

セキュリティ演習 S-Learningプロジェクト 2022

情報科学専門学校 滋野ゼミ

時間割

- 挨拶・自己紹介 10分
- 演習ガイダンス 70分
(3～4問、途中休憩時間を挟みます)
- アンケート記入 5分
- 学校紹介 15分

自己紹介

発表



名前: 佐野 柊介
(さの・しゅうすけ)

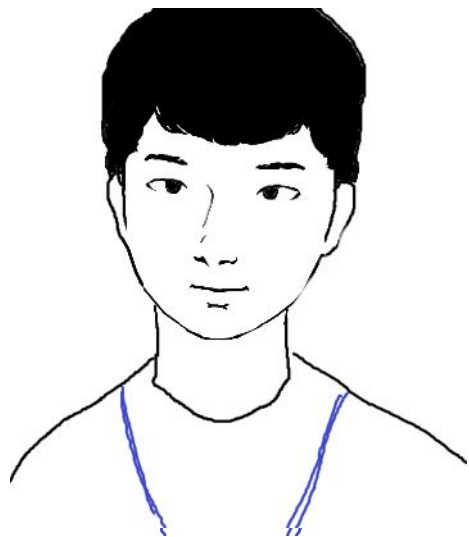
趣味:

イラスト、ゲーム作り、麻雀

一言:

来年からゲーム会社で働きます
なんでも質問してね

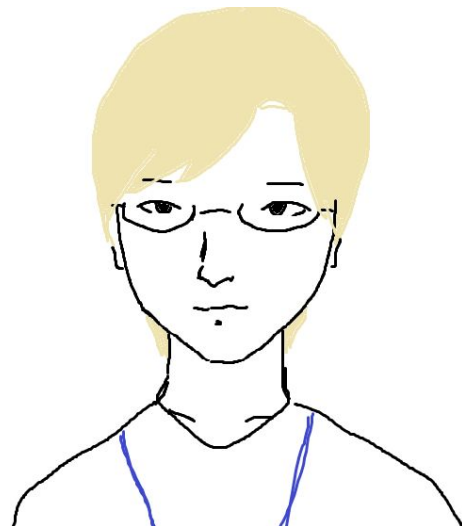
インストラクター



福元 健人



西山 雅人



萩原 優



ゼミ担任

名前：滋野 謙太郎
(しげの・けんたろう)

分野：
セキュリティ

趣味：
ゲーム

一言：
今日は一日頑張りましょう！

マスコット



ふわりん

誰ひとり名前を覚える必要はありませんが.....

【情報科学専門学校】の名前だけ
覚えて帰ってください

S-Learningって何？

一言でいうと…

中高生に

情報セキュリティ

を知ってもらう

プロジェクトです！

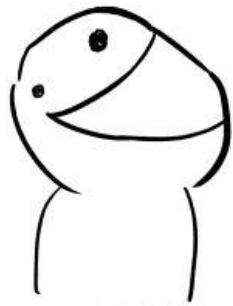
どんなことするの？

写真から場所を特定



ガチャで不正！？

S-Learningは
情報セキュリティの知識を使って
腕試しできる場所(CTF)
を提供しています

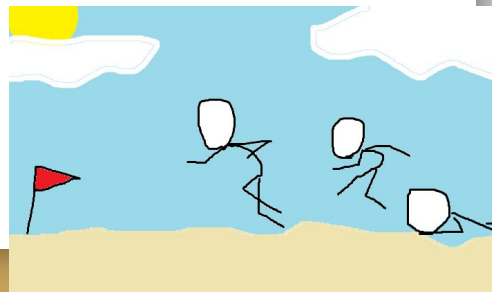


S-Learningプロジェクトの目的

CTF(Capture The Flag、**旗取り**)と呼ばれる技術者たちが知識を共有・腕試しするために行われるクイズを、一般向けに難易度を落とし**楽しみながら**セキュリティに興味を持ってもらうことを目的としています

