Idea IT College Aso
専門学校　イデアITカレッジ阿蘇

セキュリティ診断実践

ITソリューションコース・実践編

観光業界DX人材養成事業

本科目のねらい

Webアプリケーションの脆弱性が発生する仕組みを学ぶ。

本科目のゴール

❑ Webアプリケーションの脆弱性とその脅威について

理解し、その指摘・報告手順を実践する。

全体の流れ

1. Webアプリケーションの脆弱性が発生する原理
2. Webアプリケーション開発時にどのような箇所で実際に脆弱性が発生するか
3. 脆弱性の指摘方法

全体スケジュール

時数	授業内容	時数	授業内容	時数	授業内容
1	DBアクセスをよりセキュアにする	25	脆弱性演習 ディレクトリ・トラバーサル OSコマンド・インジェクション	49	Capture The Flag（CTF）2回目
2		26		50	
3		27		51	
4		28		52	
5	脆弱性演習の環境構築	29	脆弱性演習 セッション管理の不備 認証制御や認可制御の欠落	53	Webアプリ脆弱性診断 診断記録
6		30		54	
7		31		55	
8		32		56	
9	脆弱性演習 クロスサイトスクリプティング	33	Webアプリ脆弱性診断 画面遷移図	57	セキュリティ業界のキャリアパスについて
10		34		58	
11		35		59	
12		36		60	
13	脆弱性演習 クロスサイトスクリプティング SQLインジェクション	37	セキュリティ心理学	61	Webアプリ脆弱性診断 診断報告書
14		38		62	
15		39		63	
16		40		64	
17	Capture The Flag（CTF）1回目	41	セキュリティ担当者として知っておいて損はないこと	65	成果発表グループワーク
18		42		66	
19		43		67	
20		44		68	
21	脆弱性演習 SQLインジェクション クロスサイト・リクエスト・フォージェリ	45	Webアプリ脆弱性診断 診断記録	69	
22		46		70	
23		47		71	
24		48		72	

Idea IT College Aso
専門学校　イデアITカレッジ阿蘇

DBアクセスをよりセキュアにする

セキュリティ診断実践
(2023/10/2)

担当講師：吉井 幸宗（ yoshii@iica.jp ）

Ver.1.2.0

1

今日の内容とゴール

2

今日の内容

- Webアプリの改修
  - 現在の問題点
  - DBアクセスのユーザを変更する
    - MySQLユーザの作成
    - Webアプリの改修
  - パスワードをハッシュ化して保存する
    - ハッシュ化して保存する
    - ハッシュ化したパスワードを照合する

3

今日のゴール

- ✓ DBにアクセスするアカウントの扱い方を理解する
- ✓ パスワードをハッシュ化して保存することを理解する
- ✓ よりセキュアなWebアプリを作る

4

コマンドの入力について

5

コマンドの入力について

- OSのコマンドとMySQLのコマンドを明記しました
  - OSコマンド
    - OS> os command
    - 例：OS> node server.js
  - MySQL
    - SQL> sql command
    - 例：SQL> select * from user;

6

おさらい

前期で作成したWebアプリを振り返る

7

おさらい

- SQLi Handson

8

おさらい

- SQLi Handson
  - 起動します
    - OS> node server.js
  - ブラウザからアクセス
    - http://localhost:3000/sqli/signin

9

おさらい

- 問題点が2つ
  - DBに管理者アカウントでアクセスしていること
  - パスワードを平文で保存していること

10

おさらい

- DBにアクセスするアカウントが管理者アカウント

```
const express = require("express");
const mysql = require('mysql');
const router = express.Router();

const connection = mysql.createConnection({
    host: 'localhost',
    user: 'root',
    password: '[設定したパスワード]',
    database: 'handson_db'
});
```

11

おさらい

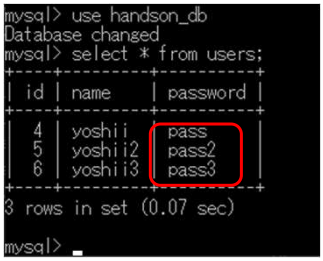
- DBにアクセスするアカウントが管理者アカウント
  - 全てのデータベースにアクセスできる
  - 全ての操作権限を持っている

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| handson_db         |
| information_schema |
| mysql              |
| performance_schema |
| sakila             |
| sys                |
| world              |
+--------------------+
7 rows in set (0.00 sec)
```

12

おさらい

- usersテーブルのパスワードを平文で保存していること



13

DBアカウントを変更する

14

DBアカウントを変更する

- Webアプリ専用のユーザーを作成する
  - MySQLに接続する
    - OS>mysql –u root –p
      - インストール時に設定したパスワードを入力
  - 新しいユーザーを作成する
    - SQL> CREATE USER 'newuser'@'localhost' IDENTIFIED BY 'password';
      - 赤字の箇所は任意の値を入力する

15

DBアカウントを変更する

- Webアプリ専用のユーザーを作成する
  - データベースにアクセスする権限を付与する
    - SQL> GRANT ALL PRIVILEGES ON handson_db . * TO 'newuser'@'localhost';
  - 権限を設定した時は必ずリロードする
    - SQL> FLUSH PRIVILEGES;
  - MySQLへの認証方式を変更する
    - SQL>ALTER USER 'newuser'@'localhost' IDENTIFIED WITH mysql_native_password BY 'password';

16

DBアカウントを変更する

- Webアプリ専用のユーザーを作成する
  - 作成したユーザーでアクセスできるか確認する
    - OS>mysql –u newuser –p
      - 設定したパスワードを入力する
    - MySQLに接続できたら操作を確認する
      - SQL>show databases;
      - SQL>use handson_db;
      - SQL>select * from users;

17

DBアカウントを変更する

- Webアプリの改修
  - routes/sqli.jsを変更する

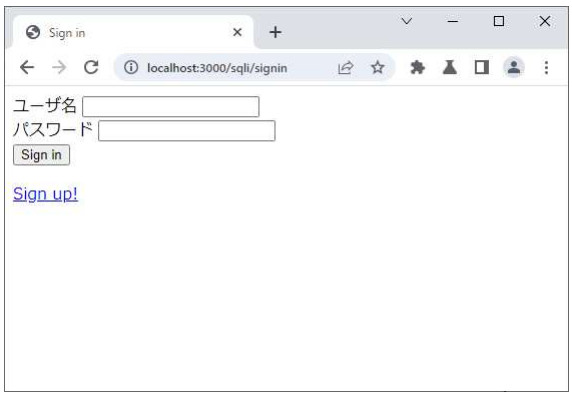
```
const express = require("express");
const mysql = require('mysql');
const router = express.Router();

const connection = mysql.createConnection({
    host: 'localhost',
    user: '[設定したユーザ]',
    password: '[設定したパスワード]',
    database: 'handson_db'
});
```

先ほど作成したnewuserとpasswordを設定する

18

DBアカウントを変更する

- アプリを起動して動作確認する
  - OS>node server.js
  - http://localhost:3000/sqli



19

パスワードをハッシュ化する

20

パスワードをハッシュ化する

- bcryptモジュールをインストール
  - OS>npm install bcrypt –save
  - routes/sqli.jsに追記する

```
const express = require("express");
const mysql = require('mysql');
const bcrypt = require("bcrypt");
const router = express.Router();
```

21

パスワードをハッシュ化する

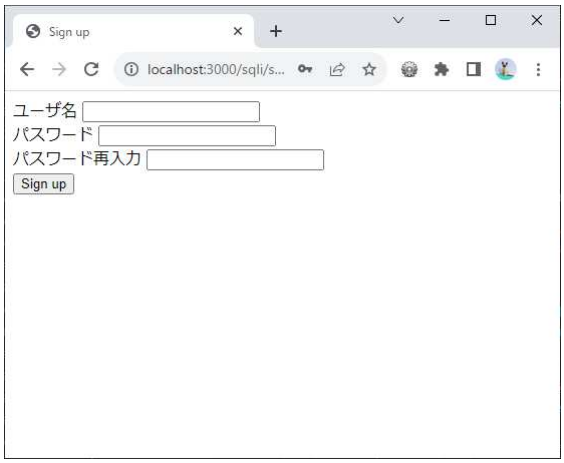
- パスワードをハッシュ化する
  - routes/sqli.jsに追記、変更する

```
if (results.length !== 0) {
    res.render("signup", {
        title: "Sign up",
        errorMessage: ["このユーザ名は既に使われています"]
    });
} else if (password === repassword) {
    const hashedPassword = bcrypt.hash(password, 10);
    console.log(hashedPassword);
    // INSERT
    connection.query(
        'insert into users (name, password) values(?, ?);',
        [username, hashedPassword],
        (error, result) => {
```

22

パスワードをハッシュ化する

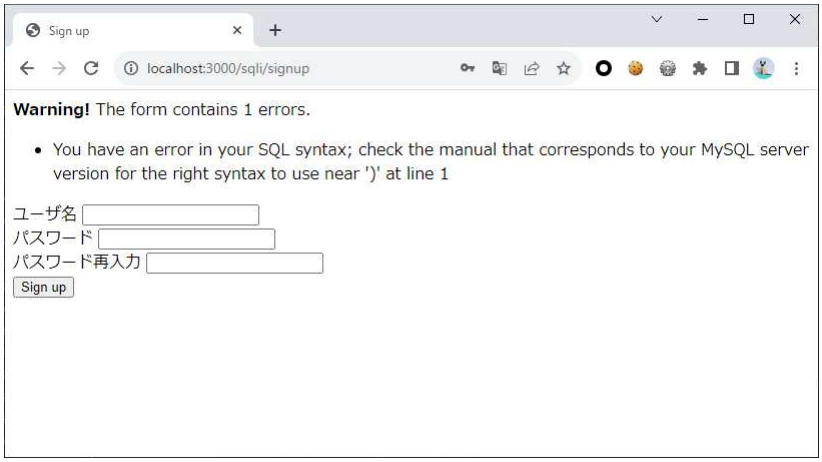
- ブラウザからアクセスしてサインアップする
  - http://localhost:3000/sqli/signup



23

パスワードをハッシュ化する

- ブラウザからアクセスしてサインアップする
  - エラーが発生する



24

パスワードをハッシュ化する

- コンソールログを確認する
  - Promise { <pending> }
    - ハッシュ化の処理中という意味
    - ハッシュ化処理が完了する前に次の処理に進んでしまったため、データベースに保存する処理が失敗してエラーが発生した

25

パスワードをハッシュ化する

- ハッシュ化処理が完了するまで待機する
  - async
    - 非同期処理であることを宣言する
  - await
    - 非同期処理の完了を待機する宣言

26

パスワードをハッシュ化する

- ハッシュ化処理が完了するまで待機する
  - routes/sqli.jsを変更する

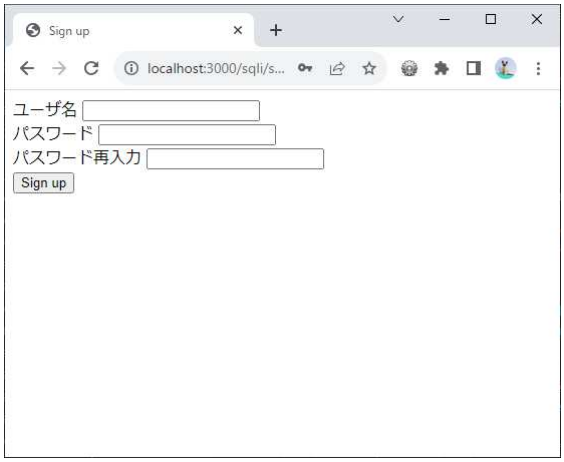
```
connection.query(
    'select * from users where name = ?;',
    [username],
    async (error, results) => {
        if (error !== null) {
```

```
} else if (password === repassword) {
    const hashedPassword = await bcrypt.hash(password, 10);
    console.log(hashedPassword);
    // INSERT
    connection.query(
```

27

パスワードをハッシュ化する

- ブラウザからアクセスしてサインアップする
  - http://localhost:3000/sqli/signup



28

パスワードをハッシュ化する

- bcryptが生成するハッシュ値の構造

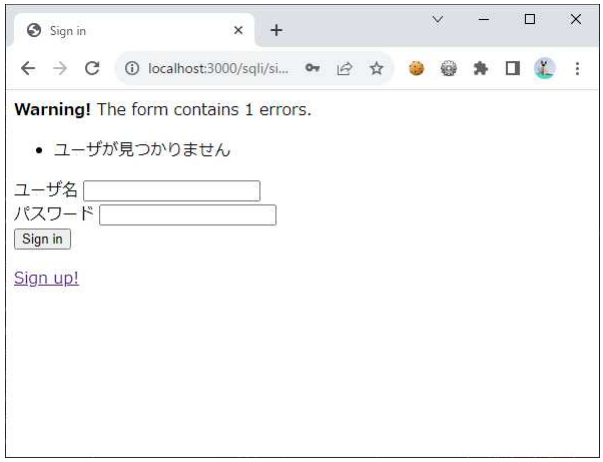
$2b$10$w7O09iHtSzCrCjcyeT.tNuH3Z67AjLt1ow.XDg8RkHpBqqsyemq9S

- 2b
  - ハッシュアルゴリズムのバージョン
- 10
  - ストレッチング回数
  - 2^nのn部分の値
    - 2^10で1024回ストレッチングが実行されたことになる
- w7O09iHtSzCrCjcyeT.tNu（22文字）
  - ソルト
- H3Z67AjLt1ow.XDg8RkHpBqqsyemq9S（残りの31文字）
  - 生成されたハッシュ値

29

パスワードをハッシュ化する

- ハッシュ化したパスワードを照合する
  - 先ほどサインアップしたユーザーでサインインする



30

パスワードをハッシュ化する

- サインインに失敗する
  - DBにはハッシュ化したパスワードが保存されているため

```
router.post("/signin", (req, res) => {
    const username = req.body.username;
    const password = req.body.password;

    connection.query(
        `select * from users where name = ? and password = ?`,
        [username, password],
        (error, results) => {
```

31

パスワードをハッシュ化する

- ハッシュ化したパスワードを照合する
  - routes/sqli.jsを変更する（1）

```
connection.query(
    `select * from users where name = '${username}';`,
    async (error, results) => {
        if (error !== null) {
```

32

パスワードをハッシュ化する

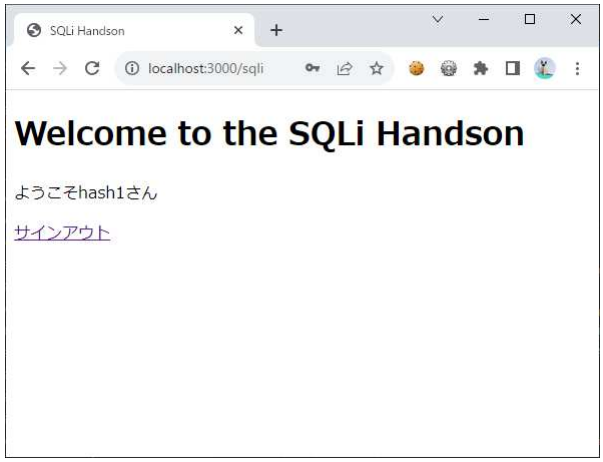
- ハッシュ化したパスワードを照合する
  - routes/sqli.jsを変更する（2）

```
if (results.length === 0) {
    res.render("signin", {
        title: "Sign in",
        errorMessage: ["ユーザが見つかりません"]
    });
} else if (await bcrypt.compare(password, results[0].password)) {
    req.session.userid = results[0].id;
    req.session.username = results[0].name;
    res.redirect("/sqli");
} else {
    res.render("signin", {
        title: "Sign in",
        errorMessage: ["ユーザが見つかりません"]
    });
}
```

33

パスワードをハッシュ化する

- ハッシュ化したパスワードを照合する
  - 先ほどサインアップしたユーザーでサインインする



34

パスワードをハッシュ化する

- usersテーブルのデータを削除する
  - ハッシュ化対応していないデータが残っている

```
Database changed
mysql> select * from users;
+----+---------+--------------------------------------------------------------+
| id | name    | password                                                     |
+----+---------+--------------------------------------------------------------+
|  4 | yoshii  | pass                                                         |
|  5 | yoshii2 | pass2                                                        |
|  6 | yoshii3 | pass3                                                        |
|  8 | hash1   | $2b$10$w7OO9iHtSzCrCjcyeT.tNuH3Z67AjLt1ow.XDg8RkHpBqqsyemq9S |
+----+---------+--------------------------------------------------------------+
4 rows in set (0.01 sec)
```

35

パスワードをハッシュ化する

- usersテーブルのデータを削除する
  - 解消方法はいくつか考えられるが、今回は全部消してしまう
    - SQL>truncate users;
  - データが削除されていることを確認
    - SQL>select * from users;

36

パスワードをハッシュ化する

- 一通り操作して問題ないことを確認する
  - サインアップ
  - サインイン
  - 2つ以上のユーザー

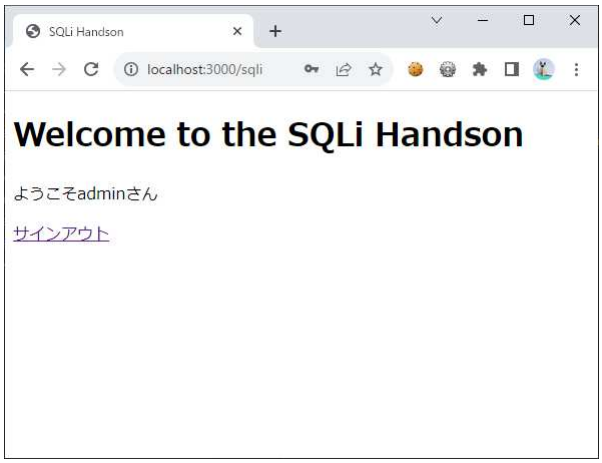
37

おまけ

38

おまけ

- SQLインジェクションを利用して認証を回避できる
  - http://192.168.200.44:3000/sqli
  - 自分用のユーザーを作成する
  - adminでサインインできたら成功



39

おまけ

- SQLインジェクションを対策する
  - routes/sqli.jsを変更する

