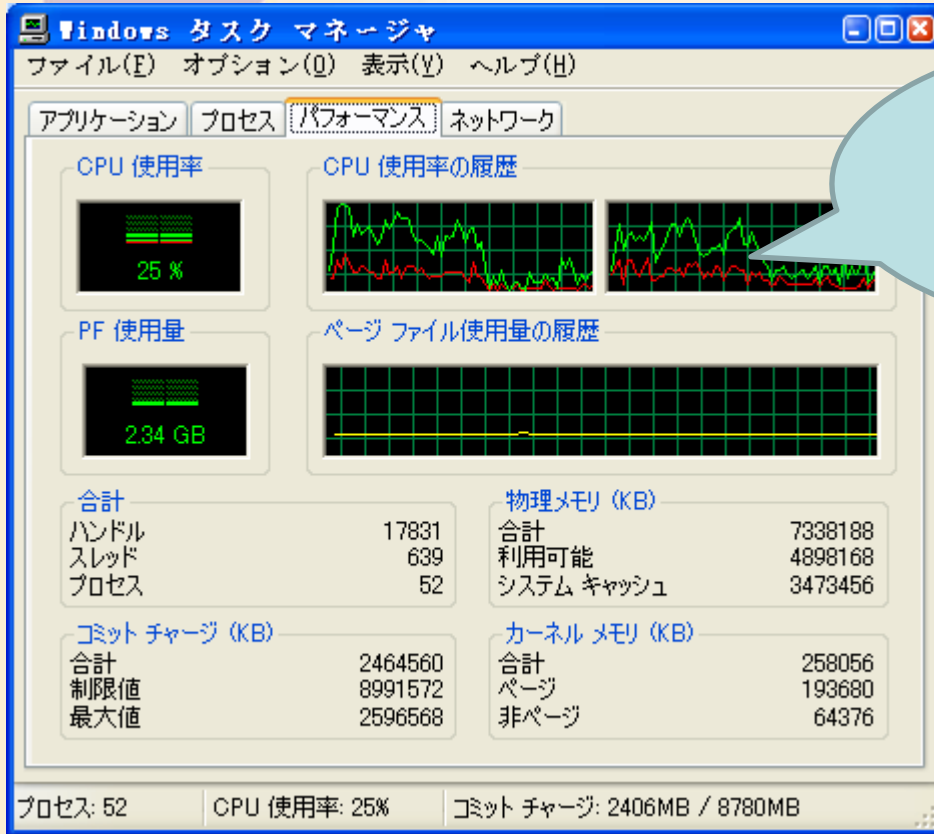
・ユーザーモード

- 普通によく使うモード。デスクトップでアプリを起動したい。
- 変なアプリを起動しても早々にWindowsがハングアップされることはありません(多分)

・カーネルモード

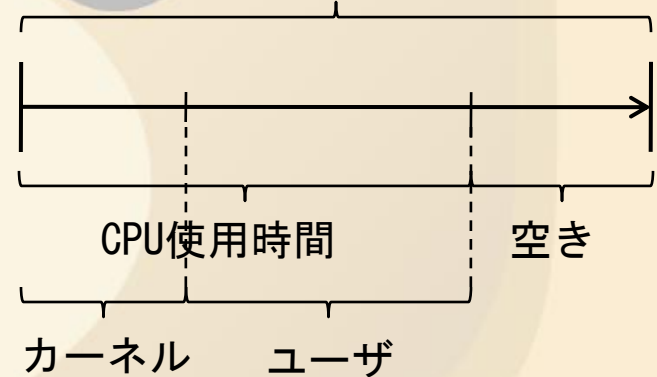
- ユーザーが意識しないところで使われているモード。
- ここで異常(例えばメモリ違反)があるとWindowsが落ちます

タスクマネージャで確認



赤い部分が
カーネル使用時間

単位時間(全体)



CreateFileの例

MyApplication.exe

アプリケーション上でCreateFileを呼び出し

Windowsサブシステム上のNtCreateFileを呼び出し

ユーザーモード

カーネルモード

SSDT上のZwCreateFileを呼び出し

I/OマネージャがIRP_MJ_CREATEを発行

各種ドライバが要求を処理

アプリケーションでの例.1

- SysinternalsのFileMon, RegMonあたりが有名です

The image shows two windows from Sysinternals. The left window is PE Explorer, displaying the resources of a file. The right window is File Monitor, showing a log of system events.