サイトやソフトウェアの脆弱性(バグや不具合、攻撃できる隙)を探し、FLAGと呼ばれる隠されたコードを入手することでクリア

ビーチフラッグ:
浜辺に埋めた旗を誰が一番最初に取りれるか
競走する遊び

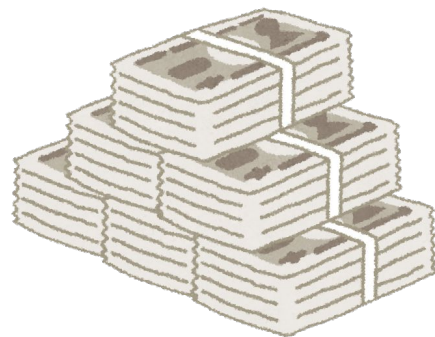


講義を提案するに至った背景

「学生からの感想が欲しい！」

「情報科学専門学校の布教！」

のためにきました



S-Learningからのお願い

自分がわからないことは他の人もわからないことが多く、こちらの説明が不足している可能性が高いです

演習の中でわからないことがあったら**遠慮せず手をあげてメンバーを呼んでください！**

演習ガイドンスを始めましょう

↓PCのデスクトップ右上からこのサイトにアクセス！

secret-learn.ssl-lolipop.jp/2022



<https://secret-learn.ssl-lo>

★ここはどこ？

ネットに写真をあげるとき、顔や看板が写っていないかなければ大丈夫だと思いませんか？



★ここはどこ？

TwitterやInstagramなどのSNSは画像を
処理してから公開するため問題ありませんが、
それ以外のサイトだと思わぬ個人情報が残って
いるかもしれません.....

(EXIF情報: 撮影に使用したデバイス、撮影した緯度経度、撮影日時
などなど.....)



早速やってみよう！

この演習の目的:

ファイルに残されたデータを探しFLAGを手に入れる

<https://secret-learn.ssl-lolipop.jp/2022/practice?app=exifInfo>



その画像、本当に信用できる？

Twitterなどで「公式マークがついているから本物だろう」と、スクリーンショットを拡散してしまうことはありませんか？

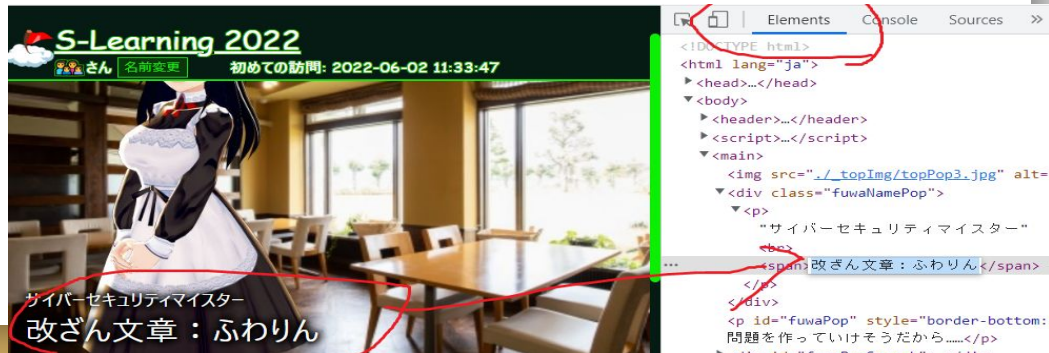
実はホームページ上のスクリーンショットは誰でも簡単に改ざんできてしまうので、自分で情報源のURLを探すなどの注意が必要です。



