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
- ふつ～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…

適当に掻い摘んでいきます！

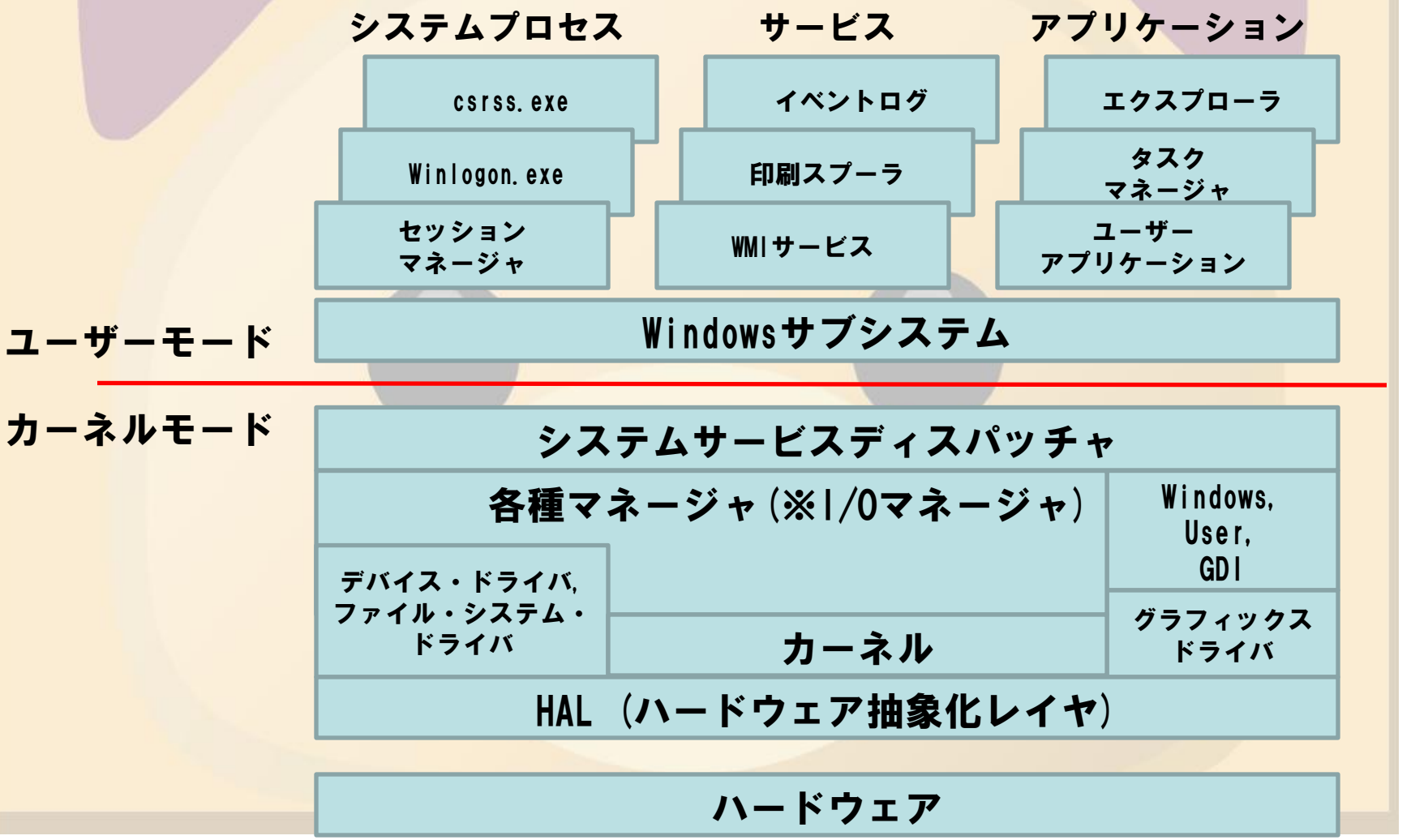
内部を知る必要があるの？

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

でもっつっつ・・・・

- こんな困ったころありませんか？
  - プロセス動かしてないのに、すっごぃ重いの
  - 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