```
connection.query(
    `select * from users where name = ?;`,
    [username],
    async (error, results) => {
        if (error !== null) {
```

40

今日の振り返り

今日のキーワード

rootアカウント、ハッシュ化、ソルト、
ストレッチング、非同期処理

今日のゴール

- ✓ DBにアクセスするアカウントの扱い方を理解する
- ✓ パスワードをハッシュ化して保存することを理解する
- ✓ よりセキュアなWebアプリを作る

41

Idea IT College Aso
専門学校　イデアITカレッジ阿蘇

脆弱性演習1

セキュリティ診断実践

（2023/10/16）

担当講師：吉井 幸宗（ yoshii@iica.jp ）

Ver.1.0.0

1

今日の内容とゴール

2

今日の内容

- 演習環境の構築
  - VirtualBoxのインストール
  - 仮想マシンイメージのインポート
- 前回のおさらい
  - DBアクセスをよりセキュアにする

3

今日のゴール

✓ AppGoatが動作する環境を作成する

✓ AppGoatを起動する

4

AppGoatについて

5

AppGoat

- 脆弱性の知識と対策方法を学べるツール
  - https://www.ipa.go.jp/security/vuln/appgoat/index.html

6

AppGoat

- 使用中はネットワークから隔離する
  - スタンドアローンの仮想環境を用意する
    - **こちらでやる想定です**
  - AppGoatをPCにインストールし、使用中はWi-Fiを切る
    - 仮想環境が用意できない場合はこちらでやります

7

AppGoat

- 仮想マシンイメージをダウンロードする
  - VirtualBoxの仮想イメージを作成してアップ済み
  - Class roomからダウンロードしてください
- zipファイルを解凍する
  - IICA-AppGoat.ova
  - 解凍が完了したらzipファイルは削除して構いません

8

VirtualBoxのインストール

9

VirtualBoxのインストール

- Oracle VM VirtualBoxとは？
  - PC上に仮想のPC環境を構築することができるソフトウェア
  - https://www.virtualbox.org/
- 類似のツール
  - VMWare
  - WSL2

10

VirtualBoxのインストール

- ダウンロード
  - https://www.virtualbox.org/wiki/Downloads

11

VirtualBoxのインストール

- インストーラを実行
  - VirtualBox-7.0.10-158379-Win.exe
    - 全てデフォルトで進めてOK
- 拡張パックをインストール
  - Oracle_VM_VirtualBox_Extension_Pack-7.0.10.vbox-extpack

12

VirtualBoxのインストール

- VirtualBoxのインストーラが起動しなかった場合
  - Microsoft Visual C++ 2019 Redistributableが必要、といったエラーが発生した場合は以下からダウンロードしてインストールする
  - https://visualstudio.microsoft.com/ja/downloads/#microsoft-visual-c-redistributable-for-visual-studio-2022

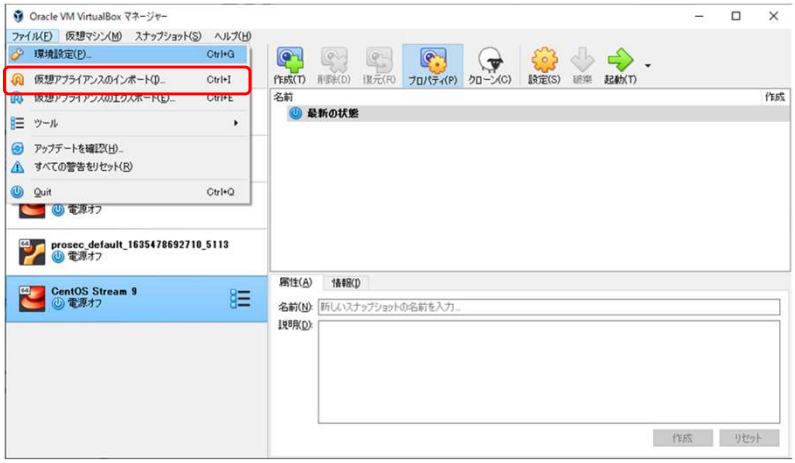
13

仮想マシン

14

仮想マシン

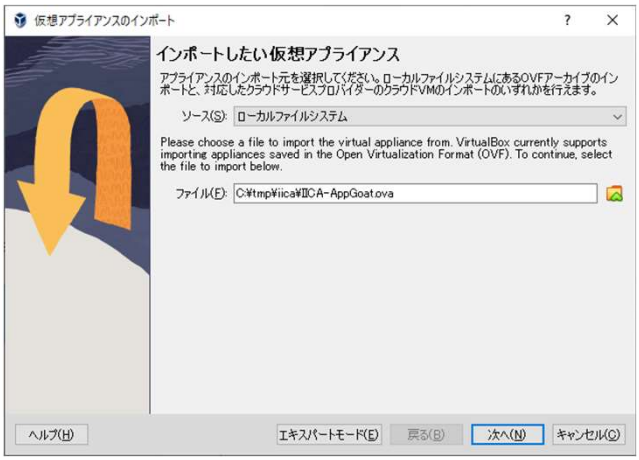
- VirtualBoxを起動
  - ファイル -> 仮想アプライアンスのインポート



15

仮想マシン

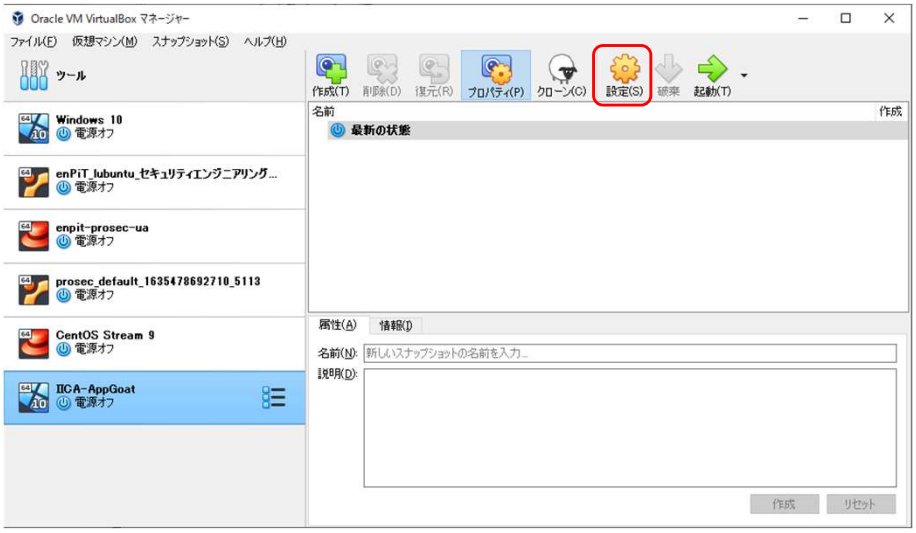
- 仮想マシンイメージファイルを選択する
  - 次へ -> 完了



16

仮想マシン

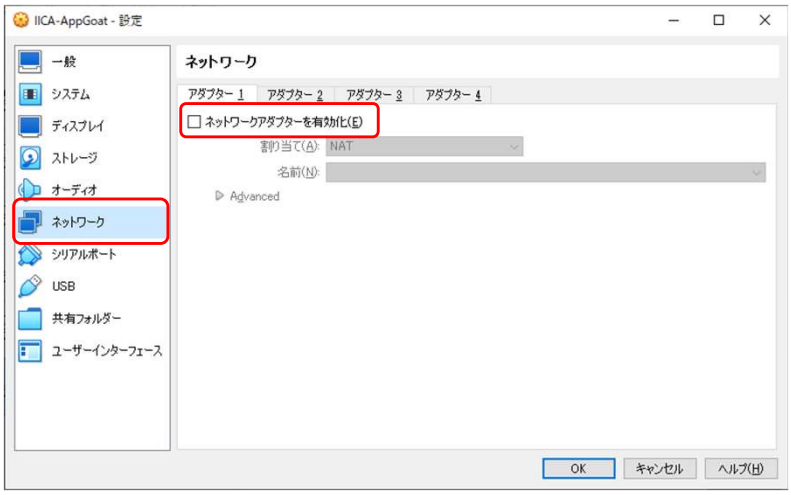
- ネットワークが無効なことを確認する



17

仮想マシン

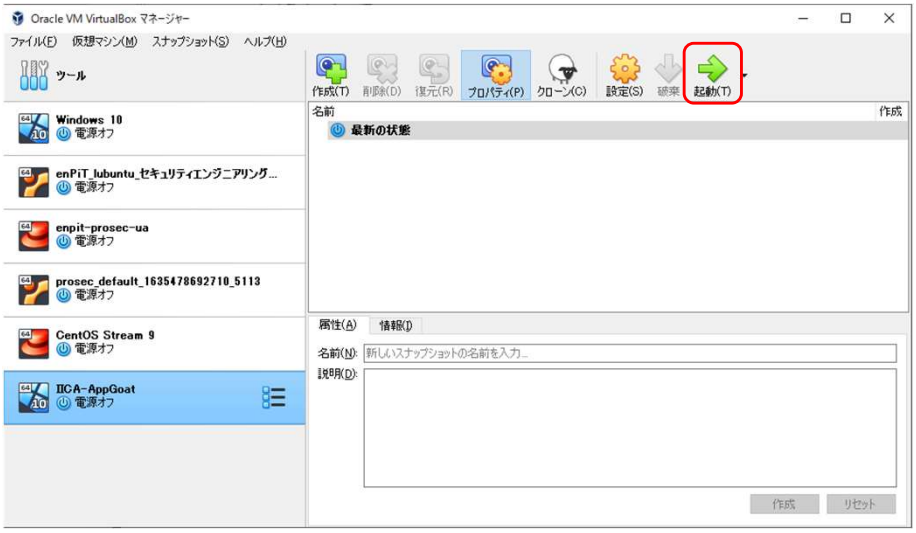
- ネットワークが無効なことを確認する



18

仮想マシン

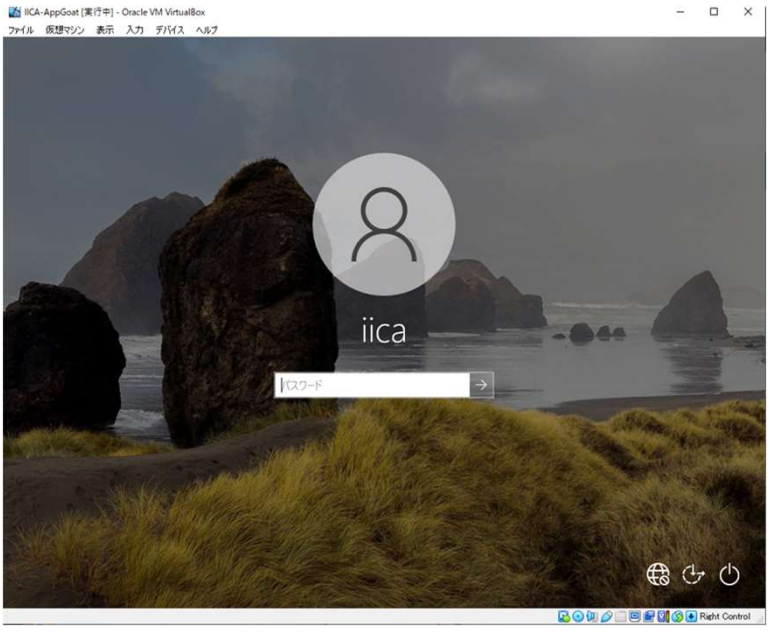
- 起動する



19

仮想マシン

- アカウント
  - iica/iica



20

仮想マシン

- あとかたづけ
  - 無事に起動したらIICA-AppGoat.ovaは削除して構いません

21

AppGoat

22

AppGoat

- AppGoatを起動する
  - デスクトップのショートカットをダブルクリック
  - Apacheを起動
  - ブラウザで総合メニューが表示されたらOK

23

今日の振り返り

今日のキーワード

仮想マシン、VirtualBox、AppGoat

今日のゴール

✓ AppGoatが動作する環境を作成する

✓ AppGoatを起動する

24

Idea IT College Aso
専門学校　イデアITカレッジ阿蘇

脆弱性演習2

セキュリティ診断実践

（2023/10/23）

担当講師：吉井 幸宗（ yoshii@iica.jp ）

Ver.1.0.0

1

今日の内容とゴール

2

今日の内容

- 質問と回答
  - 成果発表の時期
  - アンケートの回答
- AppGoatを使用した脆弱性演習
  - クロスサイトスクリプティング
  - SQLインジェクション
  - クロスサイトリクエストフォージェリ
    - 時間次第

今日のゴール

✓ AppGoatの使い方に慣れる

✓ クロスサイトスクリプティングの演習

✓ SQLインジェクションの演習

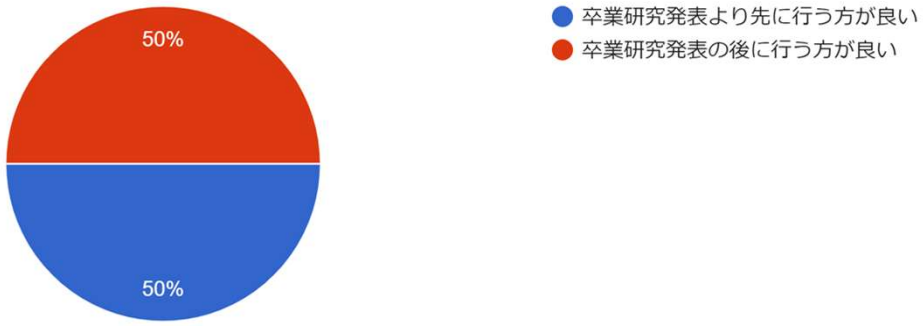
質問と回答

5

質問と回答

成果発表を行うタイミングは卒業研究発表の前か後か、どちらがよいですか？

6 件の回答



6

質問と回答

- 成果発表を行うタイミング
  - 卒業研究発表の後にします
    - 2月26日：準備
    - 3月4日：準備と発表

質問と回答

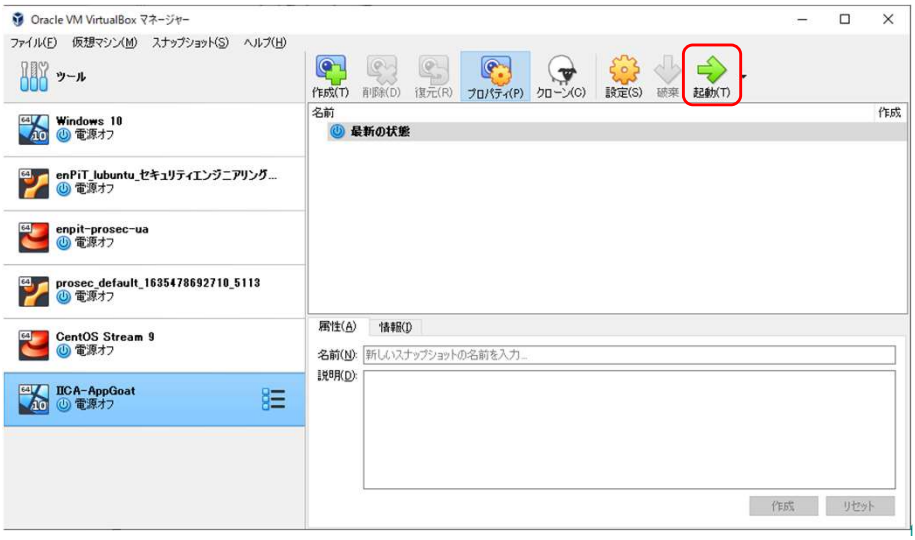
- 授業の前にダウンロードさせてほしかった
  - Classroomで事前に連絡していたがこれだと気づかない？
  - 何かいい方法があれば今後のためにも教えてください
    - 匿名アンケート
- VirtualBoxとHyper-Vの使い分けについて教えて欲しい
  - 好きな方を使うといいです
  - 出来ることはどちらも大体同じ

脆弱性演習

AppGoat

脆弱性演習

- 仮想マシンを起動する
  - iica/iica



脆弱性演習

- クロスサイトスクリプティング
  - AppGoatで演習
  - 終わったらおまけで遊んでみる
    - https://xss-game.appspot.com/

脆弱性演習

- SQLインジェクション
  - AppGoatで演習
  - ここまでが今日の範囲
- クロスサイトリクエストフォージェリ
  - 時間があったらここまでやる

今日の振り返り

今日のキーワード

クロスサイトスクリプティング、SQLインジェクション、
クロスサイトリクエストフォージェリ

今日のゴール

- ✓ AppGoatの使い方に慣れる
- ✓ クロスサイトスクリプティングの演習
- ✓ SQLインジェクションの演習

Idea IT College Aso
専門学校　イデアITカレッジ阿蘇

CTF(Capture The Flag)

セキュリティ診断 実践

（2023/10/30）

担当講師：伴 芳龍（ ban@iica.jp ）

1

今日の流れ

1.CTFの説明

2.CTF

3.問題の解説

2

今日の流れ

今日の内容とゴール

今日の内容

- CTFの説明
- CTFの登録
- 実践
- 問題の解説

今日のゴール

- ✓ CTF（Capture The Flag）について知る。
- ✓ 実際にCTFを行い、前期で学習した内容や

  その他セキュリティで気をつけることなどについて考える。

今日の内容

- CTFの説明
- CTFの登録
- 実践
- 問題の解説

CTF（Capture The Flag）とは

CTF（Capture The Flag） … 答えとなるFlagを探す、セキュリティのコンテスト

クイズのように行われる形式（Jeopardy）、
サーバやアプリケーションに含まれるフラグを（脆弱性を突くことで）
奪取する形式など、複数の形式があります。

Jeopardy形式では、問題を解くことで得られるFLAG{xxx}という形式のデータを
回答させることが多いです。

CTF（Capture The Flag）とは

CTF（Capture The Flag） … 答えとなるFlagを探す、セキュリティのコンテスト

日本ではSECCON（Security Contest）が
年に1回大規模な大会を開催しています。

それ以外にも、民間でCTFを開催されることが
あります。

https://west-sec.com/vs　など…

「SECCON CTF」が3年ぶりにリアル開催 - 1点差の接戦も

2月11日、12日と浅草橋ヒューリックホール＆カンファレンスで国内最大級のCTFイベント「SECCON CTF 2022」の決勝戦が開催された。カンファレンスイベントなども併催され、3年ぶりとなる現地開催は盛り上がりを見せた。

SECCONは、セキュリティの知識や技術を競うコンテスト。2012年にスタートし、今回で11回目。2021年からは総額100万円の賞金も出ている。新型コロナウイルス感染症の影響で前々回、前回とオンライン開催となったが、3年ぶりに現地開催が戻ってきた。

CTF会場の様子。落ち着いた雰囲気で選手が競技に集中している

11月に開催された予選では、1843人がエントリーし、726チームが得点を獲得。決勝大会は予選上位10チームによる「国際決勝」と、国内に限定した上位12チームによる「国内決勝」にわかれて争った。「国際決勝」には国内から東京大学の学生チーム「TSG」も参戦している。

https://www.security-next.com/143843　より引用

今回実施するCTFについて（ルール）

- 今回は、個人戦形式です。
- 試験とは違い、Googleなどでの検索はOKです。
  - むしろ、分からないことを調べるスキルを身につけてほしいです。
  - ただし、ChatGPTなどのAI利用はNGとします。
- ほとんどの問題は、解答数に制限はありません。
  何回でも挑戦できます。
  - 一部の問題は、入力回数を制限します。

今日の内容

- CTFの説明
- CTFの登録
- 実践
- 問題の解説

今回実施するCTFについて（登録方法）

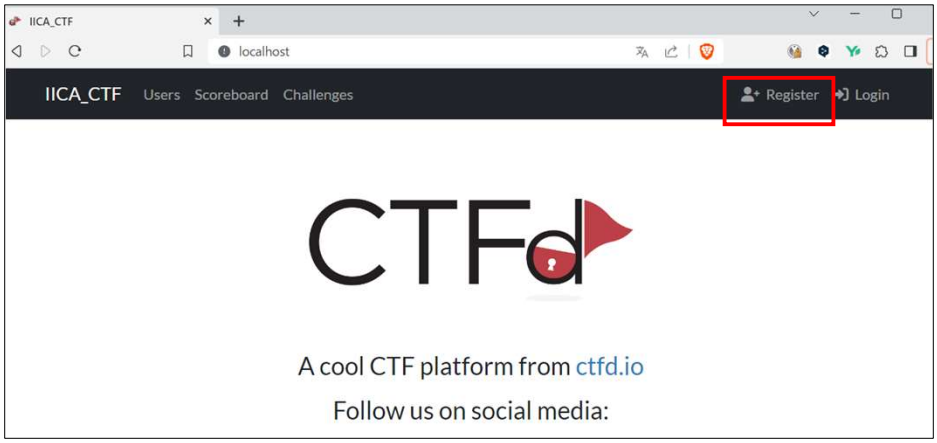
- Webブラウザを開き、以下のURLにアクセスしてください。

http://xxx.xxx.xxx.xxx/

※URLは講義当日に連絡します。

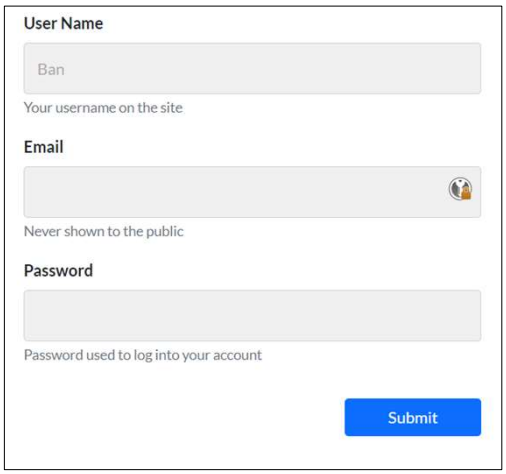
今回実施するCTFについて（登録方法）

- CTFの画面が表示されますので、右上の「Register」をクリックします。



今回実施するCTFについて（登録方法）

- フォームに入力して、「Submit」をクリックします。



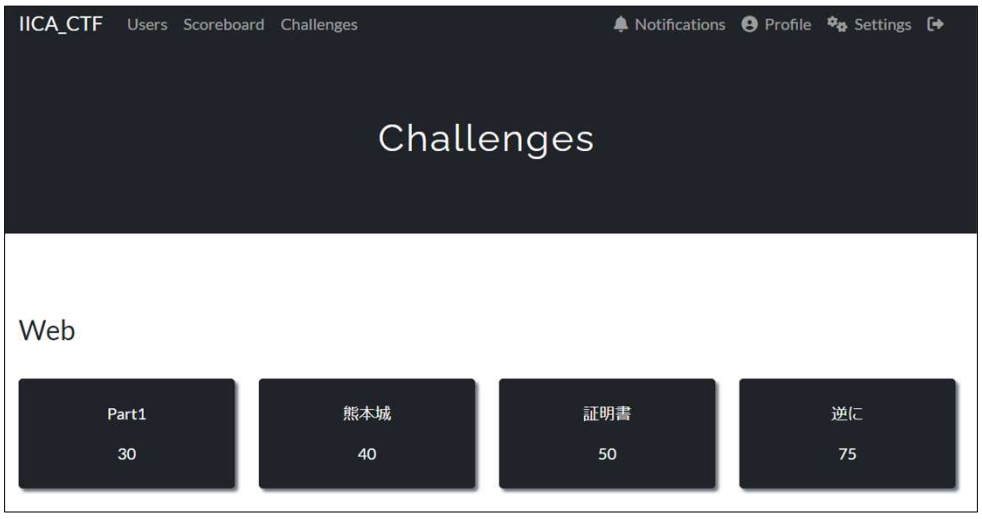
Name：名前を入力します（アルファベット）

Email：aaa@aaa.com　のように、
適当なアドレスを入力します。

Password：好きなパスワードを入力します。

今回実施するCTFについて（登録方法）

- Challenges（問題）が表示されます。



今回実施するCTFについて（問題について）

- 解きたい問題をクリックすると、以下の画面が表示されます。

15

15

今回実施するCTFについて（問題について）

- 解きたい問題をクリックすると、以下の画面が表示されます。

16

16

今回実施するCTFについて（問題について）

- 解きたい問題をクリックすると、以下の画面が表示されます。

今回実施するCTFについて（問題について）

- 問題によっては、以下のような形でFlagが書いてあります。
  - Flag is ○○
  - Flag is “○○”
  - Flag{○○}

  このような場合は、”、{}、isといった部分を含まずに
  ○○　**だけ入力して解答すればOKです**。

- 一部の問題は、得点を使ってヒントを見ることができます。

今日の内容

- CTFの説明
- CTFの登録
- 実践
- 問題の解説

実践

