This is CLR vol.2

アジェンダ

- 本日使うツールの紹介
- ネイティブPEファイル
- C++/CLI PEファイル
- マネージPEファイル
- おまけ

本日使うツール

- dumpbin.exe

dumpbin.exe

- 実行可能ファイル（PE - Portable Executableファイル)の内容を調べるもの。Windows SDK や Visual Studio に含まれる

調査できる事

- PEファイルのヘッダ情報
- TLSの構造体、コールバック関数
- PEファイルがエクスポートしている関数
- インポートしている関数とモジュール
- 逆アセンブル
- etc…。他、ヘルプ参照。

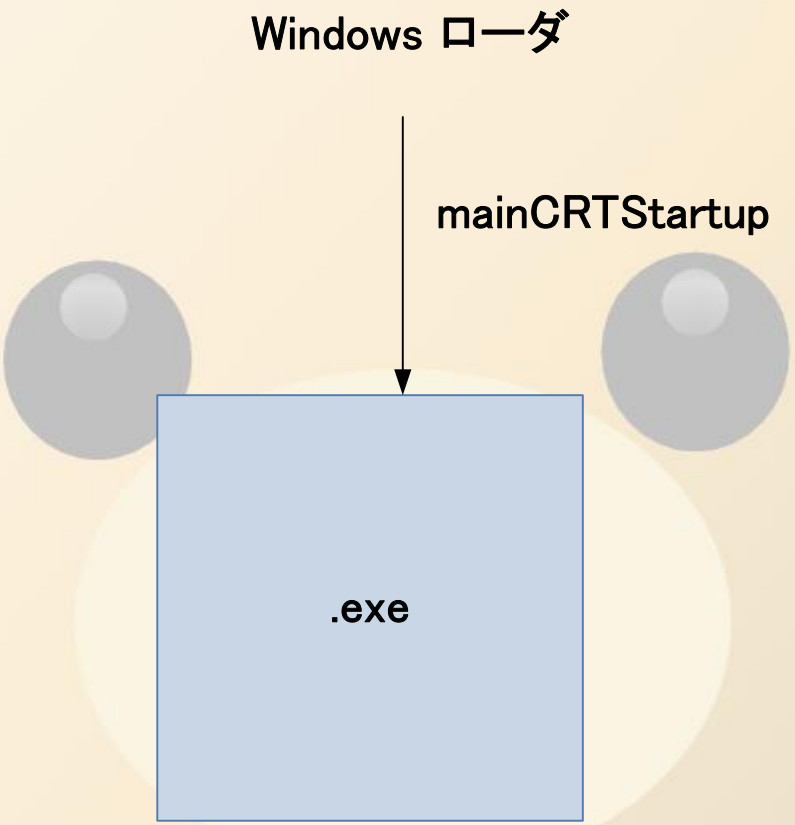
Dependency Walker

- dumpbin.exe /imports の内容を再帰的に表示してGUIで表示するもの
- 単体ダウンロードするか、Windows SDK、Visual Studio に含まれる