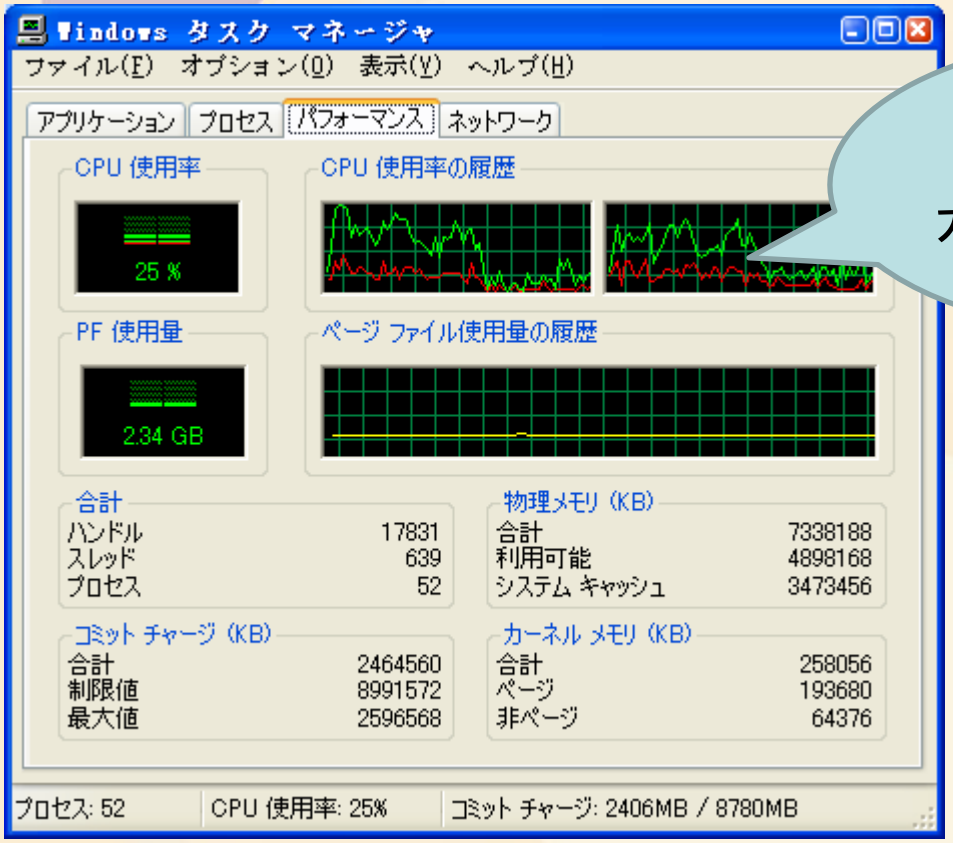
Windowsアーキテクチャの概要



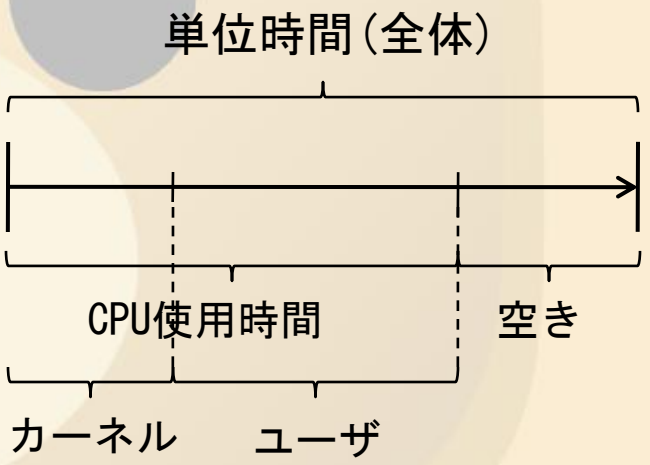
ユーザーモードとカーネルモード

- 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り。
  - 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