- それでは、実際にCTFに挑戦してみましょう。

http://xxx.xxx.xxx.xxx/

制限時間は○○分（～12:00）とします。

今日の内容

- CTFの説明
- CTFの登録
- 実践
- 問題の解説

問題の解説

- 実際のCTFでは問題の解説（答え合わせ）がされることは少ないです。
  - 参加者がWrite-Upという、自分なりの解答をネットに公開することはあります。
- 今回は講義なので、解答できた人が少なかった問題を中心に正解と解き方を解説します。

今日の振り返り

今日のキーワード

CTF

今日のゴール

- ✓ CTF（Capture The Flag）について知る。
- ✓ 実際にCTFを行い、前期で学習した内容や
  その他セキュリティで気をつけることなどについて考える。

課題について

今日の課題

- Google Classroomにアップします。
- 提出期限：11/6（月）9:00

質疑応答

- 本日の講義の中で、わからなかったこと、気になったことがあれば
  ぜひ質問してください。

- また、授業後の課題（アンケート）、メールでも質問OKです。
  次回の私の講義にて回答します。

25

Idea IT College Aso
専門学校　イデアITカレッジ阿蘇

脆弱性演習3

セキュリティ診断実践
(2023/11/6)

担当講師：吉井 幸宗（ yoshii@iica.jp ）

Ver.1.0.0

1

今日の内容とゴール

2

2

今日の内容

- 質問と回答
- 仮想環境の設定
  - 勝手にシャットダウンする問題の原因と対策
- AppGoatを使用した脆弱性演習
  - クロスサイトスクリプティングの続き
  - SQLインジェクション
  - クロスサイトリクエストフォージェリ
  - and more...

今日のゴール

- ✓ クロスサイトスクリプティングの続き
- ✓ SQLインジェクション
- ✓ クロスサイトリクエストフォージェリ

質問と回答

質問と回答

- レンタルサーバ（lolipop）等を利用したwebページの制作においても、脆弱性対策は必要ですか？
  - 必要です！
- 事前連絡の方法について
  - いくつか意見をいただきました。ありがとうございます。

仮想環境の設定

7

勝手にシャットダウンする問題

- 原因
  - Windows10 評価版
    - ライセンスが切れた状態で使用すると1時間でシャットダウンする
    - ライセンスの期限チェックを定期的に行っている
      - インターネットに接続している必要がある

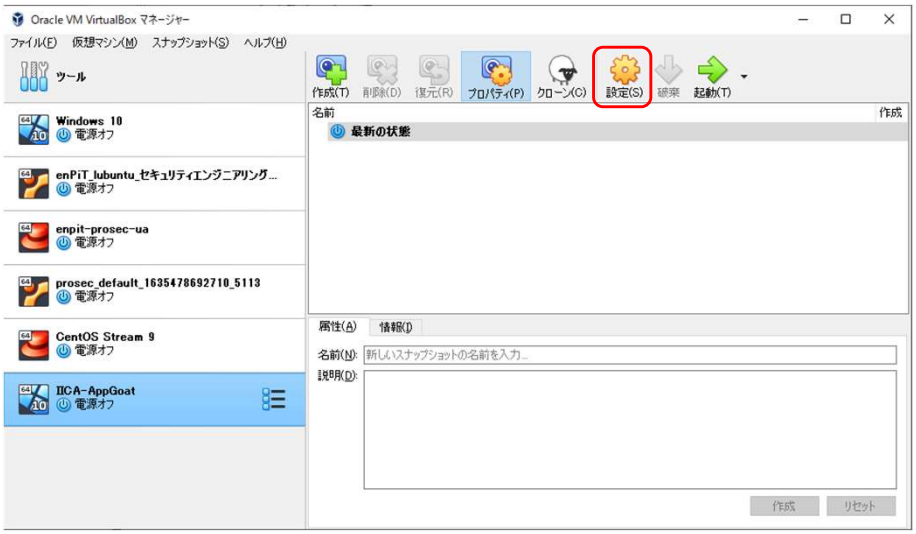
8

勝手にシャットダウンする問題

- 対策
  - インターネットに接続できるようにする
    - ただし、外部からはアクセスされないようにする必要がある

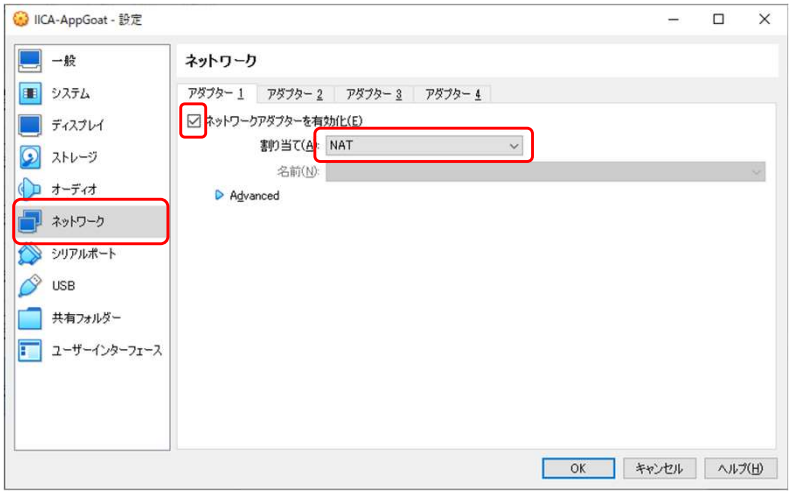
勝手にシャットダウンする問題

- 対策



勝手にシャットダウンする問題

- 対策

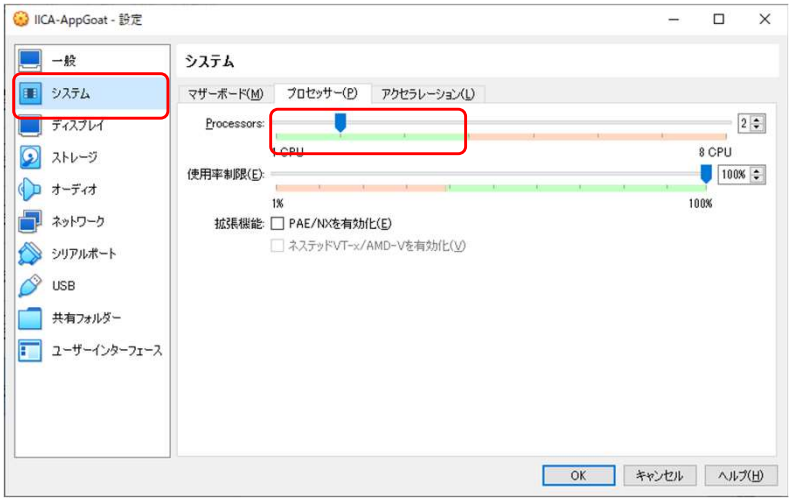


勝手にシャットダウンする問題

- その他の問題
  - ネットワークを有効にしたことでWindowsの裏で色々なプログラムが動くようになり、動作が重くなる現象が発生した
    - 例えばWindows Updateとか

勝手にシャットダウンする問題

- その他の問題



勝手にシャットダウンする問題

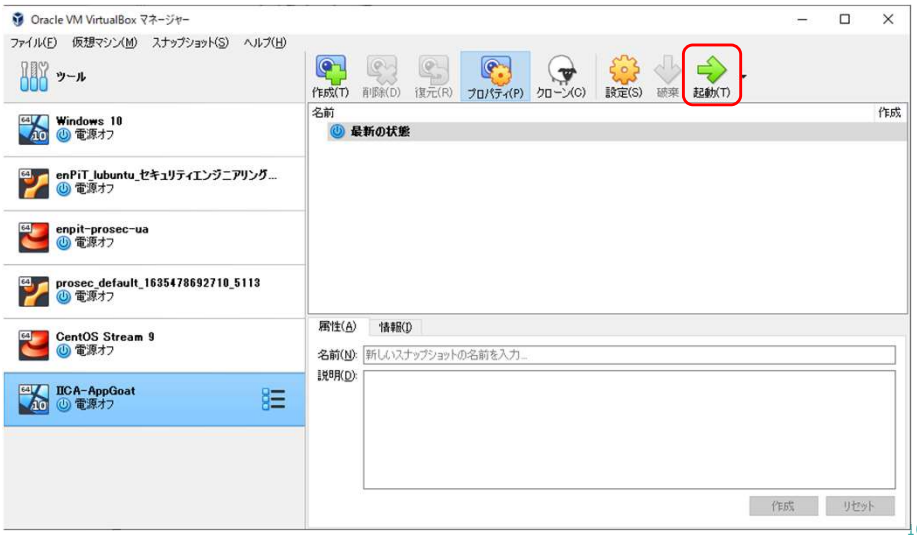
- その他の問題
  - Microsoft Storeを無効化する
    - 勝手に動作してCPU100％を占有してしまうので無効化する
    - 参考：https://jp.easeus.com/partition-manager/wsappx-cpu-memory-high-utilization.html
      - 対処法2.グループポリシーからMicrosoftストアを無効化

脆弱性演習

AppGoat

脆弱性演習

- 仮想マシンを起動する
  - iica/iica



脆弱性演習

- クロスサイトスクリプティング
  - AppGoatで演習
  - 終わったらおまけで遊んでみる
    - https://xss-game.appspot.com/

脆弱性演習

- SQLインジェクション
  - AppGoatで演習
- クロスサイトリクエストフォージェリ
  - AppGoatで演習

今日の振り返り

今日のキーワード

ゲストOS、ホストOS、SQLインジェクション、
クロスサイトリクエストフォージェリ

今日のゴール

- ✓ クロスサイトスクリプティングの続き
- ✓ SQLインジェクション
- ✓ クロスサイトリクエストフォージェリ

Idea IT College Aso
専門学校　イデアITカレッジ阿蘇

脆弱性演習4

セキュリティ診断実践
(2023/11/13)

担当講師：吉井 幸宗（ yoshii@iica.jp ）

Ver.1.1.0

1

今日の内容とゴール

2

今日の内容

- 質問と回答
  - なし
- AppGoatを使用した脆弱性演習
  - SQLインジェクションの続き
  - クロスサイト・リクエスト・フォージェリ
  - ディレクトリ・トラバーサル
  - and more...

今日のゴール

✓ SQLインジェクション

✓ クロスサイト・リクエスト・フォージェリ

✓ ディレクトリ・トラバーサル

AppGoatを使用した演習のゴール

- ✓ 基本
  - ✓ クロスサイト・スクリプティング
  - ✓ SQLインジェクション
  - ✓ クロスサイト・リクエスト・フォージェリ
  - ✓ ディレクトリ・トラバーサル
  - ✓ OSコマンド・インジェクション
  - ✓ セッション管理の不備
- ✓ 応用
  - ✓ 認証制御や認可制御の欠落

5

5

脆弱性演習

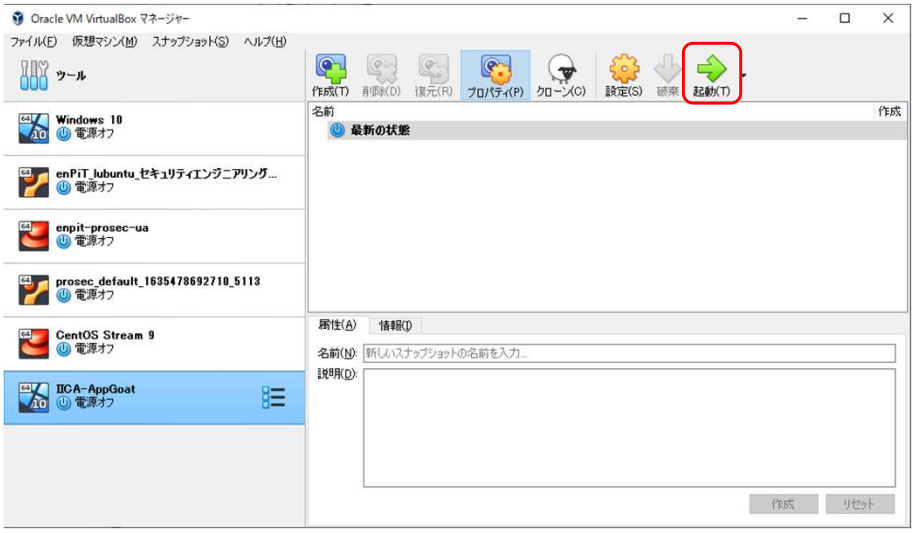
AppGoat

6

6

脆弱性演習

- 仮想マシンを起動する
  - iica/iica



7

7

今日の振り返り

今日のキーワード

ブラインドSQLインジェクション、クロスサイト・リクエスト・フォージェリ、トークン、ディレクトリ・トラバーサル

今日のゴール

- ✓ SQLインジェクション
- ✓ クロスサイトリクエストフォージェリ
- ✓ ディレクトリ・トラバーサル

8

8

Idea IT College Aso
専門学校　イデアITカレッジ阿蘇

脆弱性演習5

セキュリティ診断実践
（2023/11/20）

担当講師：吉井 幸宗（ yoshii@iica.jp ）

Ver.1.1.0

1

今日の内容とゴール

2

2

今日の内容

- 質問と回答
  - なし
- AppGoatを使用した脆弱性演習
  - ディレクトリ・トラバーサル
  - OSコマンド・インジェクション
  - セッション管理の不備
- おしらせ
  - 12月11日の授業について

今日のゴール

✓ ディレクトリ・トラバーサル

✓ OSコマンド・インジェクション

✓ セッション管理の不備

AppGoatを使用した演習のゴール

- ✓ 基本
  - ✓ クロスサイト・スクリプティング
  - ✓ SQLインジェクション
  - ✓ クロスサイト・リクエスト・フォージェリ
  - ✓ ディレクトリ・トラバーサル
  - ✓ OSコマンド・インジェクション
  - ✓ セッション管理の不備
- ✓ 応用
  - ✓ 認証制御や認可制御の欠落

5

5

脆弱性演習

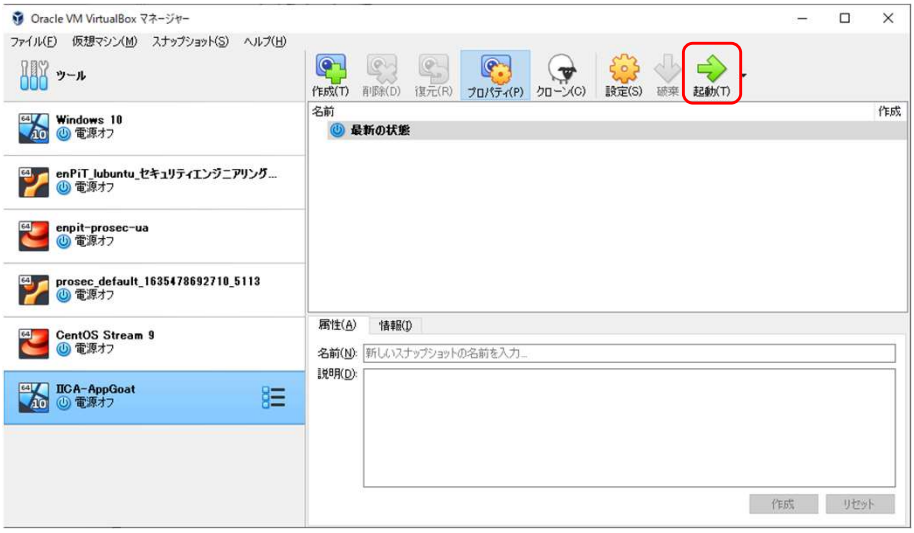
AppGoat

6

6

脆弱性演習

- 仮想マシンを起動する
  - iica/iica



7

7

今日の振り返り

今日のキーワード

ディレクトリ・トラバーサル、OSコマンド・インジェクション、シェル、セッション、セッションハイジャック

今日のゴール

- ✓ ディレクトリ・トラバーサル
- ✓ OSコマンド・インジェクション
- ✓ セッション管理の不備

8

8

おしらせ

12月11日の授業について

おしらせ

- 12月11日の授業について
  - 内田先生のゲスト講義を行います
    - セキュリティ心理学講座

Idea IT College Aso
専門学校　イデアITカレッジ阿蘇

脆弱性演習6

セキュリティ診断実践
（2023/11/27）

担当講師：吉井 幸宗（ yoshii@iica.jp ）

Ver.1.1.0

今日の内容とゴール

今日の内容

- 質問と回答
  - なし
- AppGoatを使用した脆弱性演習
  - セッション管理の不備
  - 認証制御や認可制御の欠落

今日のゴール

✓ セッション管理の不備

✓ 認証制御や認可制御の欠落

AppGoatを使用した演習のゴール

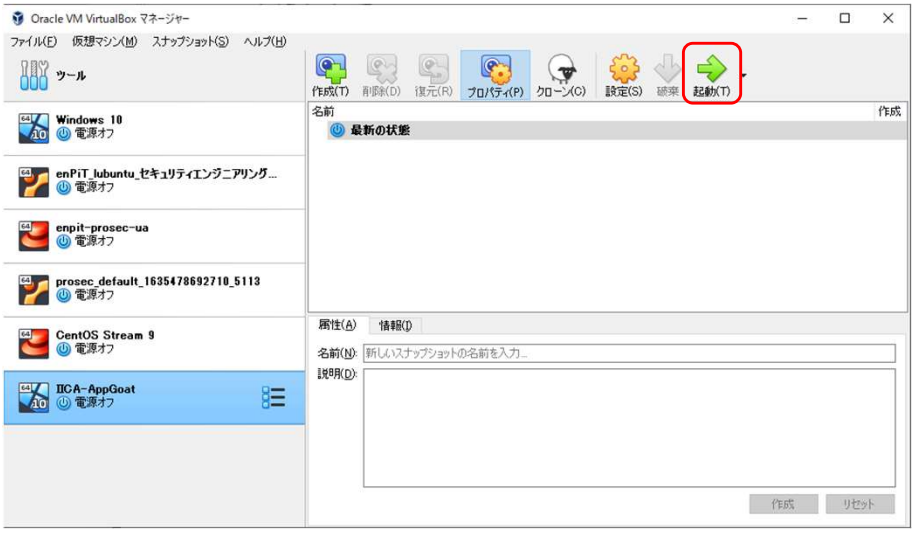
- ✓ 基本
  - ✓ クロスサイト・スクリプティング
  - ✓ SQLインジェクション
  - ✓ クロスサイト・リクエスト・フォージェリ
  - ✓ ディレクトリ・トラバーサル
  - ✓ OSコマンド・インジェクション
  - ✓ セッション管理の不備
- ✓ 応用
  - ✓ 認証制御や認可制御の欠落

脆弱性演習

AppGoat

脆弱性演習

- 仮想マシンを起動する
  - iica/iica



7

今日の振り返り

今日のキーワード

セッションID、セッション・ハイジャック、
セッションIDの固定化、認証、認可

今日のゴール

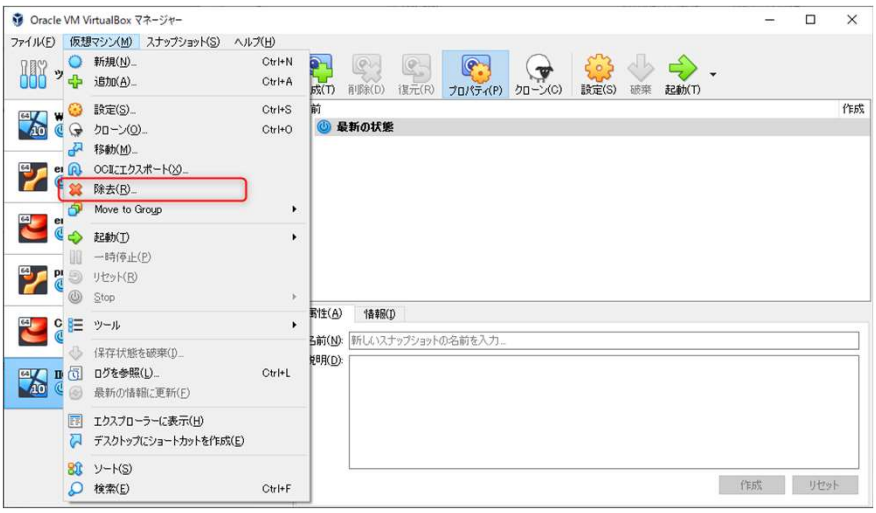
- ✓ セッション管理の不備
- ✓ 認証制御や認可制御の欠落

8

仮想環境の削除

仮想環境の削除

- 不要になった仮想環境を削除する



仮想環境の削除

- 不要になった仮想環境を削除する
  - 「すべてのファイルを削除」をクリック

Idea IT College Aso
専門学校　イデアITカレッジ阿蘇

Webアプリ脆弱性診断1

セキュリティ診断実践
(2023/12/4)

担当講師：吉井 幸宗（ yoshii@iica.jp ）

Ver.1.0.0

1

今日の内容とゴール

2

2

今日の内容

- 質問と回答
  - なし
- 画面遷移図
  - 画面遷移図とは何か？
  - 画面遷移図の作成方法について
  - Bad図書館サイトの画面遷移図を作成する

今日のゴール

✓ 画面遷移図について理解する

✓ Bad図書館サイトの画面遷移図を作成する

画面遷移図

画面遷移図

- 脆弱性診断業務の流れ

対象サイトの全体をざっくりと把握	診断対象となるページを決める。 全機能の診断はコストや期間から合理的ではないため。
↓	
診断対象ページの機能を把握	正常な挙動、各パラメータや必要な事前条件などを確認し **画面遷移図**としてまとめる
↓	
実際に診断作業を行う	ツールによる自動診断と手作業での手動診断を組み合わせる 見つかった点をメモし報告書にまとめる
↓	
報告書の提出、報告会など	わかりやすい報告 場合によっては修正後の再診断なども

画面遷移図

- 画面遷移図とは何か？
  - 診断対象のWebサイトを調査・整理し、Webサイトが動作する際に送信される各種リクエスト（通信）を一覧表にまとめて記載したもの
  - 診断対象のリクエストと診断対象外のリクエストを明確にする

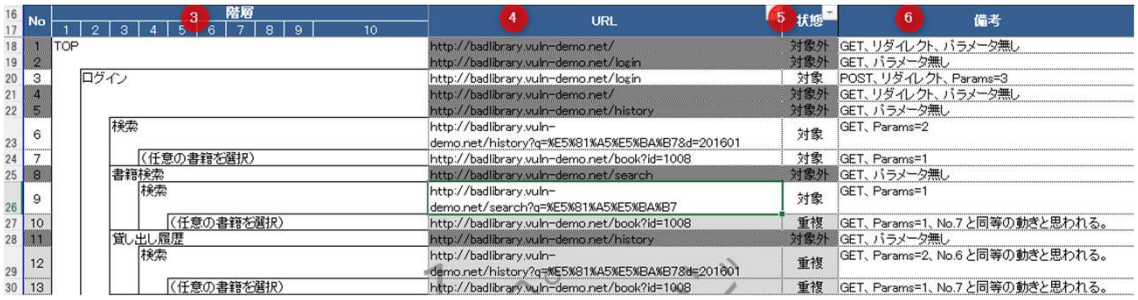
画面遷移図

- 項目詳細

  - 1. サイト名
    - 診断するサイト名
  - 2. リクエスト数
    - 各状態のリクエスト数を集計した値

画面遷移図

- 項目詳細

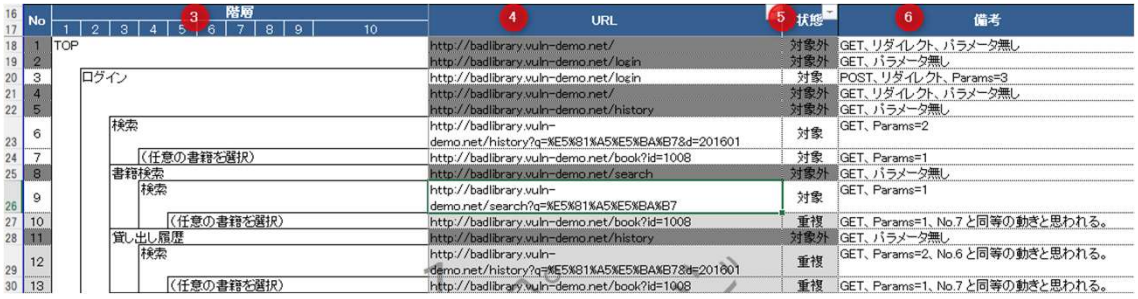


No	3 階層	4 URL	5 状態	6 備考
1	TOP	http://badlibrary.vuln-demo.net/	対象外	GET、リダイレクト、パラメータ無し
2		http://badlibrary.vuln-demo.net/login	対象外	GET、パラメータ無し
3	ログイン	http://badlibrary.vuln-demo.net/login	対象	POST、リダイレクト、Params=3
4		http://badlibrary.vuln-demo.net/	対象外	GET、リダイレクト、パラメータ無し
5		http://badlibrary.vuln-demo.net/history	対象外	GET、パラメータ無し
6	検索	http://badlibrary.vuln-demo.net/history?q=%E5%81%A5%E5%BA%B7&d=201601	対象	GET、Params=2
7	（任意の書籍を選択）	http://badlibrary.vuln-demo.net/book?id=1008	対象	GET、Params=1
8	書籍検索	http://badlibrary.vuln-demo.net/search	対象外	GET、パラメータ無し