PE Explorer Resources:

- BINRES
 - RFILEMSYS
 - RFILEMSYSX64
 - RFILEMXXD
- Cursor Entry
- Bitmap
- Icon Entry
- Menu
- Dialog
- String
- Accelerators
- Group Cursor
- Group Icon
- Version
- Manifest

File Monitor Log:

#	Time	Process	Request	Path	Result	Other
29952	11:32:29	POWERPM...	SET INFORMATION		SUCCESS	Length: 5632
29953	11:32:29	POWERPM...	SET INFORMATION		SUCCESS	Length: 5632
29954	11:32:29	POWERPM...	CLOSE		SUCCESS	
29955	11:32:29	POWERPM...	OPEN		SUCCESS	Options: Open Access...
29956	11:32:29	POWERPM...	OPEN		SUCCESS	Options: Open Directo...
29957	11:32:29	POWERPM...	QUERY INFORMATION		SUCCESS	FileAttributeInfor...
29958	11:32:29	POWERPM...	DELETE		SUCCESS	
29959	11:32:29	POWERPM...	CLOSE		SUCCESS	
29960	11:32:29	iexplor...	QUERY INFORMATION		SUCCESS	Attributes: A
29961	11:32:24	iexplor...	QUERY INFORMATION		NOT FOUND	Attributes: Error
29962	11:32:24	iexplor...	QUERY INFORMATION		SUCCESS	Attributes: A
29963	11:32:24	iexplor...	QUERY INFORMATION		NOT FOUND	Attributes: Error
29964	11:32:25	iexplor...	QUERY INFORMATION		SUCCESS	Attributes: A
29965	11:32:25	iexplor...	QUERY INFORMATION		NOT FOUND	Attributes: Error
29966	11:32:26	explore...	QUERY INFORMATION		SUCCESS	Attributes: A
29967	11:32:26	explore...	OPEN		SUCCESS	Options: Open Access...
29968	11:32:26	explore...	QUERY INFORMATION		SUCCESS	Length: 1724416
29969	11:32:26	explore...	CLOSE		SUCCESS	
29970	11:32:27	iexplor...	QUERY INFORMATION		SUCCESS	Attributes: A
29971	11:32:27	iexplor...	QUERY INFORMATION		SUCCESS	Attributes: A
29972	11:32:28	iexplor...	QUERY INFORMATION		NOT FOUND	Attributes: Error
29973	11:32:28	iexplor...	QUERY INFORMATION		SUCCESS	Attributes: A
29974	11:32:28	iexplor...	QUERY INFORMATION		NOT FOUND	Attributes: Error
29975	11:32:28	iexplor...	QUERY INFORMATION		NOT FOUND	Attributes: Error
29976	11:32:30	iexplor...	QUERY INFORMATION		SUCCESS	Attributes: A
29977	11:32:30	iexplor...	QUERY INFORMATION		SUCCESS	Attributes: A
29978	11:32:31	winlogo...	QUERY INFORMATION		NOT FOUND	Attributes: Error
29979	11:32:31	winlogo...	QUERY INFORMATION		NOT FOUND	Attributes: Error
29980	11:32:31	winlogo...	QUERY INFORMATION		NOT FOUND	Attributes: Error
29981	11:32:31	winlogo...	QUERY INFORMATION		NOT FOUND	Attributes: Error
29982	11:32:31	winlogo...	QUERY INFORMATION		NOT FOUND	Attributes: Error
29983	11:32:31	winlogo...	QUERY INFORMATION		NOT FOUND	Attributes: Error
29984	11:32:31	winlogo...	QUERY INFORMATION		NOT FOUND	Attributes: Error
29985	11:32:31	winlogo...	QUERY INFORMATION		NOT FOUND	Attributes: Error
29986	11:32:31	winlogo...	QUERY INFORMATION		NOT FOUND	Attributes: Error
29987	11:32:31	iexplor...	QUERY INFORMATION		SUCCESS	Attributes: A
29988	11:32:32	iexplor...	QUERY INFORMATION		NOT FOUND	Attributes: Error
29989	11:32:32	iexplor...	QUERY INFORMATION		NOT FOUND	Attributes: Error