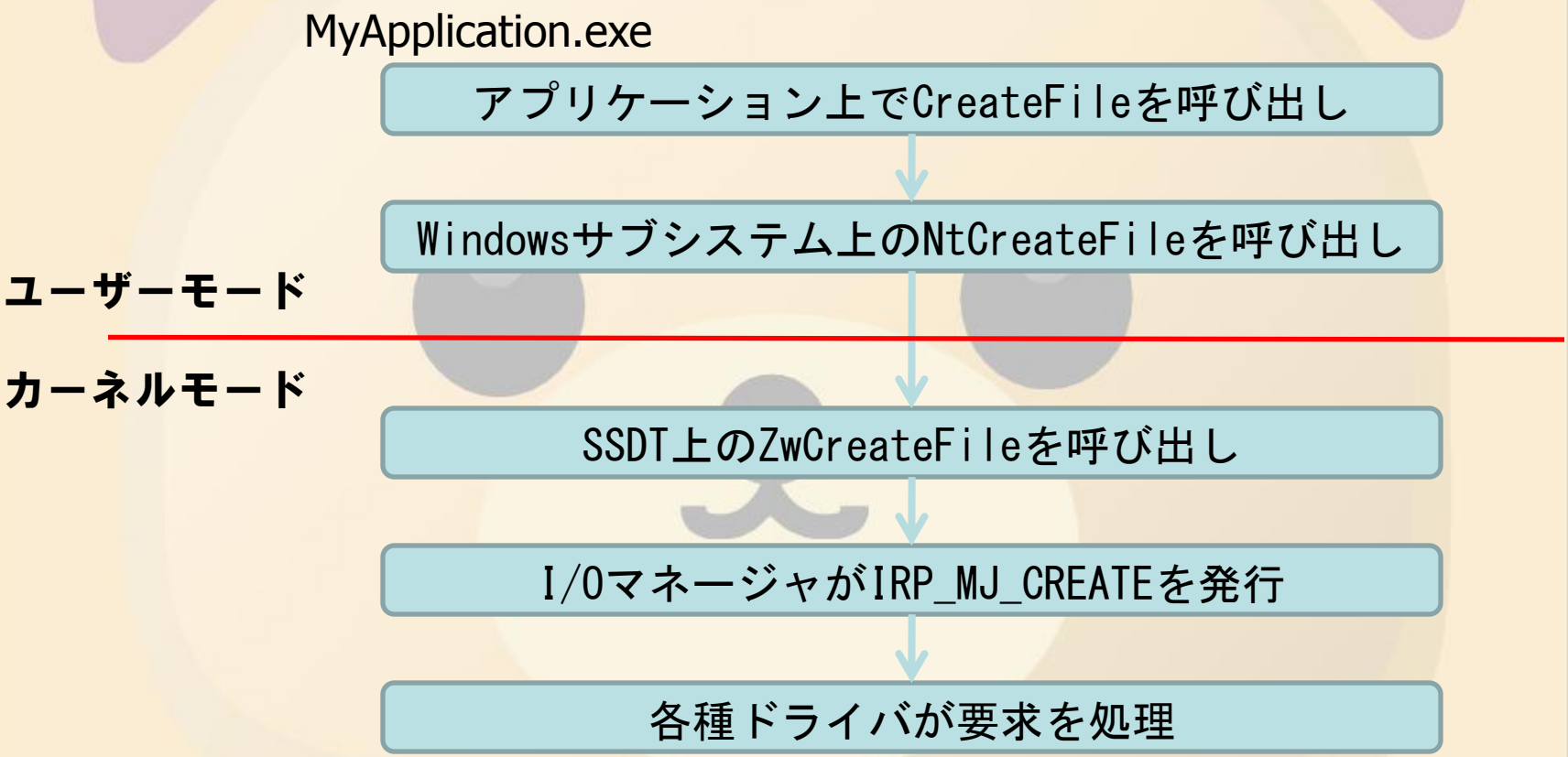
タスクマネージャで確認



赤い部分が
カーネル使用時間

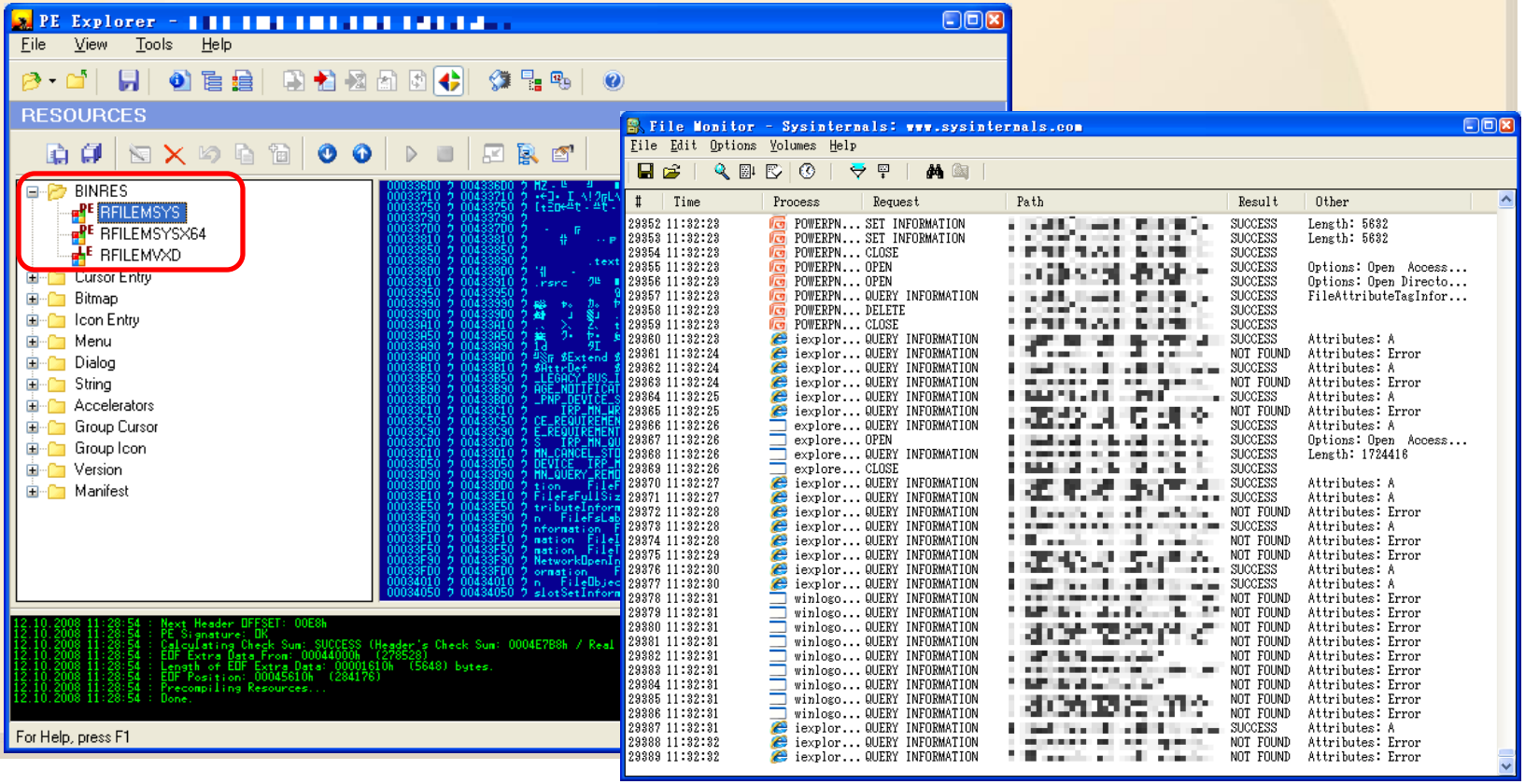


CreateFileの例



アプリケーションでの例.1

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

