

# コードサーチ

---

- コードサーチ
    - 数値サーチ
    - 変動値サーチ方法
    - メモリサーチ
    - CGなどのフラグ系コードサーチ
    - 変動アドレス対応ポインタコード
    - プログラムサーチ
- 

## 数値サーチ

主に値がゲーム内で表示されてる場合に使われるサーチ方法です

1. CWCheatの起動「Cheat searcher」を選択
  2. 「start a new search for a fixed value」を選択
  3. 検索する数値に合わせて ボタンでデータタイプを変更
    1. 8bit = 0 ~ 255
    2. 16bit = 0 ~ 65,535
    3. 32bit = 0 ~ 4,294,967,295
  4. ゲーム上で表示されている数値（金・経験値・ステータス等）を10進で入力
  5. ×ボタンでサーチ開始
  6. しばらくするとサーチにヒットしたアドレスの個数が表示される
  7. 数が多い場合は一度ゲームに戻り数値を変動させる
  8. 再度CWCheatを起動させ「Cheat searcher」を選択
  9. 「continue a search for fixed value」を選択
  10. 変動させた数値を入力し×ボタンでサーチを開始する
  11. 7~10を繰り返し個数が減ったら ボタンを押しアドレスを選択し×ボタン
  12. 変更させたい数値を入力して×ボタンを押せばコードが登録される
- 

## 変動値サーチ方法

1. CWCheatの起動「Cheat searcher」を選択
2. 「start a new search for a difference」を選択
3. 512kbの空きカーネルラムスペース、MSに25MBの空きスペースが必要  
; ボタン で、8,16,32bit \*1 のデータタイプを選択
4. ゲームに戻って、値が変わるようにゲームを進める  
;再度CWCheatを起動、「continue a new search for a difference」を選択
5. 変動サーチで2度目以降のサーチをする際はいくつか検索のやり方を選ぶことができる

ツール内の名称	直前にサーチした数値と比較して式(n,現在値/X,前回サーチ値)	
equal to before	同じ数値を検索	n = X
different than before	異なる数値を検索	n X
less than before	小さい数値を検索	n < X
greater than before	大きい数値を検索	n > X
less by than before	数値以下の数値を検索	n X
greater by than before	数値以上の数値を検索	n X

---

## メモリスーチ

数値や変動値サーチでとりあえずなんかアドレスを割り出す。memory editor でそのアドレス周辺をてきと~に書き換えてみる。HPならステータス関係なんかが見つかることが多い。CWCの0xCずつのメモリエディタが使いづらい人は他のものを使ってみるとよいかも？メモリエディタ

CWCのメモリエディタを「0xCずつ表示」から「0xFずつ表示」に変えることもできなくはない。

(CWC 0.2.2 REV.D で動作確認済み)

設定の仕方は2種類あるので、好きな方を選んでほしい。

どちらの場合もPSPの ms0:/seplugins/cwcheat/CWCHEAT.INI の内容を少し書き換える。  
(お約束だが、書き換えは自己責任で)

パターンA:

MEMEDIT BYTES= 13 を MEMEDIT BYTES= 16 に、  
ASCII ENABLE= 1 を ASCII ENABLE= 0 に書き換える。  
「0xFずつ表示」になる代わりに、ASCII表示はなくなる。

パターンB:

MEMEDIT BYTES= 13 を MEMEDIT BYTES= 16 に、  
MEMEDIT SPACE= 1 を MEMEDIT SPACE= 0 に書き換える。  
「0xFずつ表示」になる代わりに、1byte毎の区切りスペースはなくなる。

パターン番外:

MEMEDIT BYTES= 13 を MEMEDIT BYTES= 8 に書き換える。  
「0x8ずつ表示」になるので「0xCずつ表示」よりは使いやすくなる。  
但し、一画面毎のデータ量が (13\*25=) 325byteから (8\*25=) 200byteに減る。

「どれもヤダー」という人は...、自分で何とかしてください。

2009/01/18 13:30 MIB@Chiba

---

## CGなどのフラグ系コードサーチ

メモリダンプか復号化済みセーブデータをヘキサエディタ等でとにかく比較する。セーブデータで判明したらメモリダンプで似たようなところをさがせばOK。

---

## 変動アドレス対応ポインタコード

<http://sanik.imk.cx/nitePR/> に入ってるDMA(=Dynamic Memory Allocation) Hunterを使う。変動アドレスとその時にとったメモリダンプを比較することによりポインタアドレスを割り出すことが簡単に出来る。CWC公式0.2.2から似たような鶴同梱。使い方はDMAHUNTERとほぼ同じ。自動コード生成があるがbitの指定が間違ってるようなので注意。多重変動するものはDMAHUNTER同様出ません。

- [http://www.dannis.hk/wp/?page\\_id=322](http://www.dannis.hk/wp/?page_id=322)

---

## プログラムサーチ

数値サーチなんかでアドレスを割り出す。下の改造版PSPLINKを使い絶対アドレスでHardwareBreakPointを設置する。ブレイクしたところをディスアセンブラで確認し、あやしそうなところを弄る。

<http://www.sendspace.com/file/oilihs>