

バッファオーバーフロー実験

2001年9月11日

上牧瀬 誠

バッファオーバーフローとは

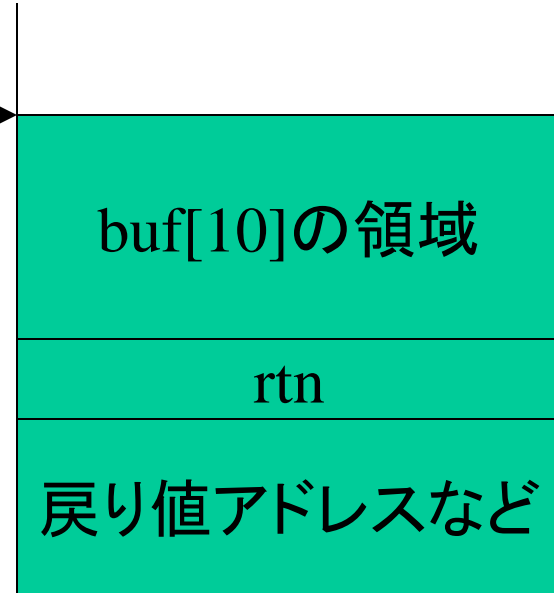
- バッファより長いデータを与える



簡単な例

```
int foo()  
{  
  char *rtn;  
  char buf[10];  
  
  gets(buf);  
  
}
```

buf[]の
先頭アドレス



スタック

buf[]の領域より大きいデータが書き込まれると、
rtn, 戻り値アドレスなどが**上書き**される

無権限利用

多くのサーバプログラムはroot権限で稼動



バッファオーバーフローで戻り値アドレスを書き換える
(別のプログラムの先頭アドレス)



root権限を取得

対策

- 入力データを読み込むときに、**長さを指定する関数**を使用する
- 入力データを保持するバッファは、長さを調べた上で**動的に確保**する

実験

1. /u/makoto_k/rinkou/buffer/から
次のファイルをコピー
 - buftest.c
 - test.dat
2. コンパイルし,実行
 - gcc buftest.c -o buftest
 - ./buftest < test.dat

```
#include <stdio.h>
#define BUFLLEN 200

int main(int argc , char **argv)
{
    char *rtn;
    char dmy[BUFLLEN];
    char buf[BUFLLEN];

    memset(dmy,'¥0',BUFLLEN);
    memset(buf,'¥0',BUFLLEN);

    printf("before¥n");
    printf("buf(len:%d) = %s¥n",strlen(buf),buf);
    printf("dmy(len:%d) = %s¥n",strlen(dmy),dmy);

    if((rtn = gets(buf)) == NULL)
        exit(1);

    printf("after¥n");
    printf("buf(len:%d) = %s¥n",strlen(buf),buf);
    printf("dmy(len:%d) = %s¥n",strlen(dmy),dmy);
}
```