
# ＜セキュリティ・キャンプ全国大会2016課題回答ページ＞

■はじめにお読みください

※このページは、60分程度でセッションが切断され、入力内容が無効となります。そのため、回答内容は応募者ご自身が適宜保存しながら回答するよう、くれぐれもご注意ください。

※一時保存機能による回答内容の保存は48時間有効です。一時保存URLは、①有効期限を過ぎた場合、②再度一時保存をした場合（新しく別の一時保存URLが発行され、古いURLは無効となります）、③回答内容を送信した場合に、無効となりますので、ご注意ください。

※回答内容が正常に送信された場合、ご記入いただいたメールアドレス宛に確認メール（ドメイン：@mail3.webcas.net）を自動送信させていただきます。24時間を経過しても確認メールが届いていない場合には、応募が受理されていない恐れがありますので、必ず、HP記載のお問い合わせ先（URL：https://www.ipa.go.jp/jinzai/camp/2016/zenkoku2016_oubo.html）までご連絡ください。

※回答の締め切りは、【2016年5月30日 17：00】です。再提出を含め、締め切りまでに回答を送信してください。

※課題の再提出をされる場合には、再度すべての設問に回答してください。再提出の回数に制限は設けませんが、前回提出いただいた回答は破棄させていただきますので、ご注意ください。
また、再提出の際には、必ず、①メールアドレスをお聞きする設問で前回提出時と同じメールアドレスをご入力いただき、②再提出かどうかをお聞きする設問でチェックをつけてください。この2点がなされていない場合、すべての回答を無効とさせていただく場合がございます。

※課題回答ページは、「基本情報」、「共通問題」、「選択問題」の3つで構成しております。「共通問題」は、全部で3問あり、すべてが回答対象です。「選択問題」は、全部で11問あり、その中から4つを選択して回答（回答欄への1文字以上の入力をもって、回答されたものと判断します）してください。
なお、「共通問題」、「選択問題」の各設問は、10,000字まで入力が可能です。

## 【基本情報】

| | |
|---|---|
| 氏名 [必須] | 姓 [ ] 名 [ ] |
| 氏名（ふりがな） [必須] | せい [ ] めい [ ] |
| 性別 [必須] | ○男性 ○女性 |
| 生年月日 [必須] | [ ]年[ ]月[ ]日 ※西暦で入力してください。 |

| | |
|---|---|
| 学校名 [必須] | |
| 学校種別 [必須] | |
| 学部／学科 [必須] | |
| 学年 [必須] | |
| 郵便番号 [必須] | - 住所検索 |
| 都道府県 [必須] | |
| 市区町村 [必須] | |
| 町名番地（ビル建物名含む） [必須] | |
| 電話番号 [必須] | - - ※日中に連絡させたいただくことがございます。 |
| メールアドレス<br>※再提出される方は、必ず、前回提出時と同じメールアドレスを入力してください。<br>[必須] | <br>※確認のため、再度ご入力ください。 |
| Twitterアカウントをお持ちの場合には、記入してください。 | |
| ホームページまたはブログをお持ちの場合は、URLを記載してください。 | |
| 応募のきっかけ<br><br>（複数回答可） | ☐ホームページ（IPA/実施協議会）<br>☐メール（IPA/実施協議会）<br>☐チラシ・ポスター（IPA/実施協議会）<br>☐Twitter（実施協議会）<br>☐Facebook（実施協議会）<br>☐先生・教授（学校関係）<br>☐友人・先輩等（学校関係）<br>☐友人・知人（学校以外）<br>☐地方大会（ミニキャンプ他）<br>☐セキュリティ・キャンプフォーラム<br>☐その他 |
| ミニキャンプ参加実績のある方は、チェックをつけてください。<br><br>（複数回答可）<br><br>※この質問に対する回答は、選考に影響ありません。 | ☐セキュリティ・ミニキャンプin四国【2016/5/21-22】<br>☐セキュリティ・ミニキャンプin沖縄【2015/12/18-20】<br>☐セキュリティ・ミニキャンプin北海道【2015/12/12-13】<br>☐セキュリティ・ミニキャンプin東北【2015/11/14-15】<br>☐セキュリティ・ミニキャンプin北陸【2015/9/26-27】<br>☐セキュリティ・キャンプ九州in福岡【2015/8/28-30】<br>☐セキュリティ・ミニキャンプin新潟【2015/5/16-5/17】 |

