Chapter 09. 함수

호출 규약

```
int sum(int x, int y)
{
    int total = x + y;
    return total;
}


int result = sum(10, 20);
int result = sum(10, 20);
```

EIP	0xff3f
EBP	0xc210
ESP	0xc1f0

0xc1d4		
0xc1d8		
0xc1dc		
0xc1e0		
0xc1e4		
0xc1e8		
0xc1ec		
0xc1f0	????	ESP

```
int result = sum(10, 20);
```

EIP	0xff3f
EBP	0xc210
ESP	0xc1ec

0xc1d4		
0xc1d8		
0xc1dc		
0xc1e0		
0xc1e4		
0xc1e8		
0xc1ec	20 (y)	ESP
0xc1f0	????	

```
int result = sum(10, 20);
```

EIP	0xff3f
EBP	0xc210
ESP	0xc1e8

0xc1d4		
0xc1d8		
0xc1dc		
0xc1e0		
0xc1e4		
0xc1e8	10 (x)	ESP
0xc1ec	20 (y)	
0xc1f0	????	

```
int result = sum(10, 20);
```

EIP	0xff3f
EBP	0xc210
ESP	0xc1e4

0xc1d4		
0xc1d8		
0xc1dc		
0xc1e0		
0xc1e4	0xff3f (EIP, Return Address)	ESP
0xc1e8	10 (x)	
0xc1ec	20 (y)	
0xc1f0	????	

```
int sum(int x, int y)
{
    int total = x + y;
    return total;
}
```

EIP	0xe018
EBP	0xc210
ESP	0xc1e8

0xc1d4		
0xc1d8		
0xc1dc		
0xc1e0		
0xc1e4	0xff3f (EIP OLD, Return Address)	ESP
0xc1e8	10 (x)	
0xc1ec	20 (y)	
0xc1f0	????	

```
int sum(int x, int y)
{
    int total = x + y;
    return total;
}
```

EIP	0xe018
EBP	0xc210
ESP	0xc1e0

0xc1d4		
0xc1d8		
0xc1dc		
0xc1e0	0xc210 (EBP)	ESP
0xc1e4	0xff3f (EIP OLD, Return Address)	
0xc1e8	10 (x)	
0xc1ec	20 (y)	
0xc1f0	????	

```
int sum(int x, int y)
{
    int total = x + y;
    return total;
}
```

EIP	0xe018
EBP	0xc1e0
ESP	0xc1e0

0xc1d4		
0xc1d8		
0xc1dc		
0xc1e0	0xc210 (EBP OLD)	ESP EBP
0xc1e4	0xff3f (EIP OLD, Return Address)	
0xc1e8	10 (x)	
0xc1ec	20 (y)	
0xc1f0	????	

```
int sum(int x, int y)
{
    int total = x + y;
    return total;
}
```

EIP	0xe018
EBP	0xc1e0
ESP	0xc1dc

0xc1d4		
0xc1d8		
0xc1dc	30 (total)	ESP
0xc1e0	0xc210 (EBP OLD)	EBP
0xc1e4	0xff3f (EIP OLD, Return Address)	
0xc1e8	10 (x)	
0xc1ec	20 (y)	
0xc1f0	????	

```
int sum(int x, int y)
{
    int total = x + y;
    return total;
}
```

EAX	30
EIP	0xe018
EBP	0xc1e0
ESP	0xc1dc

0xc1d4		
0xc1d8		
0xc1dc	30 (total)	ESP
0xc1e0	0xc210 (EBP OLD)	EBP
0xc1e4	0xff3f (EIP OLD, Return Address)	
0xc1e8	10 (x)	
0xc1ec	20 (y)	
0xc1f0	????	

```c
int sum(int x, int y)
{
    int total = x + y;
    return total;
}
```

EAX	30
EIP	0xe018
EBP	0xc1e0
ESP	0xc1e0

0xc1d4		
0xc1d8		
0xc1dc		
0xc1e0	0xc210 (EBP OLD)	ESP EBP
0xc1e4	0xff3f (EIP OLD, Return Address)	
0xc1e8	10 (x)	
0xc1ec	20 (y)	
0xc1f0	????	

```
int sum(int x, int y)
{
    int total = x + y;
    return total;
}
```

EAX	30
EIP	0xe018
EBP	0xc210
ESP	0xc1e8

0xc1d4		
0xc1d8		
0xc1dc		
0xc1e0		
0xc1e4	0xff3f (EIP OLD, Return Address)	ESP
0xc1e8	10 (x)	
0xc1ec	20 (y)	
0xc1f0	????	

```
int result = sum(10, 20);
```

EAX	30
EIP	0xff3f
EBP	0xc210
ESP	0xc1e8

0xc1d4		
0xc1d8		
0xc1dc		
0xc1e0		
0xc1e4		
0xc1e8	10 (x)	ESP
0xc1ec	20 (y)	
0xc1f0	????	

```
int result = sum(10, 20);
```

EAX	30
EIP	0xff3f
EBP	0xc210
ESP	0xc1f0

0xc1d4		
0xc1d8		
0xc1dc		
0xc1e0		
0xc1e4		
0xc1e8		
0xc1ec		
0xc1f0	????	ESP

```
int result = sum(10, 20);
```

EAX	30
EIP	0xff3f
EBP	0xc210
ESP	0xc1ec

0xc1d4		
0xc1d8		
0xc1dc		
0xc1e0		
0xc1e4		
0xc1e8		
0xc1ec	30	ESP
0xc1f0	????	