開発者ツールを使ってみよう！

Chrome上で右クリック「検証」を押すことで開発者ツールという表示されているホームページの元となる要素をみることができる。

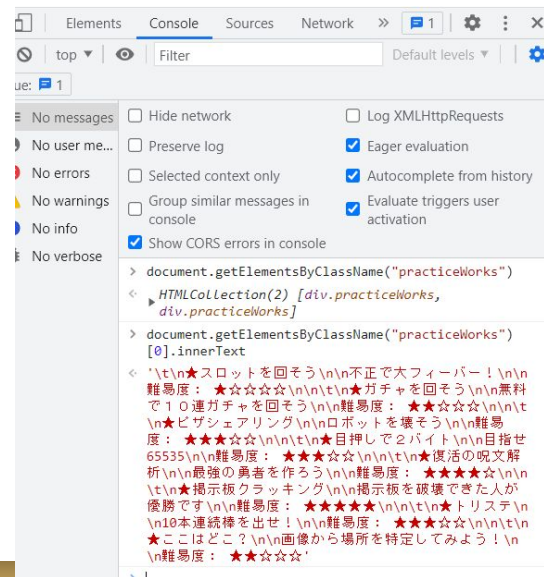
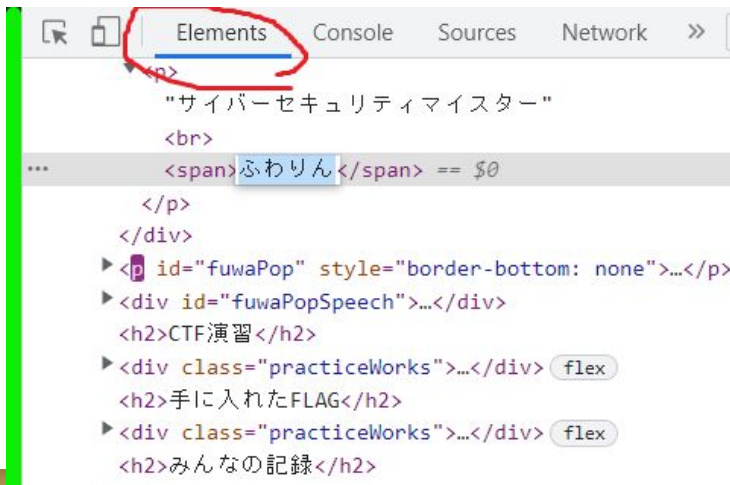
注意: 改ざんしたページのスクリーンショットを改ざんだと明記せずに投稿することは個人・団体の発言などを捏造する行為となるため悪質な場合には警察のご厄介になります。



開発者ツールとは？

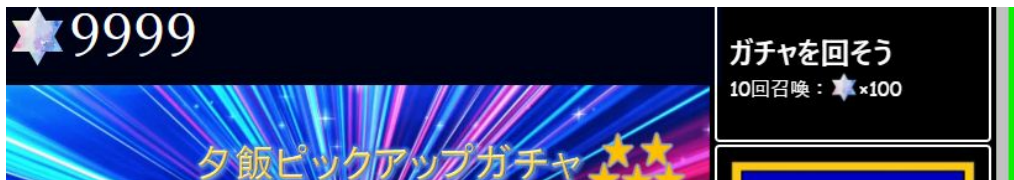
Element...ページの設計図を閲覧・編集できます

Console...ページ上で自由に命令を実行できます



★ガチャを回そう

サイト上で右クリック、検証メニューから開発者ツールを使って石の数を改ざんしてみよう！



```
<tr>
  <td style="vertical-align: top;">
    <div id="headerStone">
      
      <label id="stone">9999</label> == $0
    </div>
  </td>
</tr>
<main id="app"> </main>
```

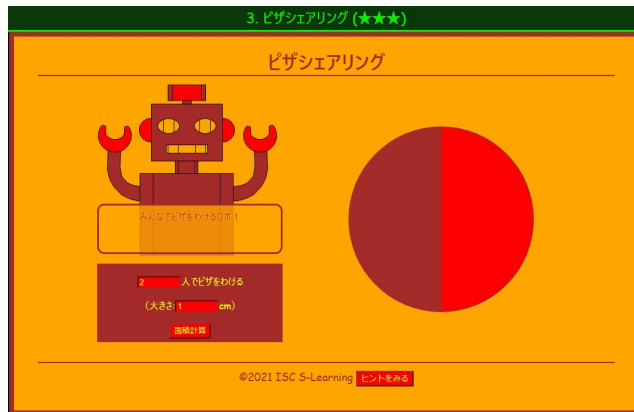
★ピザシェアリング

ロボットが n_1 センチのピザを n_2 人に分けたときの面積を計算して教えてくれるようだ。

数学でやってはいけないことはプログラミングでも同じ.....