| | |
|---|---|
| | ☐上記以前に実施されたセキュリティ・ミニキャンプに参加 |

## 【共通問題】 ※下記の共通問題にはすべて回答してください。

### 共通問題. 1

(1) あなたが今まで作ってきたものにはどのようなものがありますか？ いくつでもいいので、ありったけ自慢してください。

(2) それをどのように作りましたか？ソフトウェアの場合にはどんな言語で作ったのか、どんなライブラリを使ったのかなども教えてください。

(3) 開発記のブログなどあれば、それも教えてください。コンテストなどに出品したことがあれば、それも教えてください。

### 共通問題. 2

(1) あなたが経験した中で印象に残っている技術的な壁はなんでしょうか？（例えば、C言語プログラムを複数ファイルに分割する方法）

(2) また、その壁を乗り越えるために取った解決法を具体的に教えてください。（例えば、知人に勧められた「〇〇」という書籍を読んだ）

(3) その壁を今経験しているであろう初心者にアドバイスをするとしたら、あなたはどんなアドバイスをしますか？

## 共通問題. 3

(1) あなたが今年のセキュリティ・キャンプで受講したいと思っている講義は何ですか？（複数可）
そこで、どのようなことを学びたいですか？なぜそれを学びたいのですか？

(2) あなたがセキュリティ・キャンプでやりたいことは何ですか？身につけたいものは何ですか？（複数可）
自由に答えてください。

## 【選択問題】 ※下記の選択問題の中から 4つ 選択して回答してください。

### 選択問題. 1

以下は変数hogeとfugaのメモリアドレスを表示するプログラムと、その実行結果です。
実行結果のhogeとfugaのメモリアドレスを見て、思うことを説明してください。

・ソースコード

```
#include <stdio.h>
#include <stdlib.h>

int main(int argc, char **argv){
 int hoge[10];
 int *fuga;

 fuga = malloc(1);

 printf("hoge address = %p¥n", hoge);
 printf("fuga address = %p¥n", fuga);

 free(fuga);
 return 0;
}
```

・実行結果

```
hoge address = 0x7fff539799f0
fuga address = 0x7fca11404c70
```

### 選択問題. 2

Googleは、自社のサービスのセキュリティを高めるために様々なことを行っています。ブラウザからGoogleの検索サービス（https://www.google.co.jp/）にアクセス

を行い、どのようなセキュリティ施策が行われているかを見つけなさい。ブラウザは任意のもので構いません。ブラウザのどういった点からどういった施策を行っていると判断できるのか、その理由も含めてできるだけ多くの項目を回答してください。
拡張機能を利用しても構いませんが、ブラウザ以外の方法でアクセスしてはいけません。

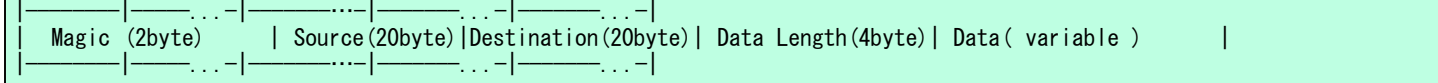
## 選択問題. 3

RAMは主記憶装置、HDDやSSDなどは補助記憶装置と呼ばれます。一般にCPUは主記憶装置上のプログラムしか実行できません。ではなぜ、私たちは普段から補助記憶装置に書き込んだプログラムを実行できているのでしょうか？パソコンの電源を入れてからのストーリーを考えてみてください。

## 選択問題. 4

突然だが、RH Protocolで用いられるRHパケットのフォーマットを以下に示す。なおRH Protocolは実在しないプロトコルであり、その内容について特に意味は無い。

Format of RH Packet




```
char Magic [2];
char Source[20]; /* null( '¥0' ) terminated ascii strings */
char Destination[20]; /* null( '¥0' ) terminated ascii strings*/
uint32_t DataLength; /* min 0, max 4,294,967,295 */
char Data[DataLength]; /* null( '¥0' ) terminated ascii strings */
```

バイトオーダーはbig endian (network byte order) とする。

添付するバイナリは、とあるRHストリームのうち片方向のみを抽出したものである。このバイナリストリームを読み込み、1つのRHパケットが以下の条件のすべてにマッチするときに標準出力に文字列”PASS”、 それ以外の場合は”REJECTED”と表示するCもしくはC++のプログラムを記述し、実行結果と共に提出せよ。また、マッチングにかかるCPUサイクル及びメモリ使用量を計測し記載した場合、評価に加味する。

Condition(条件) 1: Magicがchar[0] = 'R'、 char[1] = 'H'であること。
Condition 2: Sourceが”rise-san”または”cocoa-san”であること。なお、”RiSe”や”Cocoa”など、小文字大文字が混ざっていても、マッチさせること。
Condition 3: Destinationが”Chino-chan”または”Chino″であること。なお、cond. 2と同じく、小文字大文字が混ざっていても、マッチさせること。