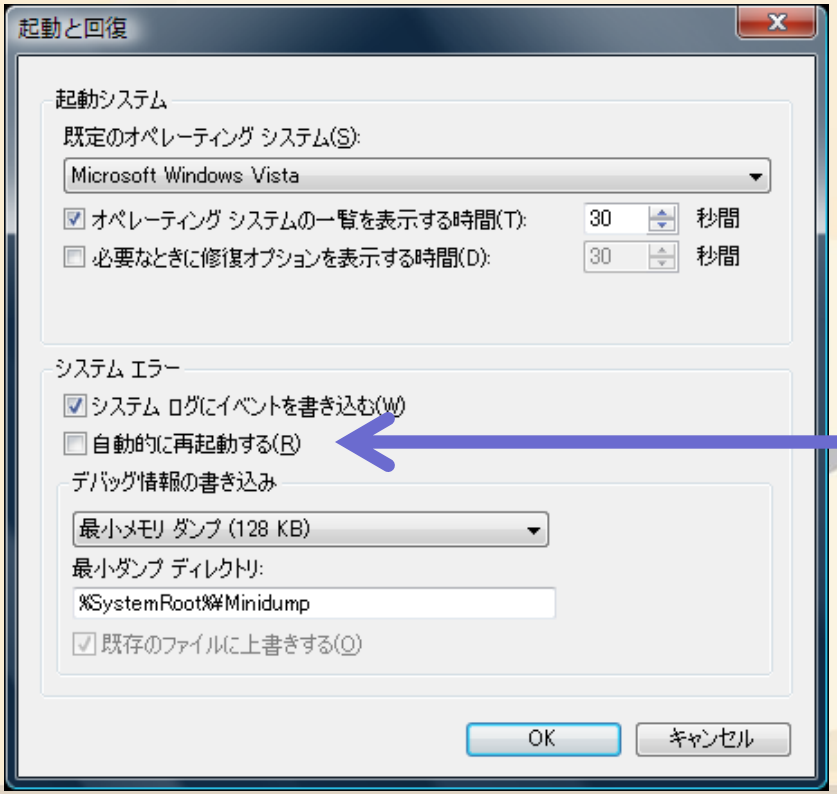


アプリケーションでの例.2

- アンチウィルスソフトウェア
  - 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が表示されようとすると自動的にリブートがかかります



