过程

汇编语言把过程定义为以返回语句结束的命名语句块。

- 使用PROC和ENDP伪指令来声明过程
- 必须定义一个过程名字（标识符）

```
main PROC
MOV EAX, 1000h
MOV EBX, 1000h
MOV ECX, 1000h
CALL MyProc
INVOKE ExitProcess, 0
main ENDP
MyProc PROC
ADD EAX, EBX
ADD EAX, ECX
RET
MyProc ENDP
```

- 除启动过程之外，其它过程以ret指令结束
- 将CPU控制权转移到过程被调用的地方

启动过程（main）

- 启动过程（main）的返回语句是 `INVOKE ExitProcess, 0`
- 将CPU的控制权转移给Windows操作系统

过程的调用与返回

- CALL指令将CPU的控制权转移到新的内存地址执行指令，实现过程的调用
- RET指令将CPU的控制权返回到程序中过程被调用的地方继续执行

- 过程返回地址的保存
    - CALL指令调用之后，将过程的返回地址压入堆栈，将过程入口地址赋值给EIP，实现CPU控制权的转移
    - RET指令调用之后，将过程的返回地址赋值给EIP寄存器，实现CPU控制权的转移

链接库

链接库（Link Library）是一个文件，包含已经编译成机器码的过程。

```
includelib \masm32\lib\masm32.lib
includelib \masm32\lib\kernel32.lib
```

相当于函数声明

```
StdOut PROTO :DWORD
StdIn PROTO :DWORD,:DWORD
ExitProcess PROTO STDCALL :DWORD
```