早速やってみましょう！

<https://secret-learn.ssl-lolipop.jp/2022/practice?app=division>



ロボットが行う計算式：

$$= (\text{半径} \times \text{半径} \times \text{円周率}) \div \text{人数}$$

円の面積の公式を分ける人数で割ったものとなる。

ピザシェアリングの目標

この演習の目的:

プログラミングでやってはいけないことに気付こう！

★復活の呪文解析 (最終問題)

サイトの脆弱性を使わなくても、復活の呪文のパターンさえつかめれば最強の勇者を作ることができる。

歩いたり敵と戦ったりしてパスワードの変わる部分を調べてみよう！

※難易度が急激に高くなるので注意！



【雑学】16進数とは

10進数: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

↑人間が使う表記法。0d00などと表記する。一桁の最大値は9。

16進数: 0 1 2 3 4 5 6 7 8 9 A B C D E F 10

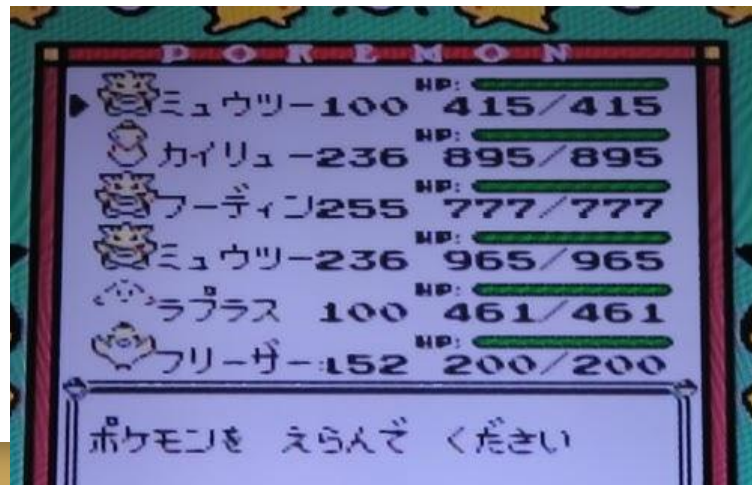
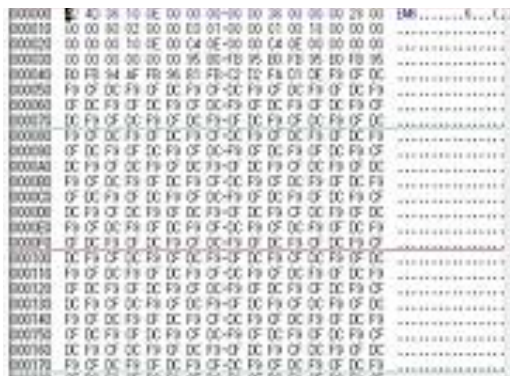
↑コンピュータなどが使うのがこれ、0x00などと表記する。

一桁の最大値はF(15)。

n進数はn番目の数字で桁が上がる $0xFF = 0d255(0xF * 16 + 0xF)$

【雑学】16進数とは

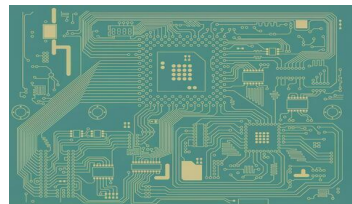
例) 初代ポケモンではバグを使うことでポケモンのレベルを255まであげることができるが、二桁の十六進数で管理しているため255から1つレベルを上げるとオーバーフローしてレベル0に戻ってしまう