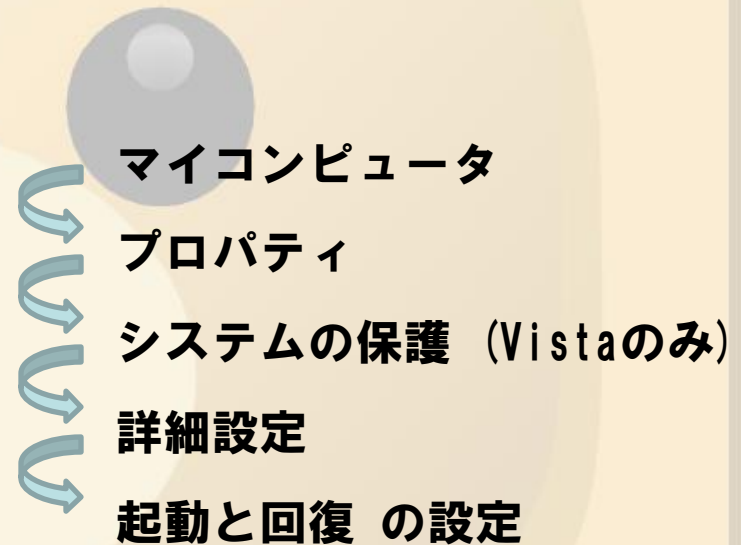
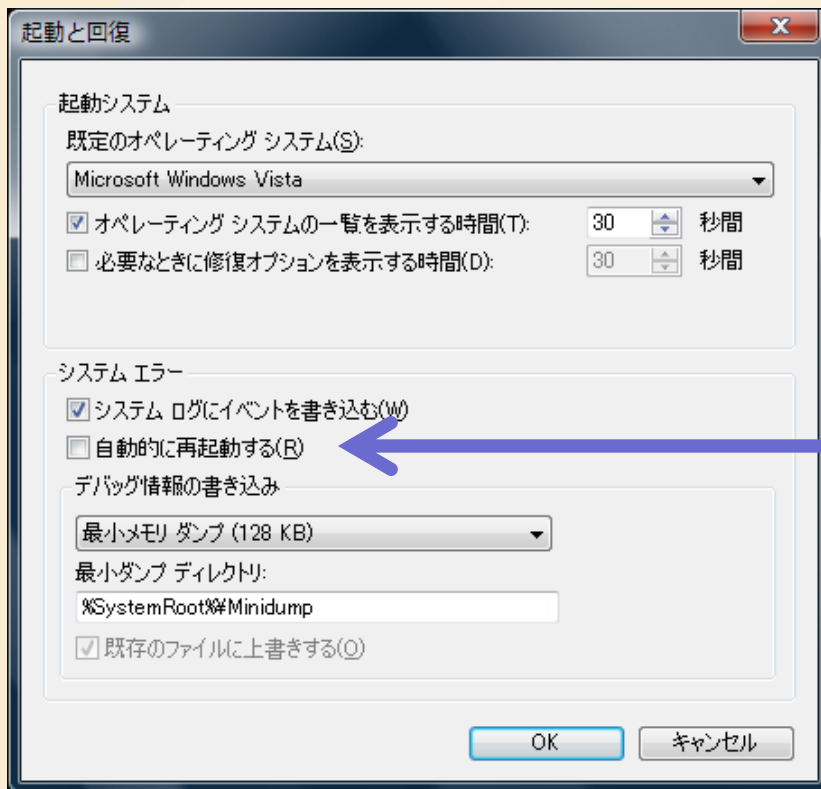


