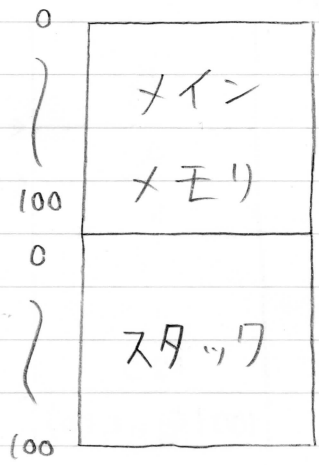
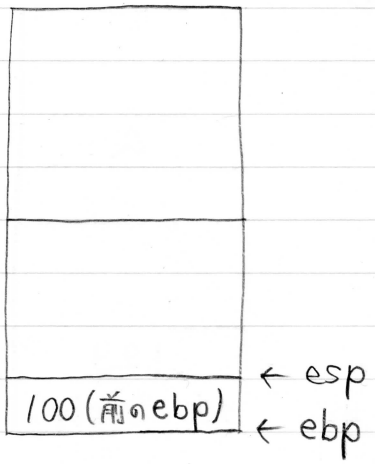
①



最初、esp = 100、ebp = 100

push ebp →

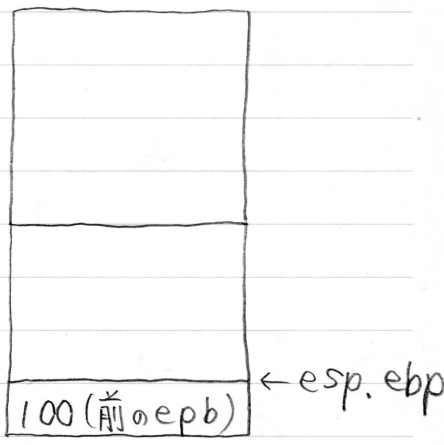
②



esp = 96、 ebp = 100

mov esp、epb ↓

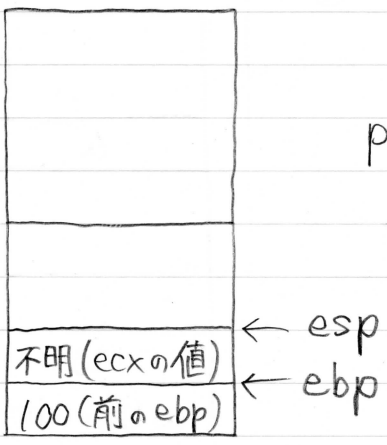
③



esp = 96 、ebp = 96

← push ecx

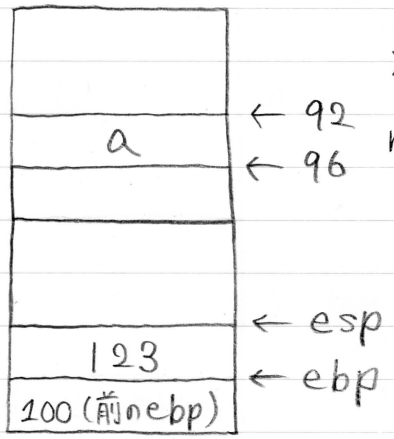
④



esp = 92 、ebp = 96

mov dword ptr _a$[ebp], 123

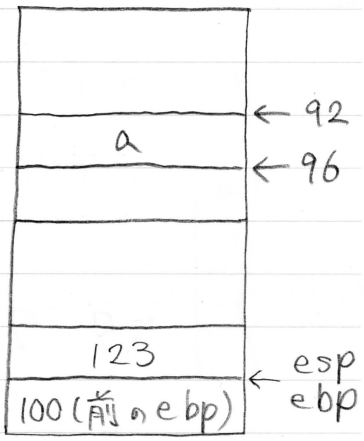
⑤



xor eax, eax

mov esp, ebp

⑥

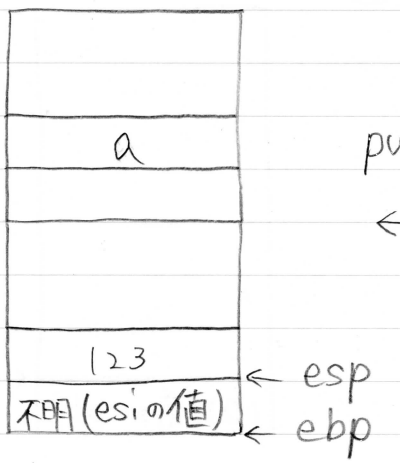


esp = 92, ebp = 96

esp = 96, ebp = 96

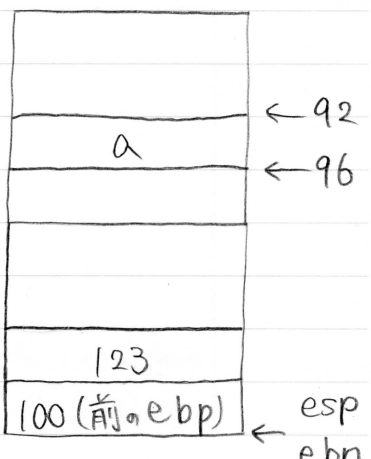
pop ebp

⑧



push esi

⑦



esp = 96, ebp = 100

esp = 100, ebp = 100