9	検索	http://badlibrary.vuln-demo.net/search?q=%E5%81%A5%E5%BA%B7	対象	GET、Params=1
10	（任意の書籍を選択）	http://badlibrary.vuln-demo.net/book?id=1008	重複	GET、Params=1、No.7と同等の動きと思われる。
11	貸し出し履歴	http://badlibrary.vuln-demo.net/history	対象外	GET、パラメータ無し
12	検索	http://badlibrary.vuln-demo.net/history?q=%E5%81%A5%E5%BA%B7&d=201601	重複	GET、Params=2、No.6と同等の動きと思われる。
13	（任意の書籍を選択）	http://badlibrary.vuln-demo.net/book?id=1008	重複	GET、Params=1、No.7と同等の動きと思われる。

  - 3. 階層
    - 後述
  - 4. URL
    - 送信されたリクエストURL

画面遷移図

- 項目詳細



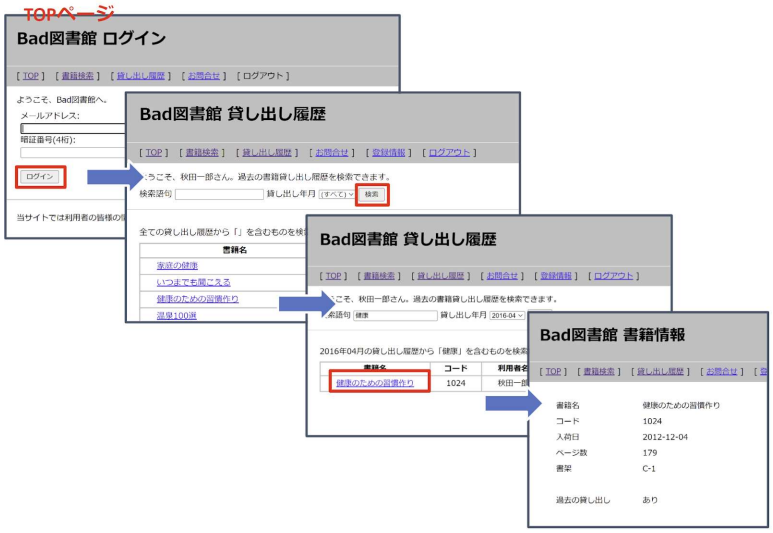
No	3 階層	4 URL	5 状態	6 備考
1	TOP	http://badlibrary.vuln-demo.net/	対象外	GET、リダイレクト、パラメータ無し
2		http://badlibrary.vuln-demo.net/login	対象外	GET、パラメータ無し
3	ログイン	http://badlibrary.vuln-demo.net/login	対象	POST、リダイレクト、Params=3
4		http://badlibrary.vuln-demo.net/	対象外	GET、リダイレクト、パラメータ無し
5		http://badlibrary.vuln-demo.net/history	対象外	GET、パラメータ無し
6	検索	http://badlibrary.vuln-demo.net/history?q=%E5%81%A5%E5%BA%B7&d=201601	対象	GET、Params=2
7	（任意の書籍を選択）	http://badlibrary.vuln-demo.net/book?id=1008	対象	GET、Params=1
8	書籍検索	http://badlibrary.vuln-demo.net/search	対象外	GET、パラメータ無し
9	検索	http://badlibrary.vuln-demo.net/search?q=%E5%81%A5%E5%BA%B7	対象	GET、Params=1
10	（任意の書籍を選択）	http://badlibrary.vuln-demo.net/book?id=1008	重複	GET、Params=1、No.7と同等の動きと思われる。
11	貸し出し履歴	http://badlibrary.vuln-demo.net/history	対象外	GET、パラメータ無し
12	検索	http://badlibrary.vuln-demo.net/history?q=%E5%81%A5%E5%BA%B7&d=201601	重複	GET、Params=2、No.6と同等の動きと思われる。
13	（任意の書籍を選択）	http://badlibrary.vuln-demo.net/book?id=1008	重複	GET、Params=1、No.7と同等の動きと思われる。

  - 5. 状態
    - 診断対象かどうかに関する状態
  - 6. 備考
    - リクエストのメソッドやパラメータの有無（個数）などを記載
      重複のリクエストの場合、どのリクエストと同じと判断したかを記載

画面遷移図

- 項目詳細：3. 階層

No	階層 1	2	3	4	5	6	7	8	9	10
1	TOP									
2										
3		ログイン								
4										
5										
6			検索							
7				（任意の書籍を選択）						
8			書籍検索							
9				検索						
10					（任意の書籍を選択）					
11			貸し出し履歴							
12				検索						
13					（任意の書籍を選択）					



11

11

画面遷移図

- 項目詳細

No	ID	PASS	備考
1	iica2023	iica2023	Basic認証
2	akita@example.jp	1234	一般ユーザー
3			
4			
5			

※ID/PASSなど

- 7. アカウント
  - 利用可能なアカウントの情報

12

12

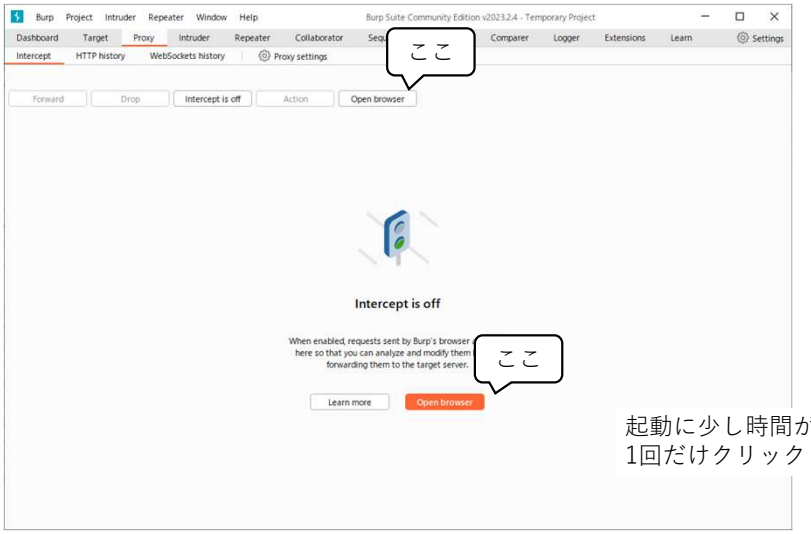
画面遷移図を作成する

Bad図書館サイト

リクエストを記録する

画面遷移図を作成する

- Burpのビルトインブラウザを起動



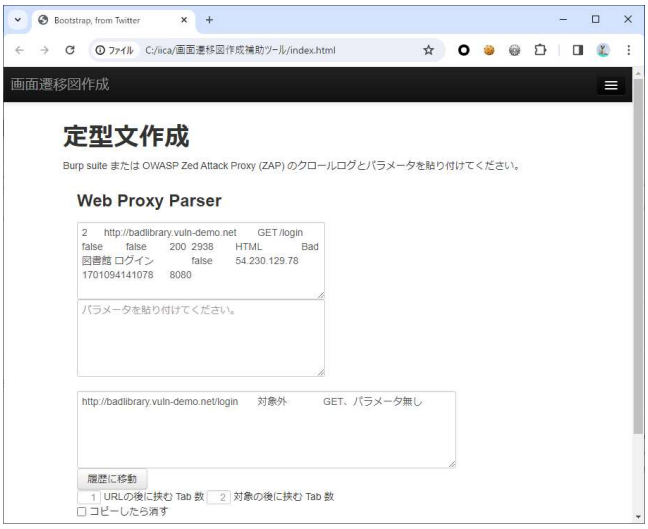
起動に少し時間がかかるので
1回だけクリックして待つ

画面遷移図を作成する

- Bad図書館サイトにアクセス
  - http://badlibrary.vuln-demo.net/
  - Basic認証
    - iica2023/iica2023

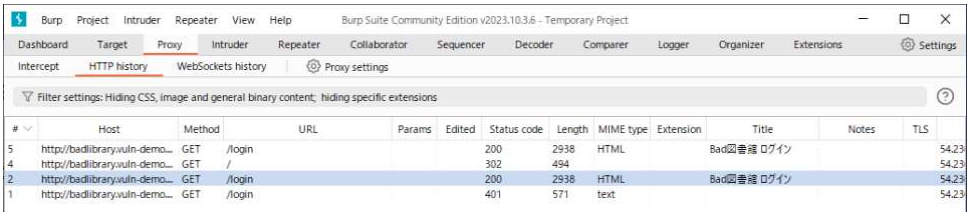
画面遷移図を作成する

- 画面遷移図作成補助ツール



画面遷移図を作成する

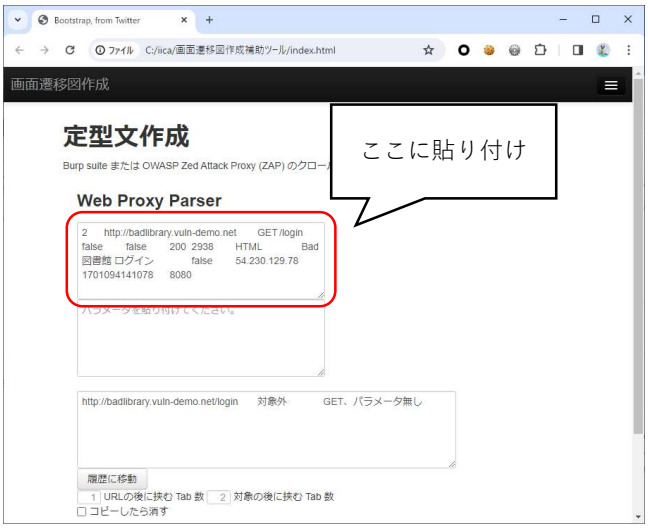
- BurpのURLをコピペする



- Ctrl+Cでコピーして

画面遷移図を作成する

- 画面遷移図作成補助ツール

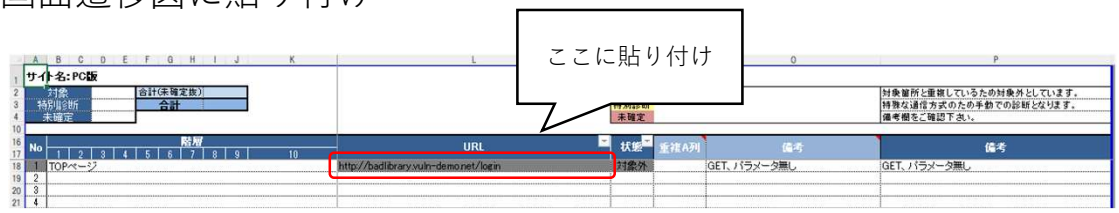


画面遷移図を作成する

- 画面遷移図作成補助ツール

画面遷移図を作成する

- 画面遷移図に貼り付け



  - 「状態」が自動で設定され、「備考」の文言も自動で生成される

画面遷移図を作成する

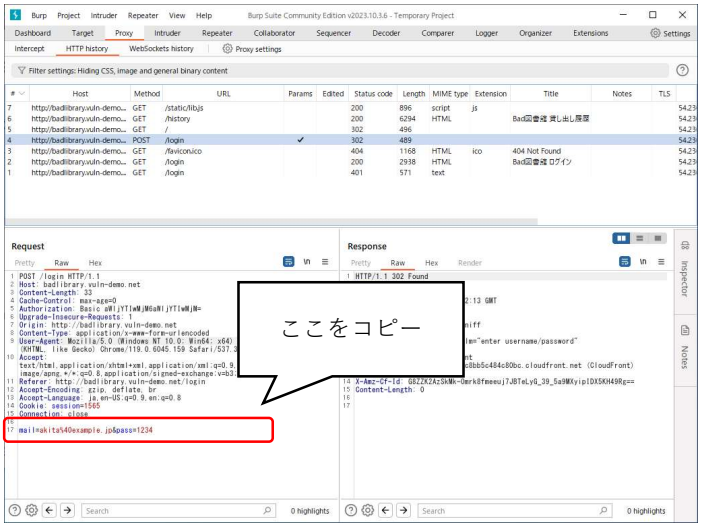
- POSTの場合
  - akita@example.jpでログイン
    暗証番号は「1234」

画面遷移図を作成する

- 画面遷移図作成補助ツール
  - URLのコピペは同様

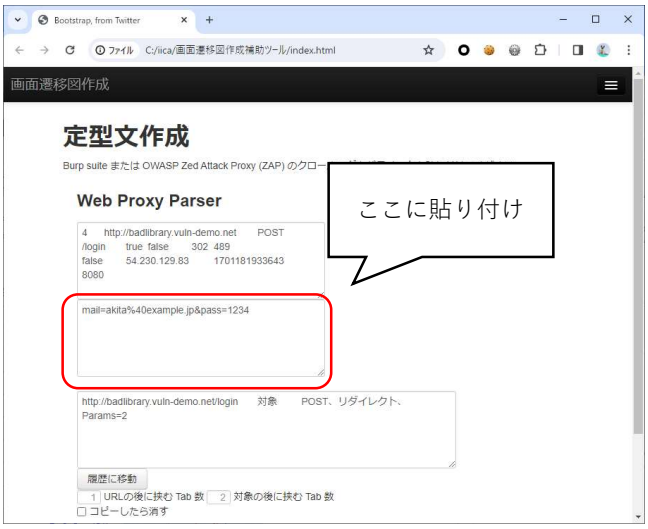
画面遷移図を作成する

- リクエストパラメータをコピー



画面遷移図を作成する

- 画面遷移図作成補助ツール

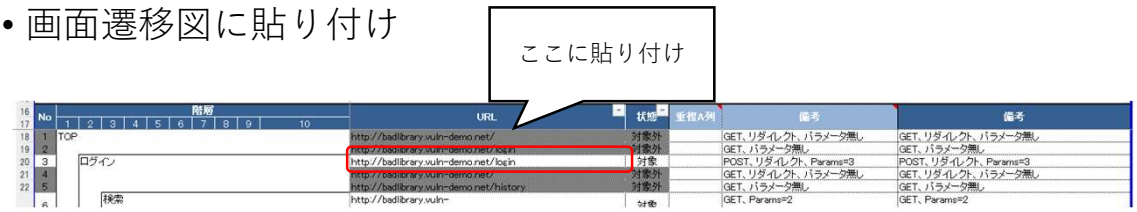


画面遷移図を作成する

- 画面遷移図作成補助ツール

画面遷移図を作成する

- 画面遷移図に貼り付け



  - 検査対象のパラメータがあるので、状態が「対象」に設定される
  - 備考欄の右側にパラメータを貼り付ける

画面遷移図を作成する

- アカウントを記載する

※ID/PASSなど

No	ID	PASS	備考
1	iica2023	iica2023	Basic認証
2	akita@example.jp	1234	一般ユーザー
3			
4			
5			

重複チェック

画面遷移図を作成する

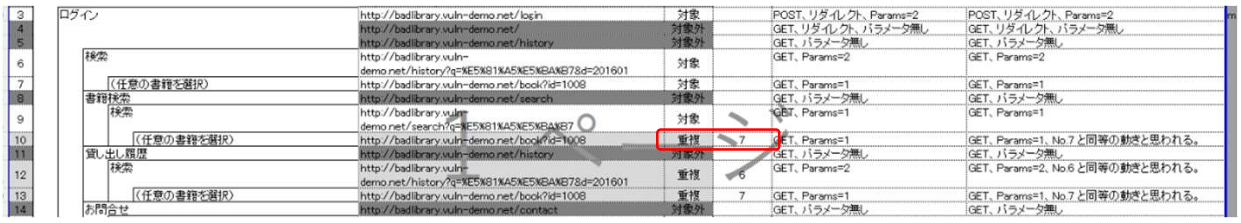
- 重複するリクエスト
  - 次の条件を満たすリクエスト
    - URLが同じ
    - パラメータ数が同じ
    - すべてのパラメータ名が同じ
  - どれか1つを診断対象とし、他は状態を「重複」にする
    - 重複するリクエストは診断対象外
    - 重複A列に該当するNo.のセルを入力する
      - 「=Ax」のような形式で記入

画面遷移図を作成する

- 重複するリクエスト
  - GETの場合
    - URLの末尾に続くパラメータの名前が完全に一致するか？
    - パラメータの順番は問わない
  - POSTの場合
    - 右端の欄外に記載したパラメータの名前が完全に一致するか？
    - パラメータの順番は問わない

画面遷移図を作成する

- 重複するリクエスト



3	ログイン	http://badlibrary.vuln-demo.net/login	対象		POST、リダイレクト、Params=2	POST、リダイレクト、Params=2
4		http://badlibrary.vuln-demo.net/	対象外		GET、リダイレクト、パラメータ無し	GET、リダイレクト、パラメータ無し
5		http://badlibrary.vuln-demo.net/history	対象外		GET、パラメータ無し	GET、パラメータ無し
6	検索	http://badlibrary.vuln-demo.net/history?q=%E5%81%A5%E5%BA%B78d=201601	対象		GET、Params=2	GET、Params=2
7	（任意の書籍を選択）	http://badlibrary.vuln-demo.net/book?id=1008	対象		GET、Params=1	GET、Params=1
8	書籍検索	http://badlibrary.vuln-demo.net/search	対象外		GET、パラメータ無し	GET、パラメータ無し
9	検索	http://badlibrary.vuln-demo.net/search?q=%E5%81%A5%E5%BA%B7	対象		GET、Params=1	GET、Params=1
10	（任意の書籍を選択）	http://badlibrary.vuln-demo.net/book?id=1008	重複	7	GET、Params=1	GET、Params=1、No.7と同等の動きと思われる。
11	貸し出し履歴	http://badlibrary.vuln-demo.net/history	対象外		GET、パラメータ無し	GET、パラメータ無し
12	検索	http://badlibrary.vuln-demo.net/history?q=%E5%81%A5%E5%BA%B78d=201601	重複	6	GET、Params=2	GET、Params=2、No.6と同等の動きと思われる。
13	（任意の書籍を選択）	http://badlibrary.vuln-demo.net/book?id=1008	重複	7	GET、Params=1	GET、Params=1、No.7と同等の動きと思われる。
14	お問合せ	http://badlibrary.vuln-demo.net/contact	対象外		GET、パラメータ無し	GET、パラメータ無し

※対象外のリクエストは重複チェックしなくてよい

仕上げ

画面遷移図を作成する

- お化粧マクロ
  - 「階層」の見た目を整える

No	階層									
	1	2	3	4	5	6	7	8	9	10
1	TOP									
2										
3		ログイン								
4										
5										
6			検索							
7				(任意の書籍を選択)						
8			書籍検索							
9				検索						
10					(任意の書籍を選択)					
11			貸し出し履歴							
12				検索						
13					(任意の書籍を選択)					
14			お問合せ							
15				送信						
16					送信					
17			登録情報							
18			ログアウト							
19										
20										

画面遷移図を作成する

- 完成
  - お客様に提出して確認してもらう
    - 様々な要因で対象が増減することもある
  - 最終的に合意できたら診断開始

今日の振り返り

今日のキーワード

画面遷移図、診断対象リクエスト

今日のゴール

- ✓ 画面遷移図について理解する
- ✓ Bad図書館サイトの画面遷移図を作成する

セキュリティ心理学入門
～ Human Element ～
その1：ヒューマンエラー　Human Error

2023. 12. 11
イデアITカレッジ阿蘇
内田 勝也

0

セキュリティ心理学
～ Human Element ～

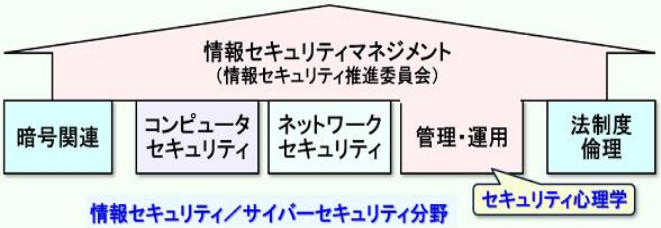
はじめに

なぜ、セキュリティ心理学か？ ⇦ セキュリティは、技術だけの問題ではない

- People are not the weakest link, they are the primary attack vector
  人間はウィーケストリンク（最弱部分）でなく、最初の攻撃対象である
- People are not as rational as they think they are and often make mistakes in simple decision making
  人間は自分が思うほど合理的でなく、単純な意思決定でもしばしば過ちを犯す
- If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.