アプリケーションでの例.2

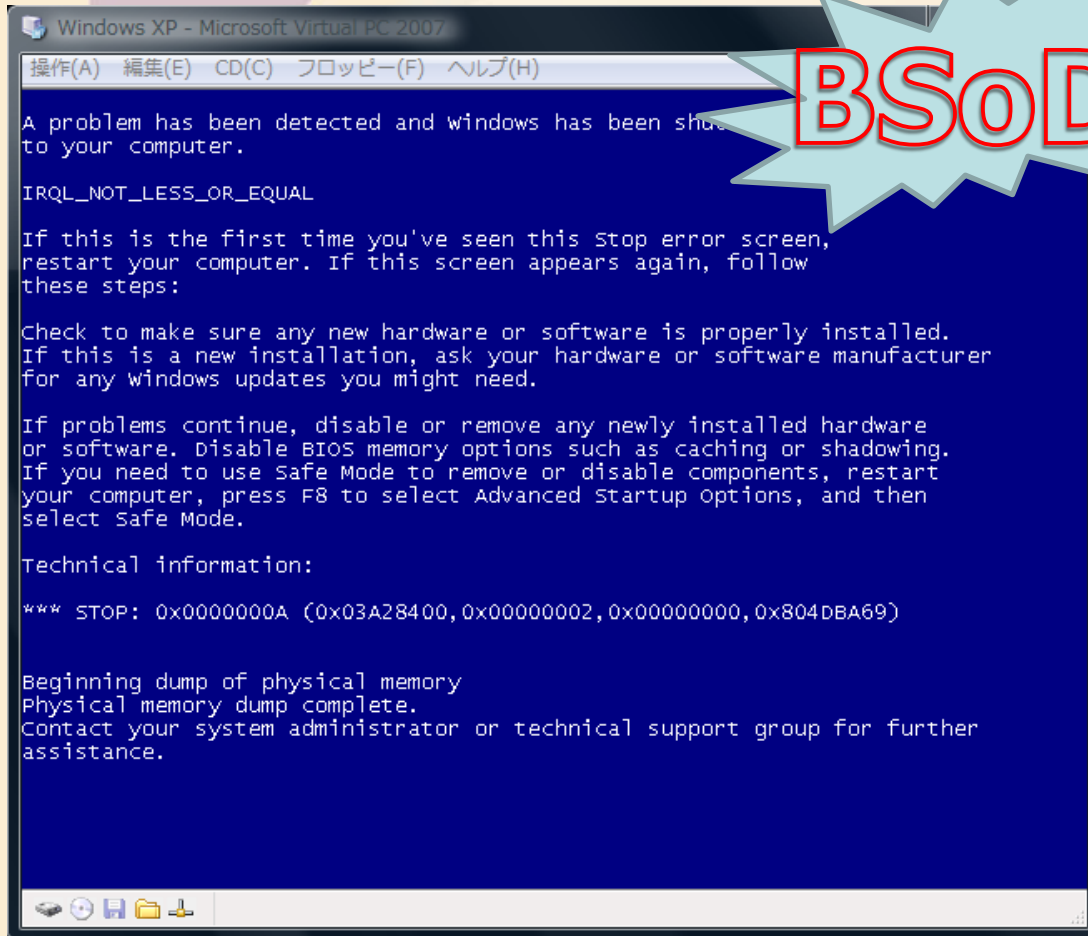
- ・ アンチウイルスソフトウェア
 - OneCareなど
- ・ 暗号化ドライブ等のソフトウェア
 - Vista搭載のBitLockerとか
- ・ 各種監視ソフト
 - USBメモリを挿したりすると…

何もしてないのにリブート?

- WindowsXP以降ではBSODが表示されようがあると自動的にリブートがかかります



自動再起動オプションを落とすと



BSOD!

STOP: 0x0000000A

エラー理由 - 関数呼び出し時のIRQLが高すぎます

第1引数 0x03A28400

不正参照のアドレス

第2引数 0x00000002

違反時のIRQL = DISPATCH_LEVEL

第3引数 0x00000000

メモリ操作 0=読み取り時

第4引数 0x804DBA69

違反を起こした命令アドレス



よくある?STOPエラー

Error Code	Message	内容
0x00000002	DEVICE_QUEUE_NOT_BUSY	デバイスの待ち行列がビジーであると予想されていたのにそうではなかったことを示しています
0x0000000A	IRQL_NOT_LESS_OR_EQUAL	ページ可能なメモリへのタッチ試行したプロセス割り込み要求レベル(IRQL)が高すぎることを示しています。通常、このエラーは不当なアドレスを使っているドライバによって引き起こされます。
0x0000000E	NO_USER_MODE_CONTEXT	中身のないユーザー モードを入力しようとしたことを示しています
0x00000012	TRAP_CAUSE_UNKNOWN	トラップの原因が不明であることを示しています
...	...	

引用元 <http://park12.wakwak.com/~iktryc/diary/2005/stoperror.html>



参考文献

- ・ **インサイドWindows 第4版**
 - Microsoft Press出版, David Solomon, Mark Russinovich著
- ・ **Windows Vistaカーネルの内部**
 - <http://technet.microsoft.com/ja-jp/magazine/cc162494.aspx>
- ・ **STOPエラー一覧**
 - <http://park12.wakwak.com/~iktryc/diary/2005/stoperror.html>
- ・ **etc...**