【WIP】

x86_64 アセンブリでのライフゲームの実装

Arch B2
tatsu
親:

背景

- OSやセキュリティに興味があったが、勉強する過程で出てきたバイナリ及びアセンブリを理解することができなかった。

- そこで、アセンブリを自分で書くことで、理解を進めたかった。

手法

- x86_64アーキテクチャのアセンブリで、ライフゲームを実装する。

- ただし、コンパイラから生成されたアセンブリからのコピペはしない。

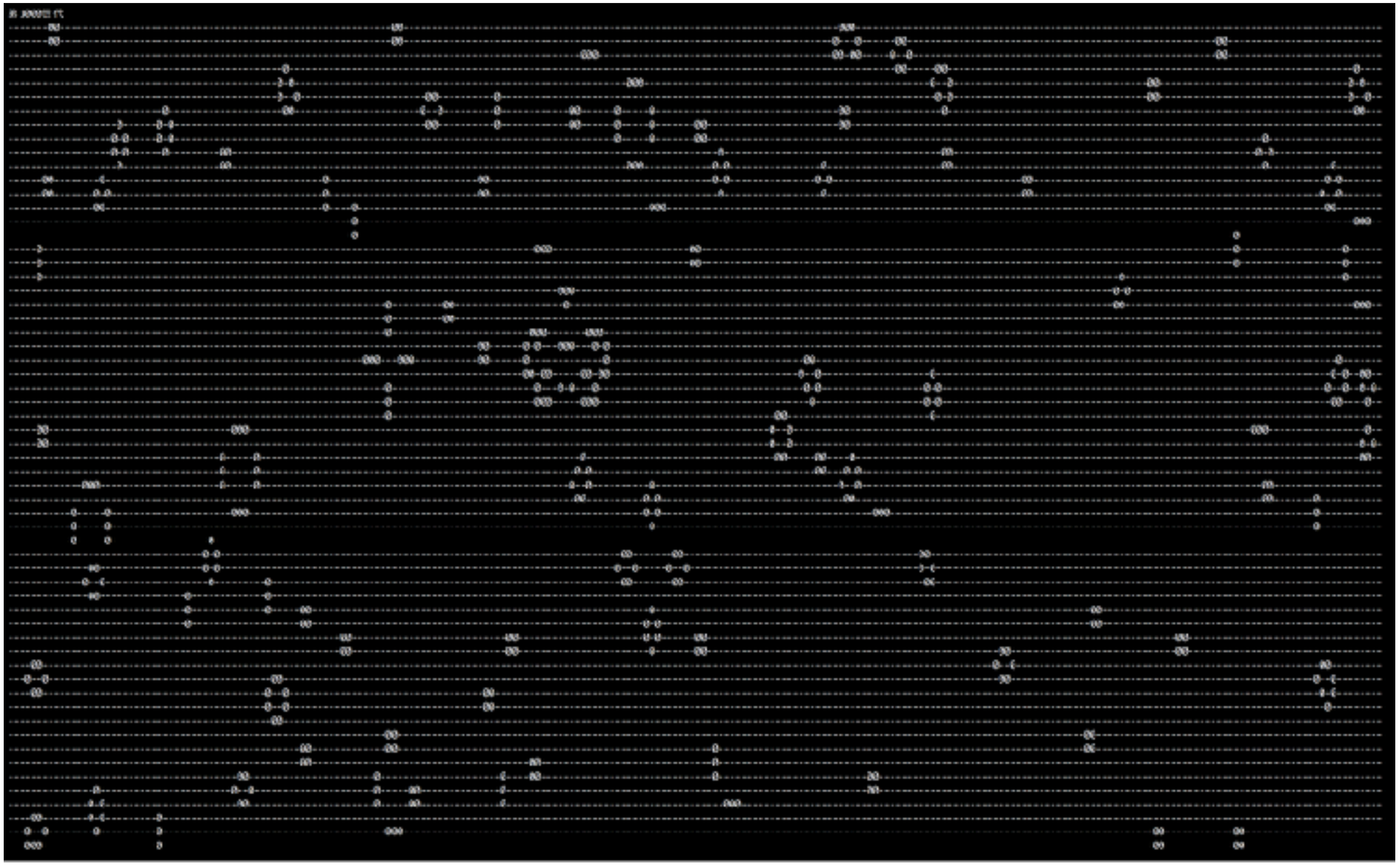
- 全部自分で書く。

工程

- Cでライフゲームを書き、ロジックを確認する。
  https://github.com/doooooooooingggggg/lifegame/blob/master/lifegame.c
- このコードを参考に、フルスクラッチでアセンブリを書いていく。
- 書いたコードを、nasmを用いてアセンブルし、
  `ELF 64-bit LSB relocatable`なオブジェクトファイルを生成
- ld で、データをリロケートし、シンボルの参照をまとめる。
- 実行

実装

- Cでの実装を実行した結果



実装

アセンブリでの実装

- 暫定で、現在の進捗。
- 必要そうな処理を考えてみたところ、
    - printf
    - 分岐
    - ループ
    - 配列の操作
    - 関数ジャンプ
    - sleep
- 以上を組み合わせて、頑張る。

アセンブリでの実装

- 暫定で、現在の進捗。
- 必要そうな処理を考えてみたところ、
    - printf -> システムコールのwriteを使うことで解決
    - 分岐 -> cmpで解決
    - ループ -> 今ここ
    - 配列の操作
    - 関数ジャンプ
    - sleep
- 以上を組み合わせて、頑張る。

参考文献

- 「Jun's Homepage」http://www.mztn.org/index.html
- 「原書で学ぶ64bitアセンブラ入門」
  http://warabanshi.hatenablog.com/search?q=%E5%8E%9F%E6%9B%B8%E3%81%A7%E5%AD%A6%E3%81%B6