  技術でセキュリティの問題を解決できると思うのは、問題も技術も理解していない　Bruce Schneier

(*) Bruce Schneier is an American cryptographer, computer security professional, privacy specialist, and writer. Schneier is a Lecturer in Public Policy at the Harvard Kennedy School[2] and a Fellow at the Berkman Klein Center for Internet & Society as of Nov., 2013.

楽しいセキュリティを！



ウィーケストリンクでセキュリティレベルを判断する
- ◆セキュリティレベルは、セキュリティ対策の平均値でない
- ◆最弱所が そのシステムのセキュリティレベル

Determine Security Level with Weakest link
- ◆ Security level is not an average of security measures
- ◆ The weakest point is the security level of the system.

Katsuya Uchida　uchidak@gol.com

1

セキュリティ心理学 ～ Human Element ～

はじめに

なぜ、セキュリティ心理学か？ ⇦ セキュリティは、技術だけの問題ではない

- Security First　July 1, 2002　(http://www.govtech.com/security/Security-First.html)
  - Howard Schmidt, the former Chief Security Officer at Microsoft, speaks about the national plan and other cyber security issues. (元ホワイトハウス サイバーセキュリティコーディネーター)

Q: What kinds of technology will be needed to stave off electronic attacks? Do we need bigger anti-virus programs?

A: The common misconception is this is a technology issue. But it's not a technology issue. For example, the DOD did an analysis last year and it's somewhere in the high 90s, like 97% to 98% of things that have hit the DOD systems have been the result not of some new piece of technology but exploitation of people that have not had processes in place to install patches or to configure their systems properly.

米国国防総省の調査では、 97～98%は「パッチ未適用か設定ミス」

パッチ未適用も設定ミスも、「やるべき事をやらなかった(不作為)」であり、ヒューマンエラーと考えることができる

Howard Schmidt
1949.10.05～2017.03.02

不作為: 当事者・組織がやるべきことをやらなかったため、問題が発生したが、当事者・組織は、
① 実行しなかったことを自覚はある： 実行可能な環境でなかった／実行が面倒であった
② 実行しなかったことの自覚がない： 知識がないため、行うべき行為を実施しなかった

2

セキュリティ心理学 ～ Human Element ～

ヒューマンエラーへの誤解

国内では特にヒューマンエラーに対する誤解が多い。 ヒューマンエラーは、『緊張感が足りない』、『やる気がない』、『注意力が散漫』という個人の問題と考えられる。 このため、

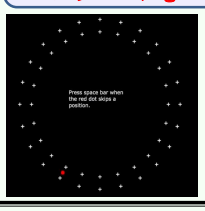
従来型対処方法は、
ヒューマンエラーは，作業者の原因と考える人が多く、
① 注意をしていれば、エラーは防げる
② 教育・訓練や動機づけで防げる
③ 複数人で確認・チェックすれば防げる
と言われるが・・・

Many people think that human error is caused by workers,
① Errors can be prevented by paying attention
② Can be prevented by education, training, and motivation
③ Can be prevented if multiple workers check and confirm

① 注意をしていれば、エラーは防げる(？)
- 下表は、各段階のエラー発生率を示した。「Ⅲ正常、明晰状態」であれば、エラーはゼロに近づく(ゼロにはならない)が、長時間維持できない
- Ⅲの状態の維持は、30分程度[注]と言われている

段階	意識モード	生理的状態	エラー発生率
Ⅰ	意識ボケ	疲労、居眠り	0.1以上
Ⅱ	正常、リラックス	定例作業時	0.01～0.0001
Ⅲ	正常、明晰状態	積極活動時	0.000001以下
Ⅳ	興奮状態	慌てている時 パニックの時	0.1以上

Norman Mackworth (ノーマン・マックワース) の研究
時計の文字盤が真っ白な盤面上を時計の黒い指針が毎秒1回の割合で持続的に時刻を刻み、100ステップで1周する。 この指針は時折通常の2倍で進む場合がある。 これを被験者は、7フィート離れた位置で、監視し、この現象が発生したら、キーを押す。 この実験を2時間行うと、30分過ぎる辺りから、検出能力が落ちた
「ビジランス(Vigilance)の30分効果」とも言われる



Mackworth Clock Test
https://www.infosecpsychology.com/Movies/Mackworth.mp4

3

セキュリティ心理学
～ Human Element ～

ヒューマンエラーへの誤解

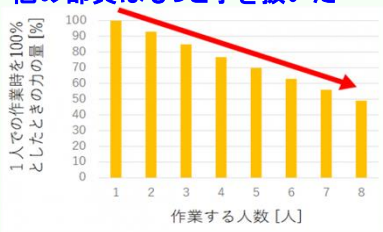
ヒューマンエラーの誤解

従来型対処方法(1)の表

③ 複数人での確認・チェックは、エラーの可能性は低くなるが、『Ⅲ正常、明晰状態』の状態を長く維持できなければ、エラー発生の可能性はある。 更に、複数人の場合、他者への依存度が高くなるため、一人一人のエラー率が悪くなり、全体のエラー発生率があまり良くならないこともある（リンゲルマン効果）

「社会的手抜き」Social loafing　(https://sites.google.com/site/jssppr/discover_psychology)

- 1人で綱引きをした時に綱を引く力の強さを100%とすると、2人で綱を引いた時の1人当たりの力は93%、3人で85%、8人では49%／人 に減少した
- 集団で暮らすのに最適なように進化した私たちは、人に頼ったり、責任が分散することで、集団だと手を抜くことを覚えた
- 綱引きを究めた綱引き連盟の人たちは、ほとんど1人あたりの力は低減しなかった
- 普通の人でも手抜きを防ぐ方法として、チアリーダーが綱引き中に応援してくれた。筋骨隆々組をチアリーダーたちが「がんばれ！がんばれ！」と応援すると1人ずつの時とほぼ同程度の力を出した
- サッカー部員で「特定の1人だけ名前を呼んで応援」すると、その部員は手抜きをせず頑張ったが、他の部員はもっと手を抜いた



Ringelmann, M. (1913). Recherches sur les moteurs animés: Travail de l'homme. [Research on animate sources of power: The work of man] Annales de l'Institut National Agronomique, 2nd series, 12, 1-40.

Katsuya Uchida　uchidak@gol.com

4

セキュリティ心理学
～ Human Element ～

ヒューマンエラーをどう防ぐか？

CRM (Crew Resource Management)

- 個人からチームへ：1976年、NASA は技術・経験豊富なベテランクルー36組を集めてシミュレーターを使い膨大な実験を行った。その結果、適切な状況認識を行いチームワークが取れていれば無事に乗り越えられるはずの負荷・トラブルから生還出来たのは1組であった。この実験結果を解析したNASA は1979年に「コックピットにおけるリソース・マネジメント（Cockpit Resource Management：CRM）」の中で
  ① 積極的コミュニケーション　② 機長のリーダーシップ
  ③ 適切な権威勾配　④ 正確な意思決定等
  のヒューマンファクターに関わる訓練が航空機事故を減少させるために大変重要であると指摘
- 1995年 アメリカ連邦航空局（FAA: Federal Aviation Administrations）が同訓練を米国航空会社に義務付けた
  1998年 日本も義務化された
- 心技体に優れ、あらゆる訓練・試験をこなしつつ10年以上の経験を経て初めて機長となるが，個人の能力には限界があり（過ちは人の常）コックピット内の人的・機械的なすべてを発揮しないと最高の安全性は保てないというのがCRMの中核で、利用可能な資源（知識・経験を含む人間や情報、機器）を有効に活用してこそ航空安全を実現する。 即ち，コミュニケーションやチームワークを向上させヒューマンエラーを防ぎ、チームの業務遂行能力を向上してゆくこととされる
  ① CRM 訓練の変遷：CRM訓練は，当初の個人の行動改善を主体としたものからチームのパフォーマンスへと対象を拡大し，名称もCockpitから「Crew」に変更し，Crew を客室乗務員、地上運航管理者、整備士にも拡大し領域を広げた。さらにエラーを有益な情報源と捉えるエラーマネジメント（Error Management）の導入、運航乗務員のエラーの発生の可能性を高める潜在的要素を脅威（Threat）とし事故防止上この脅威に適切に対処することが重要との認識から、TEM（Threat and Error Management）に重点を置いたものへと変化してきた
  ② CRM の他分野への広がり：航空事故削減のために開発されたCRMは、限られた作業現場内におけるヒューマンエラーの諸問題に焦点を当てるとともにチーム全体のパフォーマンスを高めるという汎用性、普遍性により、他分野にも拡大している

医療現場への適用（ Team STEPPS ）

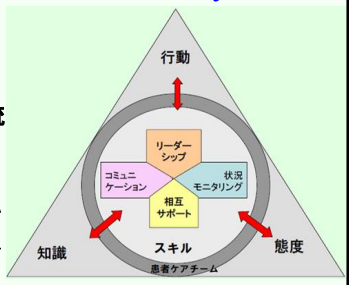
Katsuya Uchida　uchidak@gol.com

5

セキュリティ心理学 ～ Human Element ～

ヒューマンエラーをどう防ぐか？

Team STEPPS (Team Strategies and Tools to Enhance Performance and Patient Safety)



1. リーダーシップ

チーム活動を理解し、変化する情報をチームメンバーと共有し、必要な人的・物的資源の確実な供給によりチームメンバーの活動を調整する能力で、適切な労務管理を行うとともに、定期／不定期の打ち合わせを積極的に行うことで意識統一をはかる

2. 状況モニタリング

チームとして協働するため、周囲や自己の状況を積極的に解析・評価し、それを共有することで、エラーの発生を防止する方法を示す。 状況評価に関する個人差をなくすため、評価項目を定めて継続して評価することを推奨

3. 相互支援

責任感や労働負荷などを正確に評価し、他メンバーの要求や状況を把握し、労働や知識を支援する。情報や状況の不認識による誤った判断は必ず繰り返し、呈示し、指摘する「2回チャレンジルール」、不安なことは不安であると躊躇せず表現する「CUS（カス）」等がある。職種、経験年数に関係なく、患者の安全第一だと思ったことは何でも言える、聞ける雰囲気を作り、安全性を飛躍的に高める

4. コミュニケーション

コミュニケーション関連医療事故は全体の2／3以上ある。 チームSTEPPSはチームメンバー間の情報伝達を、誤りなく順序立て、確実に行うプロセスとして、(1)SBAR：エスバー(Situation-Background-Assessment-Recommendation)状況が正確に伝わるよう、状況、背景、評価、提案という順番で連絡を取る方法、(2)コールアウト：重大事態に際してより緊急性の伝わる状況の伝え方、(3)チェックバック：正確な情報伝達のため情報の発信、受領、再確認を決まりとして行う、(4)ハンドオフ：申し送り項目を共通化することでエラーの発生を防止する方法、等がある

6

セキュリティ心理学 ～ Human Element ～

楽しいセキュリティを！

楽しいセキュリティをやろう！

- セキュリティは、本来楽しいものです。 厳格な規則で縛るのは、専門性がないからかも知れません