ネイティブPEファイルをdumpbin

- DEMO

mainCRTStartUp



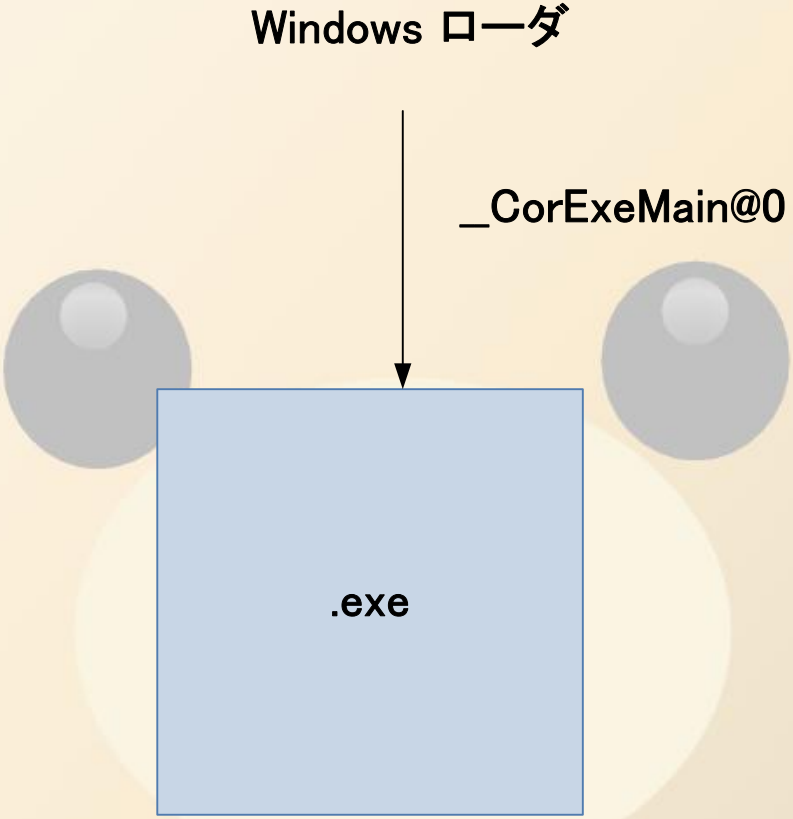
CRTのスタートアップコードを読む

- DEMO

C++/CLIのPEファイルをdumpbin

- DEMO

__CorExeMain@0



マネージPEファイルをdumpbin

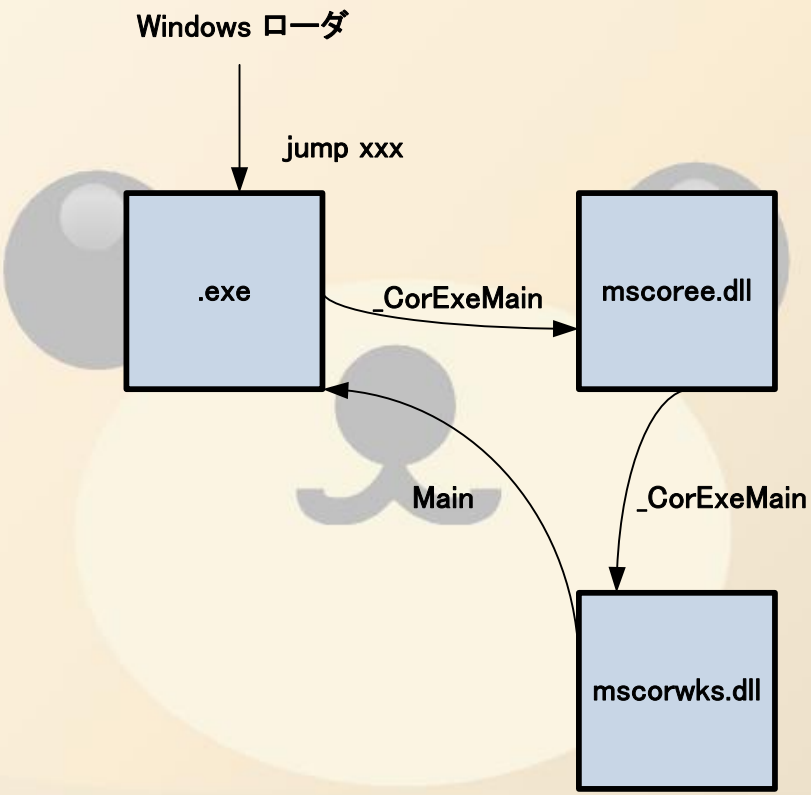
- DEMO

mscoree.dllとは

- アンマネージ実行ファイルが実行された際、最初に呼ばれる関数「_CorExeMain」をエクスポートしている。
- DLLの場合は「_CorDllMain」。
- CLRではない。
- CLRへ処理を移譲する前の「シム」と呼ばれる。
- %SYSTEMROOT%system32 にインストールされる。
- 常に最新バージョンのmscoree.dllが上書きインストールされる（side-by-sideではない）。

- .NET Framework がインストールされていない環境で .NET アプリケーションを実行すると「mscoree.dllが見つかりません」というエラーが表示される。

マネージPEファイルのロード



mscorwrk.dll

- CLR本体
- .NET Frmework のバージョン毎にインストールされる(side-by-side)。
- ワークステーション版（mscorwrk.dll）とサーバー版（mscorsrv.dll）がある。
- .NET Framework 2.0 からサーバー版はない？おそらく一つに統合されている？ 2.0 の mscorwrk.dll のサイズが 1.x の 2倍以上になっていることから一つのファイルで切り替え？

SSCLIを読む

- DEMO

おまけ

- mscorlib.dll、System.dll などの .NET Framework のアセンブリは、どうして2箇所にインストールされるのか。

単にコンパイルするときに便利

- GACのディレクトリ構造は強烈に複雑