マイコンピュータ

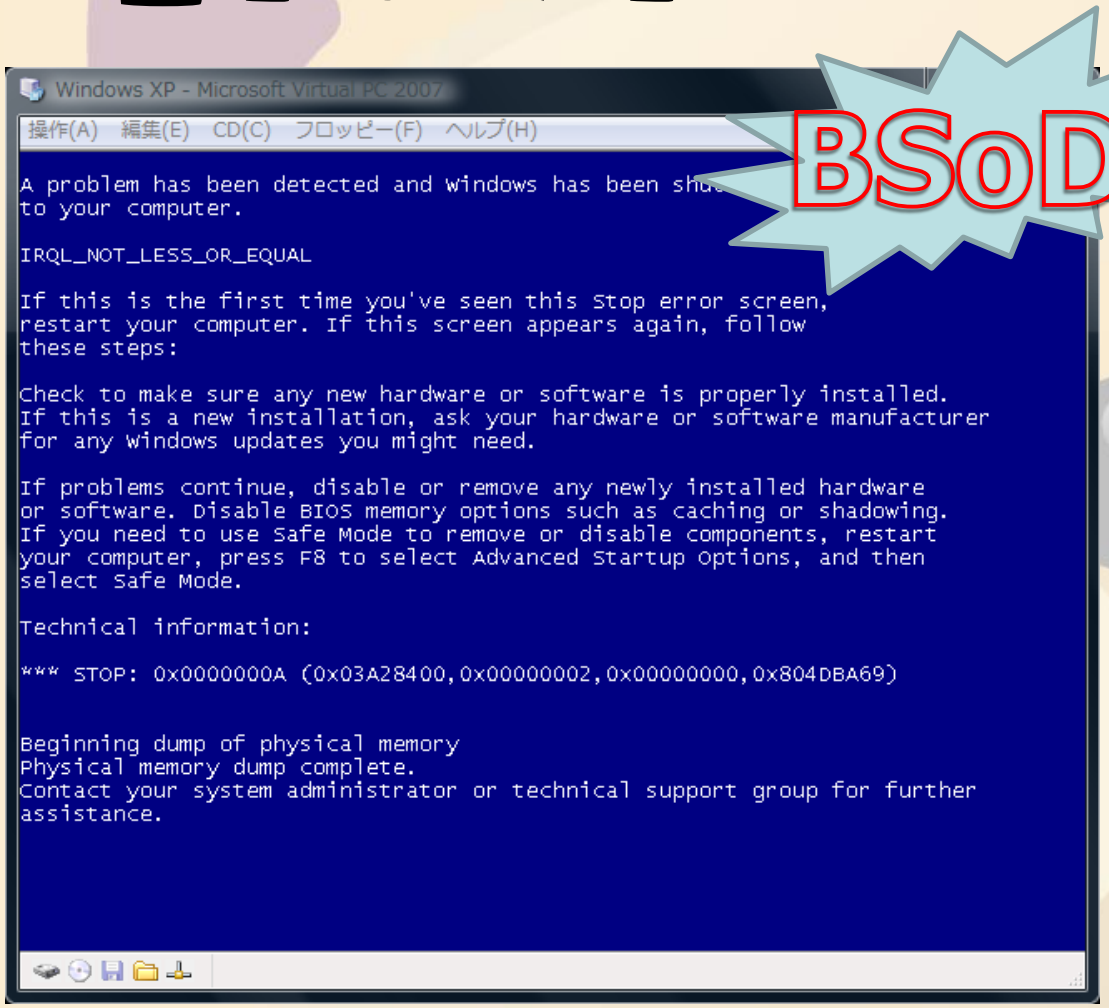
プロパティ

システムの保護 (Vistaのみ)

詳細設定

起動と回復 の設定

自動再起動オプションを落とすと



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…