- 参考： CGOドットコム「ギャル式ブレスト」 https://cgo-gal.com/
  https://www.youtube.com/watch?v=ftD9bWkQ84o

明るい明号、楽しいセキュリティ！

ブレーンストーミング（Brainstorming）

- 自由に意見を出し合い，新たな発想を生み出したり、アイデアを昇華させる会議手法
- ここから画期的な商品やサービス、社内制度や取り組みなどが生まれることも
- Brainstorming is a group problem-solving method that involves the spontaneous contribution of creative ideas and solutions. This technique requires intensive, freewheeling discussion in which every member of the group is encouraged to think aloud and suggest as many ideas as possible based on their diverse knowledge.

この様な考えを『心理的安全性』と言う。

7

セキュリティ心理学 ～ Human Element ～

ヒューマンエラーをどう防ぐか？（実践）

- ヒューマンエラー対策は，**個人の質を高めることで，不適格者を排除するものでない**
- 以下のビデオは，ヒューマンエラーではないが，組織で教育・訓練を考える上で参考になる

参考： NHK クローズアップ現代「あらゆる人材を戦力に ～変わる雇用の現場～」2015年6月29日

- 作業を徹底的に可視化：口頭での教えを**異物の選別作業を写真と名前**で示し、教えた
- 繰り返しの確認で、ほぼ理解している
- 障害者雇用率：８％ （1年で達成）
  厚労省基準： 2.4％（2018.04.01～）

- 多くの業務遂行で利用可能！
- ヒューマンエラー防止に活かす

進捗状況・遅延等、ボードを見れば判断可能

- 作業の**見える化の典型例**。 ここでは、障害者の作業を工夫し、非常に効率的な作業を行っている
- この進捗ボードは大手運送会社も利用。作業者全員に**情報公開、共有し エラー削減を目指す**

8

セキュリティ心理学 ～ Human Element ～

ヒューマンエラーをどう防ぐか？

作業の可視化を徹底！ NHK クローズアップ現代 「あらゆる人材を戦力に ～変わる雇用の現場～」2015年6月29日

9

セキュリティ心理学 ～ Human Element ～

ヒューマンエラーをどう防ぐか？ 教育・訓練による脆弱性の認識を

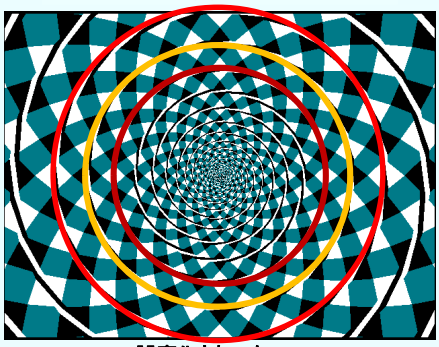
基本的な教育・訓練を考える

- 普段理解していると思っていることでも、意外と正しく理解していないことが多い。以下はその例
  - 「駐車禁止マーク」正しいマークは 左？ 右？ その理由は？
    マークをみたことがない人はいないが、2択だから適当に回答しても正答の可能性もあるが、理由を聞くと回答できない
  - 「フレイザーの錯視」は、知らない限り、誤魔化される。 経験の重要性を考えて欲しい
  - 「ミュラー・リヤーの錯視」は 良く知られているが、安易に知識・経験だけで判断しない
- カクテルパーティ効果：大勢の人が雑談をしていても、自分が興味ある会話や自分の名前等は聞き取れる。 興味がないと「見えない」、「聞こえない」ことがある（「選択的注意」ともいう）

駐車禁止マーク（確実な記憶法）

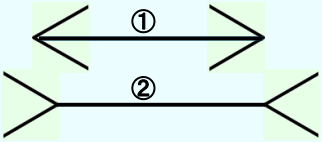
正しい駐禁マークは？
また、その理由は？

フレイザーの錯視（経験の重要性）



誤魔化されてない？

ミュラー・リヤーの錯視（確認の大切さ）



どちらが長い？

Katsuya Uchida uchidak@gol.com

10

セキュリティ心理学 ～ Human Element ～

ヒューマンエラーをどう防ぐか？ 他分野の知見から学ぶ（原子力）

組織の心理学 IAEA（国際原子力機関）の安全文化の確立

鎌田晶子「『組織風土』とヒューマンエラー」（大山正・丸山康則 編「ヒューマンエラーの科学」）

安全風土・安全文化の考察 『Safety Culture』（1986.04.26 チェルノブイリ原発事故）

国際原子力機関（IAEA）の国際原子力安全諮問グループ（INSAG）がまとめた報告書（1991年）
安全文化とは『原子力施設の安全性の問題が、すべてに優先し、その重要性にふさわしい注意が払われること』が実現されている組織・個人における姿勢・ありようを集約したもの
「安全」とは、技術的な意味で原子力施設を運転しても、放射能漏れなどの事故を引起こす危険がないことをいう。原子力施設の「安全」は、施設の設備の健全性と、施設の運転管理をする人間の「安全文化」の徹底によって実現される。このような努力で「安全」を積み重ね、事業者や規制機関が情報公開を行い、地元の人々に「安心」を提供することができる。
組織内の全ての個人が安全に対し責任を負い、基本方針、管理者、個人の3階層のレベルがある

- 基本方針レベル： 政府・経営層等、組織の高い意思決定レベルの決定事項で、組織・個人活動を左右する
- 管理者レベル： 基本方針に則った個人の態度や慣行を醸成する環境作りと制度の整備
- 個人レベル： 安全業務遂行前に、自分の任務、責任、知識が十分か、状況に異常がないか、支援が必要か等を問いかける姿勢で臨むことが求められる。 規則・手順等を遵守し、問題発生時には立ち止まって考え、近道や大胆な行動を避けるような厳密かつ慎重なアプローチで臨まなければならない

【日本における安全文化の取り組み】
チェルノブイリの事故対応で安全文化の重要性が認識されたが、当時の日本の原発は優れた運転実績を上げており、安全文化を自らの問題と考えなかった（？）

WEB セミナー「IAEA 安全文化の解明」（資料はウェブにありません）

日本のシステム技術者の奢り？（1995年 阪神大地震 高速道路崩壊）

1994 Northridge earthquake（米国 ノースリッジ地震）

Katsuya Uchida uchidak@gol.com

11

ヒューマンエラーをどう防ぐか？
セキュリティガイドライン（OECD）

OECD セキュリティガイドライン ～セキュリティ文化の普及に向けて ～（2002年7月版）

2002年に公開された本ガイドラインでは、「セキュリティ文化（Culture of Security）の普及」を唱っている。私見だが、IAEAの報告書のタイトルは『Safety Culture』で、安全文化を述べており、これを参考にして、OECDは、『Culture of Security』としたと考えている

Ⅰ セキュリティ文化の普及　外務省の仮訳を編集　http://www.mofa.go.jp/mofaj/gaiko/oecd/security_gl_a.html

- セキュリティ文化の促進は，変化するセキュリティ環境に対応するもので，このガイドラインは，情報通信システムの安全な設計及び利用が後知恵の結果であったことが余りにも多かった時代との明確な決別の合図で，参加者は情報通信システム 及び関連するサービスに一層依存するようになっており，これらすべてが信頼でき，かつ安全なものであることが必要となっている。すべての参加者の利益，情報通信システム及び関連サービスの性質を適切に考慮したアプローチのみが，効果的なセキュリティを提供し得る
- 各参加者は，セキュリティ確保の重要な担い手で，自らの役割に応じ，関連するセキュリティリスクと予防手段を認識し，責任を持って，情報通信システムのセキュリティ強化の措置をとるべき
- セキュリティ文化の普及は，リーダーシップと広範な参画が必要で，全ての参加者間でセキュリティの必要性が理解され，セキュリティ計画及びマネジメントに高い優先順位が与えられるべき
- セキュリティの課題は，政府，企業等の全レベル，全参加者が関心と責任を持つ事項
- このガイドラインは，社会全体でセキュリティ文化普及の取組み基礎で，参加者が全ての情報通信システムの設計・利用にセキュリティを組込むことができ，全参加者が情報通信システムの運用を考え，評価し，影響を与える方法として，セキュリティ文化を取入れ，普及を提案する

注）情報システム及びネットワーク，ネットワーク及びシステム を「情報通信システム」とする

Katsuya Uchida　uchidak@gol.com

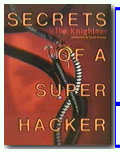
12

ヒューマンエラーをどう防ぐか？
教育・訓練（歴史から学ぶ）

教育・訓練手法について

ネットワーク構築から、約50年になり、その間 多くの課題が発生しており、過去（歴史）から学ぶ必要もある。　更に、事故・事件から現在、将来を考えることも大切になる

- 情報共有：ハンガーフライト（Hangar Flight）
  - 航空業界のCRM（Crew Resource Management）に、「ハンガーフライト（Hangar Flight）」があった。天候の悪化で パイロットは、天候の回復を待つため、格納庫（Hangar）に集まり、経験談や自慢話を行い、情報交換／情報収集等を行った。他人の経験を学び、成長した
  - セキュリティでは，過去のインシデントをりようし、情報共有を行い，将来発生する事件・事故への対処を考える良い機会になる
    愚者は経験に学び、賢者は歴史に学ぶ
    Fools say they learn from experience; I prefer to learn from the experience of others.



1994 (1995) UNIX ディフォルト → 2004.10 LINUX ディフォルト → 2013.11 ネットワーク複合機 → 2013.11 監視カメラ → IoT

既知のユーザID / PWの組合せ

脆弱性の指摘
Secret of a Super Hacker
シークレット・オブ・ スーパーハッカー

踏み台の危険性	情報漏洩（イメージ）	情報のぞき見
東芝 インターネット接続	ネットワーク複合機各社	監視カメラ（ネットワーク接続）
「ネットdeナビ」機能搭載	複合機HDD内のイメージ	監視画像ののぞき見
HDD／DVDビデオレコーダー	（印刷，コピー，FAX等の内容）	

Katsuya Uchida　uchidak@gol.com

13

セキュリティ心理学 ～ Human Element ～

Garbage in, Garbage out!

Garbage in, Garbage out!【ゴミを入れれば，ゴミしかでてこない！】

最近，気になっている言葉がこれ！

『ゴミを入れれば，ゴミしか出てこない』　『Garbage in Garbage out!』

どんなに処理が良くても，データがゴミであれば，その処理結果はゴミでしかない．

一時，『ビックデータ』の時代だと言われた頃，適切なデータでなければ，結果が悪くなりますよね？ と質問してきた方がいました．それで，この言葉で説明したことがある．

もう少し言えば，コンピュータ処理は，以下の手順を踏む

EDPS：
Electronic Data Processing System

【入力処理】⇒【データ処理】⇒【出力処理】

【データ処理】は，計算（Computing）でなく，データ（情報）の保存・検索だと，青山学院大学の学長等の経歴を持つ『鵜沢昌和先生』から教えを受けた．

最近のマイナンバーシステムでの不祥事の最大の問題は，【入力軽視】であろう！

今回のトラブルでは，入力処理は，自分達に関係ない。そこは重要ではないと指摘する有識者もいる．

サイボウズの青野社長は

デジタル大臣は、「一連の事案の原因は事務処理の誤りなどで、
マイナンバー制度そのものに起因しているわけではない」と述べた。
マイナンバーシステムの問題ではなく、人的ミスだとの主張だ

人的ミスが発生している多くは，【入力処理】部分であり，この部分が正しくできていなければ，システム全体はボロボロになるのは，上記の諺が示している．

データ処理以降では，正しいデータを扱うので，よほどレベルの低いプログラマーでなければ，エラーになる可能性は低い（今回のコンビニ交付は，その例外かも知れない），コンビニ交付を 出力処理 だと考えることもできる．

セキュリティ心理学 ～ Human Element ～

Garbage in, Garbage out!

Garbage in, Garbage out!【ゴミを入れれば，ゴミしかでてこない！】

入力処理も出力処理も適切にできていなかった．

コンビニ交付 を ヒューマンエラー だと考えるかどうかは別にしても，もう少し対応が可能であった気がするのは，古いシステム屋のボヤキかも知れないが・・・

マイナンバーシステムを考える場合，入力処理の部分の多くは，国民一人一人が関係する部分のはず．

先日，韓国ツアーに参加したが，自治体が住民の「リテラシー教育」を行っていた．日本でも，ボランティア的にコンピュータ等に詳しい高齢者を講師にして，リテラシー教育（システムだけでなく，セキュリティも）を行うことができるはず．

マイナンバーシステムが，重要な案件であればあるほど，入力処理をどの様に行うかを関係各所は，ぜひ真剣に考え，推進して欲しい．

