

assembly - 1120(summary)

data, heap, stack - 변수 영역

매개변수 - parameter

인수 - argument

stack frame - argument, return 값, local variable(지역변수), register 자동 저장

BP(base pointer) - stack의 시작 주소

SP - stack pointer(top)

call by value- 팔호 안에 변수를 호출

call by reference - 팔호 안에 객체변수를 호출

연산 결과는 기본적으로 ax

[pdf 7페이지]**

만약에 [EBP+4] 위치에 다른 것이 들어가면 return address가 사라져서 돌아갈 주소가 없어짐

EBP 바로 위는 무조건 return address

EBP를 기준으로 위는 return address를 제외하고 parameter / 밑으로 가면 local variable

EBP를 기준으로 +면 parameter / -면 local variable

[pdf 16페이지]

4번째 줄 sub esp, 32 → sub esp, 30

Recursion: 종료 조건을 무조건 넣어야함(넣지 않으면 무한으로 돌아감)

procedure 호출하면 stack frame 만들어지고 bp도 생성

INVOKE는 다음을 자동으로 수행해 주는 함수 호출용 매크로

1. 파라미터(push) 순서를 자동으로 맞춰서 스택에 넣고
2. call 명령으로 함수 실행
3. 호출 규칙(stdcall, cdecl 등)에 따라 스택 정리까지 자동 처리