【雑学】なんで16進数を使うの？

コンピュータの元となる基盤は電流のON/OFF
二択でしか情報を保つことができません。

そこで現在でも広く用いられる**ノイマン型**というコンピュータの設計を提唱した天才数学者フォン＝ノイマンは「**コンピュータはすべからく2進法たるべきである**」と提唱しました。

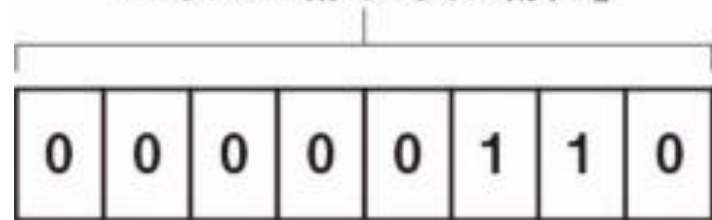


【雑学】なんで16進数を使うの？

2進数は0と1のみで数値を表す手法ですが、0d100を表すのに7桁(0b1100100)必要となり、冗長で人間にとってわかりにくいため、2進数を8桁(8ビット)まとめて「1バイト」とし、2桁に収まる16進数が採用されました。

余談ですが、PCやSDカードの容量に16, 256, 512GBなどの中途半端な数字が多いのは2進数を使っている都合上2のべき乗を使うほうが都合がいいからです
($2^4=16$, $2^8=256$, $2^9=512$)


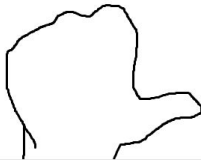


1ビットが8桁ある入れ物「a」



【雑学】なんで16進数を使うの？

10進数を指で数えると0-5までしか数えられないが、
2進数で数えると指が立っているか否かで表せるため
0-31(2⁵パターン)、両手で0-1023まで表せる(2¹⁰パターン)