かつて，銀行のATMの普及で 銀行内のエラーを減らした．従来は，入出金用の用紙と通帳を窓口に持参し，窓口の行員が処理を行い，現金の出し入れなどを行った．

ATMの導入により，預金者がATMを操作し，現金の出し入れを行う．ATMのトラブルを除いて，問題は【行員から預金者】に移った．窓口の行員によるエラーはなくなり，そのための対応も銀行では不要になった．

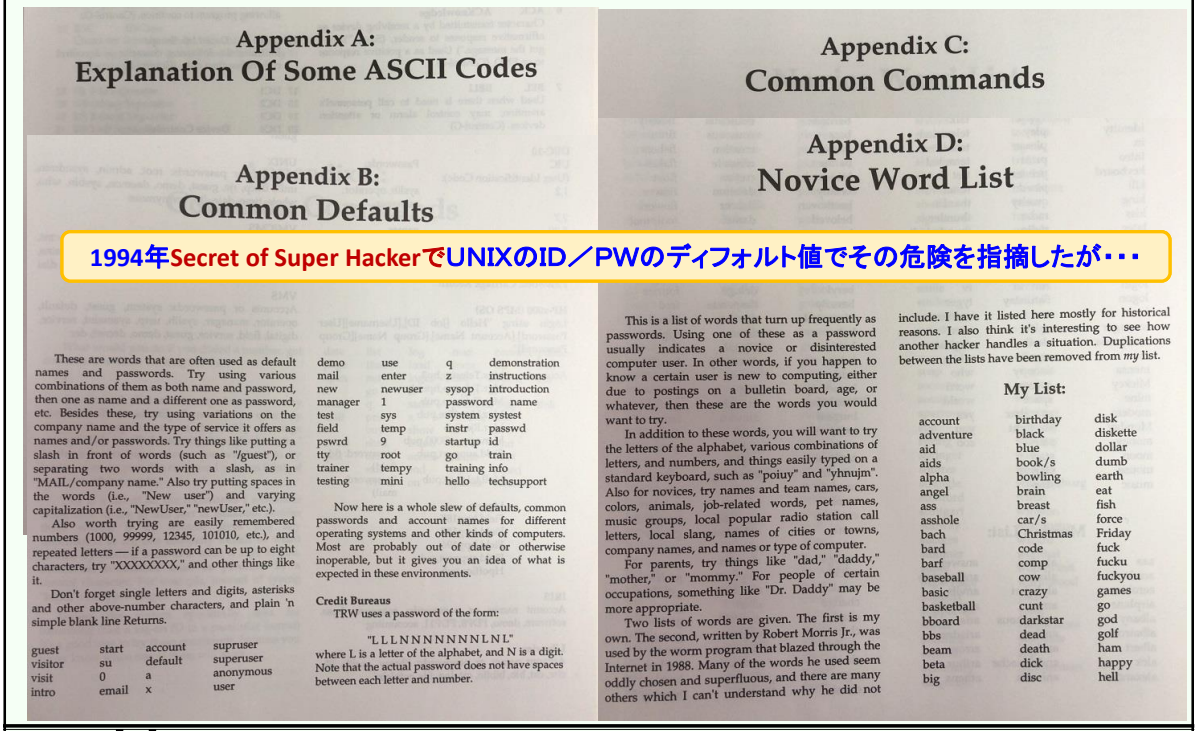
マイナンバーシステム関連の処理では，健康保険証の問題だけでなく，今後とも色々発生してくるのであろう！

金融機関のATM的対応ができるかを見守っていきたい・・・

注） 思っていた通りの展開」…サイボウズ青野社長に聞く
「マイナカード」トラブル解決の唯一の方法とは
https://news.yahoo.co.jp/articles/003bdbcc7448650e75f88f6ca5a7d3082d110118

セキュリティ心理学 ～ Human Element ～

ヒューマンエラーをどう防ぐか？
教育・訓練（歴史から学ぶ）



Appendix A:
Explanation Of Some ASCII Codes

Appendix B:
Common Defaults

Appendix C:
Common Commands

Appendix D:
Novice Word List

1994年Secret of Super HackerでUNIXのID／PWのディフォルト値でその危険を指摘したが・・・

These are words that are often used as default names and passwords. Try using various combinations of them as both name and password, then one as name and a different one as password, etc. Besides these, try using variations on the company name and the type of service it offers as names and/or passwords. Try things like putting a slash in front of words (such as "/guest"), or separating two words with a slash, as in "MAIL/company name." Also try putting spaces in the words (i.e., "New user") and varying capitalization (i.e., "NewUser," "newUser," etc.).

Also worth trying are easily remembered numbers (1000, 99999, 12345, 101010, etc.), and repeated letters — if a password can be up to eight characters, try "XXXXXXXX," and other things like it.

Don't forget single letters and digits, asterisks and other above-number characters, and plain 'n simple blank line Returns.

guest	start	account	supruser
visitor	su	default	superuser
visit	0	a	anonymous
intro	email	x	user

demo	use	q	demonstration
mail	enter	z	instructions
new	newuser	sysop	introduction
manager	1	password	name
test	sys	system	systest
field	temp	instr	passwd
pswrd	9	startup	id
tty	root	go	train
trainer	tempy	training	info
testing	mini	hello	techsupport

Now here is a whole slew of defaults, common passwords and account names for different operating systems and other kinds of computers. Most are probably out of date or otherwise inoperable, but it gives you an idea of what is expected in these environments.

Credit Bureaus
TRW uses a password of the form:

"LLLNNNNNNNLNL"
where L is a letter of the alphabet, and N is a digit. Note that the actual password does not have spaces between each letter and number.

This is a list of words that turn up frequently as passwords. Using one of these as a password usually indicates a novice or disinterested computer user. In other words, if you happen to know a certain user is new to computing, either due to postings on a bulletin board, age, or whatever, then these are the words you would want to try.

In addition to these words, you will want to try the letters of the alphabet, various combinations of letters, and numbers, and things easily typed on a standard keyboard, such as "poiuy" and "yhnujm". Also for novices, try names and team names, cars, colors, animals, job-related words, pet names, music groups, local popular radio station call letters, local slang, names of cities or towns, company names, and names or type of computer.

For parents, try things like "dad," "daddy," "mother," or "mommy." For people of certain occupations, something like "Dr. Daddy" may be more appropriate.

Two lists of words are given. The first is my own. The second, written by Robert Morris Jr., was used by the worm program that blazed through the Internet in 1988. Many of the words he used seem oddly chosen and superfluous, and there are many others which I can't understand why he did not include. I have it listed here mostly for historical reasons. I also think it's interesting to see how another hacker handles a situation. Duplications between the lists have been removed from *my* list.

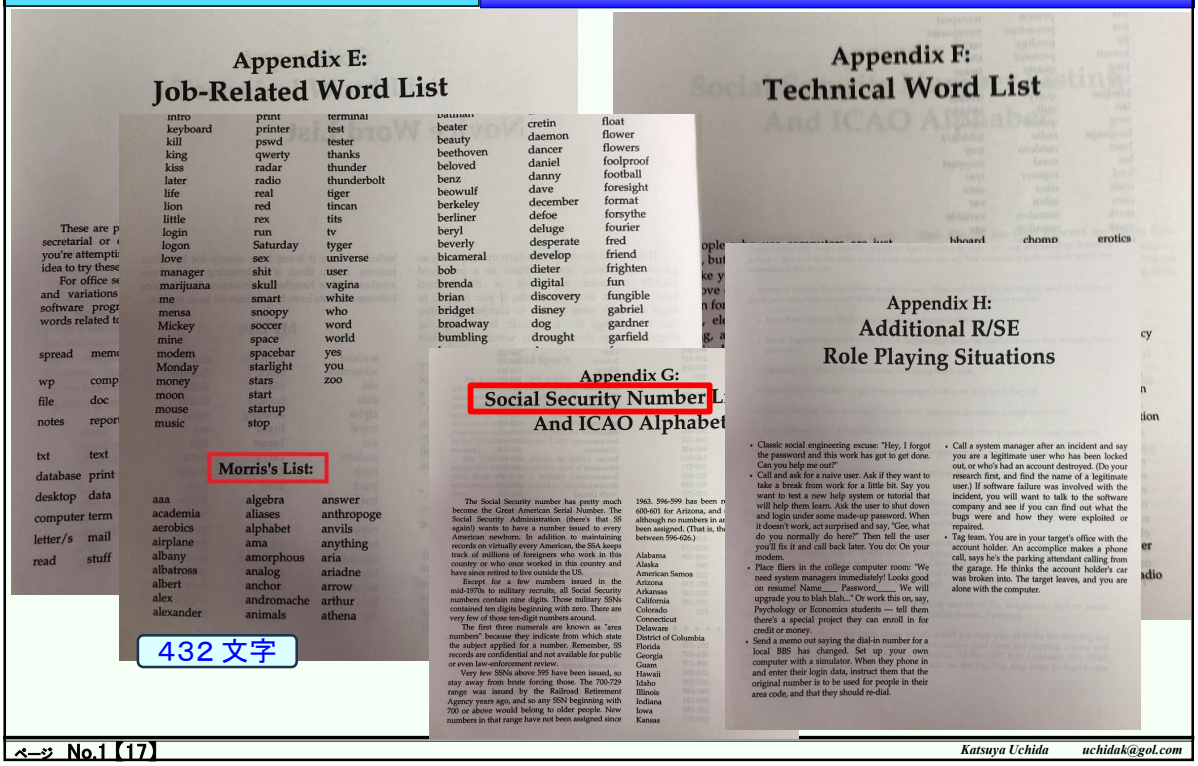
My List:

account	birthday	disk
adventure	black	diskette
aid	blue	dollar
aids	book/s	dumb
alpha	bowling	earth
angel	brain	eat
ass	breast	fish
asshole	car/s	force
bach	Christmas	Friday
bard	code	fuck
barf	comp	fucku
baseball	cow	fuckyou
basic	crazy	games
basketball	cunt	go
bboard	darkstar	god
bbs	dead	golf
beam	death	ham
beta	dick	happy
big	disc	hell

16

セキュリティ心理学 ～ Human Element ～

Appendices of Secret of Super Hacker



Appendix E:
Job-Related Word List

Appendix F:
Technical Word List

Appendix G:
Social Security Number
And ICAO Alphabet

Appendix H:
Additional R/SE
Role Playing Situations

Morris's List:

intro	print	terminal					
keyboard	printer	test					
kill	pswd	tester	beater	cretin	float		
king	qwerty	thanks	beauty	daemon	flower		
kiss	radar	thunder	beethoven	dancer	flowers		
later	radio	thunderbolt	beloved	daniel	foolproof		
life	real	tiger	benz	danny	football		
lion	red	tincan	beowulf	dave	foresight		
little	rex	tits	berkeley	december	format		
login	run	tv	berliner	defoe	forsythe		
logon	Saturday	tyger	beryl	deluge	fourier		
love	sex	universe	beverly	desperate	fred		
manager	shit	user	bicameral	develop	friend		
marijuana	skull	vagina	bob	dieter	frighten		
me	smart	white	brenda	digital	fun		
mensa	snoopy	who	brian	discovery	fungible		
Mickey	soccer	word	bridget	disney	gabriel		
mine	space	world	broadway	dog	gardner		
modem	spacebar	yes	bumbling	drought	garfield		
Monday	starlight	you					
money	stars	zoo					
moon	start						
mouse	startup						
music	stop						

aaa	algebra	answer
academia	aliases	anthropoge
aerobics	alphabet	anvils
airplane	ama	anything
albany	amorphous	aria
albatross	analog	ariadne
albert	anchor	arrow
alex	andromache	arthur
alexander	animals	athena

432 文字

17

セキュリティ心理学入門
～ Human Element ～
ソーシャルエンジニアリング Social Engineering

2023.12.11
イデアITカレッジ阿蘇
内田 勝也

18

セキュリティ心理学 ～ Human Element ～

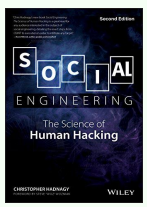
ソーシャルエンジニアリングの定義

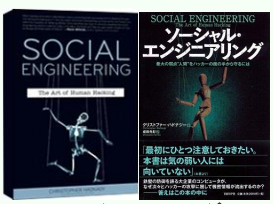
定まった定義はないが、以下の様に考えている