Condition 4: Sourceが”cocoa-san”かつDestinationが”Chino”の場合はREJECTする。
Condition 5:  Dataに下記の文字列を厳密に含むこと。
char** valid_order_brand =
{
	“BlueMountain”
	“Columbia”,
	“OriginalBlend”
};
Condition 6: Dataに下記の文字列を厳密に含まないこと。なお、cond. 4よりも、cond. 5が優先される。
char** invalid_order_brand =
{
	“DandySoda”
	“FrozenEvergreen”
};

## 選択問題. 5

PCなどに搭載されているOSは「汎用OS」と呼ばれますが、それに対して、家電やAV機器などの「組込みシステム」に搭載されているOSは「組込みOS」と呼ばれます。
組込みOSと汎用OSの違い、「OSが無い」や「ベアメタル」という環境、そもそもOSとは何なのか？など、あなた自身はどう考えているのかを、
あなた自身の言葉で自由に説明してください。(「正しい答え」を聞いているわけではありません。あなた自身の考えを教えてください)

## 選択問題. 6

IDとパスワードを入力してユーザの認証を行うWebアプリがあります。あなたがこのアプリに対してセキュリティテストを行う場合、まず、どのようなテストをしますか？
なぜそのテストを選択したのか、その背景や技術的根拠と共に記載してください。アプリの内部で使われている技術やシステム構成に、前提を置いても構いません。

## 選択問題. 7

あなたが管理するネットワークに悪意ある第三者が存在しない事を証明する方法を思いつく限り列挙してください。なお、条件として物理的にアクセスされる可能性を想定してください。

## 選択問題. 8

以下のダンプはあるプログラムのobjdumpの結果である。このプログラムが行っていることを調べ、その結果を記述してください。完全には分からなくても構いませんので、理解できたところまでの情報や調査の過程で使ったツール、感じたこと等について記述してください。
==

```
$ objdump -d challenge00

challenge00:     ファイル形式 elf64-x86-64

セクション .text の逆アセンブル:

0000000000400080 <.text>:
 400080:     68 19 01 40 00           pushq  $0x400119
 400085:     6a 01                    pushq  $0x1
 400087:     68 06 01 40 00           pushq  $0x400106
 40008c:     68 19 01 40 00           pushq  $0x400119
 400091:     68 29 01 40 00           pushq  $0x400129
 400096:     6a 3c                    pushq  $0x3c
 400098:     68 02 01 40 00           pushq  $0x400102
 40009d:     68 10 01 40 00           pushq  $0x400110
 4000a2:     48 b8 36 15 1b 25 67     movabs $0x63391a67251b1536,%rax
 4000a9:     1a 39 63
 4000ac:     50                       push   %rax
 4000ad:     68 02 01 40 00           pushq  $0x400102
 4000b2:     6a 00                    pushq  $0x0
 4000b4:     68 06 01 40 00           pushq  $0x400106
 4000b9:     68 14 01 40 00           pushq  $0x400114
```

```
 4000be:    68 0c 01 40 00            pushq  $0x40010c
 4000c3:    68 02 01 40 00            pushq  $0x400102
 4000c8:    68 26 01 40 00            pushq  $0x400126
 4000cd:    68 14 01 40 00            pushq  $0x400114
 4000d2:    6a 07                      pushq  $0x7
 4000d4:    68 0a 01 40 00            pushq  $0x40010a
 4000d9:    6a e0                      pushq  $0xffffffffffffffe0
 4000db:    68 08 01 40 00            pushq  $0x400108
 4000e0:    68 19 01 40 00            pushq  $0x400119
 4000e5:    6a 08                      pushq  $0x8
 4000e7:    68 04 01 40 00            pushq  $0x400104
 4000ec:    6a 00                      pushq  $0x0
 4000ee:    68 1c 01 40 00            pushq  $0x40011c
 4000f3:    6a 00                      pushq  $0x0
 4000f5:    68 06 01 40 00            pushq  $0x400106
 4000fa:    6a 00                      pushq  $0x0
 4000fc:    68 02 01 40 00            pushq  $0x400102
 400101:    c3                         retq
 400102:    58                         pop    %rax
 400103:    c3                         retq
 400104:    5a                         pop    %rdx
 400105:    c3                         retq
 400106:    5f                         pop    %rdi
 400107:    c3                         retq
 400108:    5d                         pop    %rbp
 400109:    c3                         retq
 40010a:    59                         pop    %rcx
 40010b:    c3                         retq
 40010c:    48 01 ec                   add    %rbp,%rsp
 40010f:    c3                         retq
 400110:    48 39 06                   cmp    %rax,(%rsi)
 400113:    c3                         retq
 400114:    80 34 0e 55                xorb   $0x55,(%rsi,%rcx,1)
 400118:    c3                         retq
 400119:    0f 05                      syscall
 40011b:    c3                         retq
 40011c:    48 89 e6                   mov    %rsp,%rsi
 40011f:    41 5a                      pop    %r10
 400121:    c3                         retq
 400122:    48 89 f1                   mov    %rsi,%rcx
 400125:    c3                         retq
 400126:    48 ff c9                   dec    %rcx
 400129:    75 01                      jne    0x40012c
 40012b:    c3                         retq
 40012c:    41 5a                      pop    %r10
 40012e:    c3                         retq
==
```