				
2進数	0b00000	0b00001	0b00010	0b00100
10進数	0	1	2	4

さっそくやってみよう！

パスワードには16進数が使われている。

移動したり敵と戦ったりしてパスワードの値がどう変わるか見てみよう！

この演習の目的：

パスワードを解読し最強の勇者を作ろう！

<https://secret-learn.ssl-lolipop.jp/2022/practice?app=hexagon>



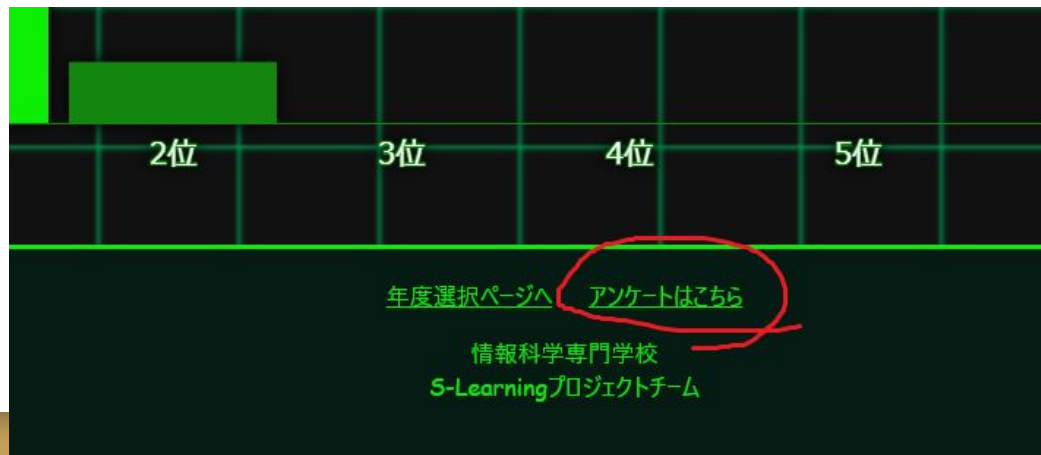
演習終了：質問タイム

ここまでを通してわからない点などあれば忌憚なくご質問ください！

アンケートご協力をお願い

ページ下のアンケートフォーム、もしくは右のQRコードからアンケートページに飛んでみよう！

<https://forms.gle/Sd31j2gtaZwi43KN8>



情報科学専門学校の紹介

- ・横浜駅近辺で唯一の情報系の学校！（駅から約5分）
- ・プログラミング未経験でもパソコンさえ慣れていれば大丈夫！
- ・学費は一般的な私大と同水準！（108万＋教科書代、
資格や活動によって特待生に選ばれればもっと減らせる！）
- ・1, 2, 3, 4年制から選べる8つの学科！
（一部は入学後転科可能）
- ・一部リモート授業対応！（学科、学年による）



情報科学専門学校の紹介

- 駅チカなのでランチの選択肢はよりどりみどり！
 - こみ入った人間関係なし。好きな人とだけ話してればOK！
 - 授業内で行われる手厚い資格サポート、履歴書にかける！
 - プログラマ以外にもエンジニアとして求められるインフラ、マネジメント、設計など幅広い知識が蓄えられる！
 - 医療、ファッション、デザイン、福祉の系列校との交流が盛ん！
- まずは資料請求から！！(<https://isc.iwasaki.ac.jp/>)

こういう人におすすめ！

- ・一日中椅子に座ってPCに向き合ってることに抵抗がない
- ・読めるほどではないが英語に抵抗がない(英語アレルギーがない)
- ・数学はそこまで使わないが中学一年以上の知識はある
- ・ハードウェア(機器)かソフトウェア(スマホアプリ等)にそこそこ興味がある
- ・プログラミングをやってみたい/電子・ロボット工作/ネットワーク構築/セキュリティをやってみたい

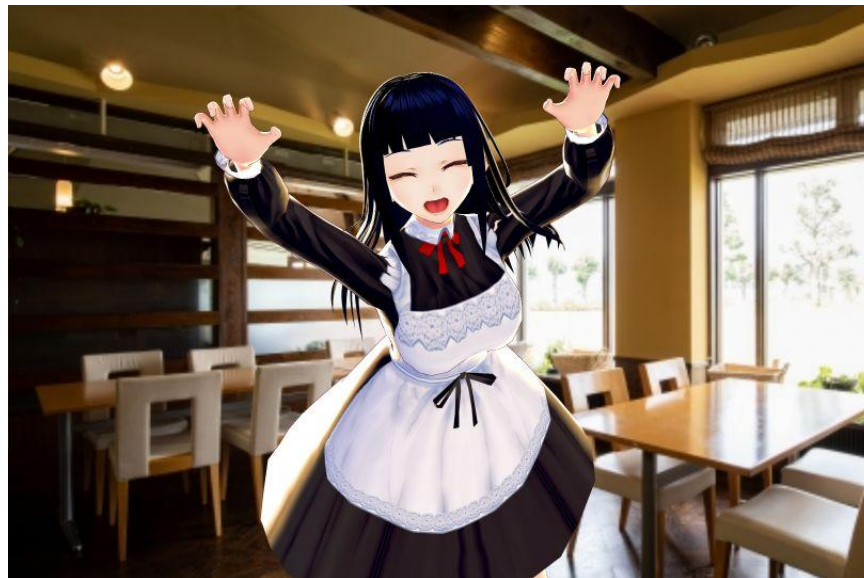
総括

誰かなにかあれば

S-Learningプロジェクトにご協力いただき ありがとうございました！

皆さんがこの体験を有益にご活用
いただけることを、メンバー一同心
から願っております！

家にPCがある人は問題の続きや色
んなCTF問題にも挑戦していただい
けると幸いです！



時間割

50分程度(1コマ)の場合:

- 挨拶・自己紹介 5分
- 演習ガイダンス 30分(2～4問)
- アンケート記入 5分
- 学校紹介 10分