## 選択問題. ９

マイナンバーカードの配布システムを構築・運用することになりました。あなたなら何に気をつけてどんなサービスを構築しますか？
マイナンバーカードの仕様は現実通りのICカードとします。
※ 注意: マイナンバーでは無くマイナンバーカードです。

## 選択問題. １０

まずは以下のプログラムを物理PCと複数の仮想化ソフトウェア（qemu、 VMware、 Virtual PCなど）を使って実行し、それぞれの結果の違いを確認してください。そして、なぜそうした結果が得られたのか、物理PCと同じ振る舞いを実現するには仮想化ソフトウェアをどのように改造すればよいかを考察し、その内容を記述してください。

==

```
#include <stdio.h>
#include <signal.h>
#include <stdlib.h>

void sighandler()
{
   printf("OK¥n");
   exit(0);
}

__asm__("check00:¥n¥
   mov $0x564D5868, %eax¥n¥
   mov $0xa, %cx¥n¥
   mov $0x5658, %dx¥n¥
   in %dx, %eax¥n¥
   ret¥n¥
");
void check00();
```

```
__asm__("check01:¥n¥
   .byte 0xf3,0xf3,0xf3,0xf3,0xf3¥n¥
   .byte 0xf3,0xf3,0xf3,0xf3,0xf3¥n¥
   .byte 0xf3,0xf3,0xf3,0xf3,0xf3¥n¥
   ret¥n¥
");
int check01();

__asm__("check02:¥n¥
   .byte 0x0f,0x3f,0x07,0x0b¥n¥
   ret¥n¥
");
int check02();

int main(int argc, char **argv)
{
   int cmd;
   if(argc == 2){
       cmd = atoi(argv[1]);
   }else{
       printf("USAGE: %s <command>¥n", argv[0]);
       exit(1);
   }
   signal(SIGSEGV, sighandler);
   signal(SIGILL, sighandler);
   switch(cmd){
   case 0: check00(); break;
   case 1: check01(); break;
   case 2: check02(); break;
   default: exit(1);
   }
   printf("NG¥n");
   return 1;
}
==
```

## 選択問題. １１

2015 年に発行された CVE の内、あなたが興味を持った”サーバに存在した”脆弱性について１つ提示してください。その脆弱性を悪用した攻撃を検知する方法について詳細に記述してください。また、興味を持った理由を記述してください。
CVE番号:CVE-2015-○○○○

攻撃を検知する方法：

興味を持った理由：

| | |
|---|---|
| ■注意<br>再提出の方は、必ずチェックをしてください。<br><br>本項目にチェックをしないで再提出をいただいた場合、応募を無効とさせていただく場合がございますので、ご注意ください。<br><br>※初めて本フォームにご回答いただく場合、<br>チェックはつけず、次の設問へ進んでください。 | ☐再提出する（上記で回答したメールアドレスが、前回提出時と同じメールアドレスであることを確認しました） |
| 本ページから送信いただいた内容につきましては、セキュリティ・キャンプ事業の運営・実施に係る連絡や資料送付を目的として、独立行政法人情報処理推進機構（IPA）の個人情報保護方針（下記のURLをご参照ください）に基づき、弊機構ならびにセキュリティ・キャンプ実施協議会が適正に取り扱います。<br>https://www.ipa.go.jp/about/privacypolicy/index.html<br><br>ご確認の上、チェックをお願いいたします。<br>[必須] | ☐個人情報の取り扱いに同意する |

設問は以上です。

ご回答が完了された方は以下の「確認」ボタンをクリックしてください。

※ご回答が途中の方は一時保存が可能です。【保存有効時間：48時間】

「一時保存」ボタンをクリックしてください。

確認

一時保存