- 【wikipedia】人を操って行動を起こさせたり，機密情報を漏らさせたりする行為。 信用詐欺や単純な詐欺に似ているが，この用語は通常，情報収集，不正行為，あるいはコンピュータ・システムへのアクセスの目的で，ペテンにかけたり騙したりすることに適用される。 多くの場合，攻撃者が被害者と顔を合わせることはけしてない
- 【クリス・ハドナジー SE: The Science of Human Hacking】人に影響を与え、その人の利益になるかならないかわからない行動を取らせるあらゆる行為のことである
- 【内田 勝也】人間の心理的な弱さのを利用や他人になりすまし、必要な情報を収集（盗み見、盗取、ヒアリング）し，更に、いくつかの方法を組み合わせる、複数人や方法、場所等で情報収集を行うこともある。犯罪に利用されるだけでなく、医者や弁護士、コンサルタント，お笑い芸人等 多くの職種の人が意識／無意識に利用している

- ソーシャルエンジニアリング関連の書籍はあまり出版されてない感じがある
- 狭いセキュリティ分野でなく，医者や弁護士，コンサル等を含めて考えることが，ソーシャルエンジニアリングの認知が進む可能性がある
- クリスは，「利益になるかならないかわからない行動」と言っており，内田は，医者や弁護士、コンサルタント，お笑い芸人等 多くの職種の人が意識／無意識に利用しているものと定義している

翻訳本なし
Social Engineering:
The Science of Human Hacking





ソーシャル・エンジニアリング
2010年12月 翻訳 2012年11月

シークレット・オブ・スーパーハッカー
(Secret of a Super Hacker)
1994年、翻訳1995年

19

ソーシャルエンジニアリングの手法

ソーシャルエンジニアリングの手法

① **なりすまし**：他人になりすまし，必要な情報を収集する。電話利用が多いが，電子メールや手紙，FAX 等の利用もある
最近の**標的型攻撃**や**フィッシング**の多くは電子メールによる方法を利用している

② **ゴミ箱漁り**：トラッシング（Trashing）とか，Dumper Diving と呼ばれ，廃棄されたゴミから，目的情報を取得する。ハードディスク等の磁気媒体やCD，DVD，マニュアル，報告書，重要書類等を回収し，有効情報を得る

③ **サイト侵入**：清掃員，電気・電話工事人，警備員等になりすまし，オフィスや工場等に侵入

④ **のぞき見**：他人のものをのぞき見するもので，情報が机上やコンピュータ上に露出しているものを意識的にのぞき見し，情報収集を行う

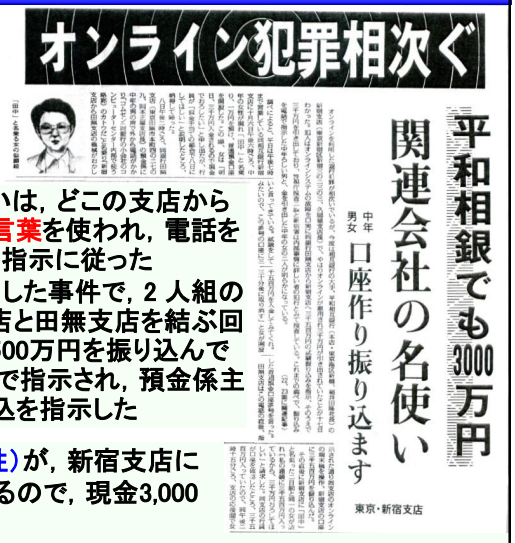
⑤ **Elicitation technique（誘導質問術）**：慎重に情報収集するために利用する技術で，特定の目的で，容易に入手できない情報を対象者（被害者）に疑いを抱かせずに収集すること。対面でも，電話でも，書面でも行われる．　高度な誘導質問術利用者は，通常の会話の中でも，専門的な会話の中でも使い，対象者は，誘導質問術の対象になっているとか，重要な情報を提供していることさえ気づかないことがある．『人々が尋問されているような感じることなく，情報収集する先約的な会話術であり，路上や電話，会議，インターネットでも行われる可能性がある』

⑥ **その他**：メーリングリスト，ブログ等：メーリングリスト等の質問メッセージを利用し，質問者の技術レベル，利用システム，ソフトウェア，セキュリティ等の情報を収集する

20

なりすまし：pretexting

なりすまし：攻撃者は，身分をなりすまし，機密情報の盗取，情報や金銭を送付させるもので，電話、メール、対面など、さまざまな方法が取られる。攻撃者は，この攻撃実行前に、攻撃対象について可能な限り多くの情報を収集し、自分が知っている人物であると信じさせる


オンライン犯罪相次ぐ

平和相銀でも3000万円

関連会社の名使い

中年男女 口座作り振り込ます

東京・新宿支店

- 銀行のオンラインシステムが一般的になり，預金の預払いは，どこの支店からも可能になった時に起こった事件で，当該銀行の**特別な言葉**を使われ，電話を受けた支店の預金係主任は自行内の職員であると信じ，指示に従った
  - 1981 年10月8日（木）平和相互銀行でオンラインを悪用した事件で，2 人組の犯人の一人が田無支店に「**コムセン**の者だが，新宿支店と田無支店を結ぶ回線の調子がおかしい．テストをするので，指示口座に3,500万円を振り込んで欲しい．正常であれば，30分後に入金訂正する」と電話で指示され，預金係主任は女子行員に端末機から新宿支店の指定口座に振込を指示した
  - 新宿支店の当該口座は数日前に，**もう一人の犯人（女性）**が，新宿支店に来店して口座を開設し，数日後に3,500万円の振込があるので，現金3,000万円を引き出したいと申し出ていた．
  - テスト送金指示の電話の直後に，口座開設をした犯人が新宿支店に通帳を持って来店し，3,500万円が振り込まれているので，3,000万円を引き出したいと言って，支店で事前に準備していた現金，3,000 万円を受け取った．
    - 「**コムセン**」は，相互銀行の**コンピュータセンターの略称**で，当時子会社が運用していたが，従来通り，コムセンと呼んでいた

3億円事件 1968.12
現金輸送車内の**現金約 3億円**が白バイ警察官になりすました男に奪われた窃盗事件

21

なりすまし：pretexting
逗子市における個人情報漏えい

逗子市における個人情報漏えいについて

以下の内容を読み、どの様に考える必要がありますか？

- 神奈川県逗子市のストーカー殺人事件をめぐり、被害者の三好梨絵さん（当時33）の住所などの個人情報が同市役所・納税課から調査会社に漏洩した疑いが濃厚となった
- 納税課には当時、課長を含む正規職員6人と定年退職後に再任用された職員2人、非常勤職員1人が在籍。非常勤職員を除く職員8人にそれぞれ、システムを閲覧できるパソコンと、接続用のパスワードが与えられていた
- 利用された端末は終日、ログイン状態で、利用されたIDのログイン記録では、午前8時8分から午後5時13分まで、昼休みも含めてつながったままだった
- 小浜容疑者は三好さんの夫を装い、家族の税滞納状況などを聞いてきたため、職員は三好さんの情報を検索し、やりとりの中で詳しい住所を漏らしたとみられ、この情報が、別の探偵業者を介して元交際相手の男に伝わり、殺害につながったとみている
- 三好さんは当時、元交際相手の男によるストーカー被害から逃れるため、逗子市役所に、第三者による三好さんの住民基本台帳の閲覧や住民票の交付の制限などを申し出ていた
- 職員がパソコン端末で、制限がかかった個人情報にアクセスすると、画面に赤文字の警告が表示される仕組みになっている
- ストーカー被害者のほか、ドメスティックバイオレンス（DV）の被害者か家族が閲覧制限を自治体に申請すれば、認められる
- 総務省の通達では、電話での問い合わせで本人や家族を名乗った場合でも、自治体職員は個人情報を開示してはならないとされている

Katsuya Uchida uchidak@gol.com

22

なりすまし：pretexting
逗子市における個人情報漏えい

逗子市との一問一答

- 個人情報を閲覧していたことが発覚した経緯は
  警察の捜査の過程で、昨年１１月５日に三好さんの納税記録を閲覧した形跡があることが分かった。昨年１２月に市の内部調査で非常勤を含む納税課職員９人を対象に事情を聴いたが、閲覧したという申し出はなかった。外部流出の確認まで至っていない。外部から電話で問い合わせがあったのかどうかも確認できていない
- 情報システムの実際の運用方法は
  職員個人に与えられたパスワードでアクセスする仕組み。席を長時間離れる場合はログアウトするのが基本。ただ、問い合わせにできるだけ早く応じたいという気持ちから、日常的につながったままの状態が続いていた。不適切な対応だったと認識している
- ストーカーなど被害を受けている人の個人情報の扱いは
  情報システムの画面上に『住基支援申出』という赤い文字表示され、注意喚起するようになっている。その個人情報は外部に出さないというのが原則。三好さんがそうだったかは答えられない
- 電話で個人情報の問い合わせに答えるのか
  電話で個人情報を伝えることはしないのが原則。ただ、氏名、生年月日、住所、納税通知書の番号など本人と確認できる情報があれば、状況に応じて対応する場合もある
- 本人確認するための基準は
  明確な基準はない。個人情報に十分注意して対応するということしかない。住民サービスという側面から電話での問い合わせを一切断るということはできない。どこまで対応できるのか、常識的な範囲で運用している。具体にどこまで確認しなければいけないかというのは、現段階では具体的にはない
- 市役所から個人情報が外部に流出した疑いが持たれている
  大変遺憾。行政への市民の信頼をなくしてしまっている状況に申し訳なく思っている。捜査に協力しながら適切な対応をしていく。このようなことが二度と起きないよう全身全霊で仕事をしていきたい

Katsuya Uchida uchidak@gol.com

23

セキュリティ心理学 ～ Human Element ～

ソーシャルエンジニアリング訓練

ソーシャルエンジニアリング訓練（なりすまし）

- 電話を利用して成りすますことにより、パスワードを電話で聞き出す方法

NHKスペシャル「世紀を超えて」2000年1月30日放送

- 簡単に パスワードを教えてしまう
- 教えるものは、パスワードだけではない
- このようなソーシャルエンジニアリング対策が重要に・・・
- 高度なソーシャルエンジニアリングでは、教えた事さえも気づかない

セキュリティ心理学 ～ Human Element ～

トロイの木馬ウイルス【ランサムウェア】

エイズウイルス（トロイの木馬）【ランサムウェア】

- 1989 年12 月に、欧州を中心に世界各国にトロイの木馬プログラムが入ったフロッピーディスクを送りつけ、金を脅し取ろうとした事件が発生した。6 月にスイスで開催されたAIDS 国際学会の出席者や欧米の金融機関のシステム責任者を中心に、世界中で約2万枚のフロッピーが送付された
- 日本にも数枚が郵送されたが被害はなかった。 英国の政府機関ではファイルを破壊されるなどの被害が発生
- このフロッピーディスクには、「AIDS Information Introductory Diskette」（後天性免疫不全症候群：AIDS 情報入門）」と印刷されたラベルが貼ってあり、このフロッピーに格納されているプログラムをパソコンのハードディスクにインストールし実行すると、AIDS に関する質問が行われ、それらの回答結果を基にしてAIDS 感染の危険性診断が行われた
- パソコンの起動が一定回数（約90 回）に達すると、このプログラムの本来機能、ハードディスク内のファイルを全て暗号化し、通常の方法では元に戻せなくなり、パナマの金融機関にあるPC Cyborg 社の口座へ378 米ドルを送金する送金指図書を印刷する仕組みになっていた
- 送金後、暗号化されたハードディスクの内容を復号化するプログラムが送られてきた
- このAIDS プログラムは、ハードディスクにプログラムを導入する時に、隠しファイルや隠しディレクトリを作成して、DOS のAUTOEXEC.BAT ファイルの内容を書き換え、パソコンの起動回数を数えるプログラムを起動していた
- このプログラムを作成した犯人、Dr. Joseph Popp は逮捕された
- 国内に送付されたフロッピーディスクの解析を行い，1990年6月に「学会での報告」を行った

内田他「有害プログラム」共立出版

セキュリティ心理学 ～ Human Element ～

ゴミ箱漁り

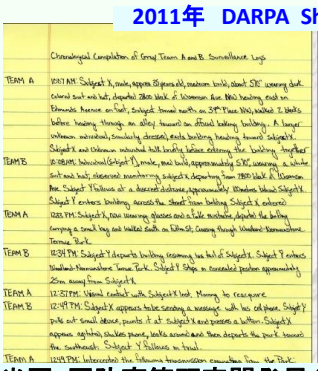
ゴミ箱漁り

- **ゴミ箱は情報の宝庫**であり、**メモ・会議録**等（社員名、所属、電話、プロジェクト担当）、**組織図、報告書下書**きなどを見つけられる可能性がある。 日本では、4月前後の異動時期には大量の資料（情報）が捨てられる
- その他、CD、DVD、名刺やコンピュータマニュアル等のドキュメントも入手できる可能性があり、コンピュータのOS、利用アプリ等も知ることができる

ゴミ箱には多くの重要情報が捨てられるが、
シュレッダー細片も最早安全でない？

1979年「**イラン革命**」で米国大使館人質事件があり、ストレートカットされたシュレッダー細片が手作業で復元（左図）。この人質事件の映画（**アルゴ**）も作成されたが、映画と異なり、左図の文書が手作業で復元された

2011年　DARPA Shredder Challenge



米国・国防高等研究開発局（DARPA）は、5万ドルの賞金を与えるクロスカット細片の復元コンテストを実施

セキュリティ心理学 ～ Human Element ～

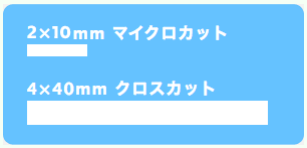
ゴミ箱漁り

ドイツのDIN規格

ドイツ規格協会 DIN 66399 による 7 段階のセキュリティレベル

Level 7	細断面積が 5 ㎟以下でかつ細断幅が 1mm 以下
Level 6	細断面積が 10 ㎟以下でかつ細断幅が 1mm 以下
Level 5	細断面積が 30 ㎟以下でかつ細断幅が 2mm 以下
Level 4	細断面積が 160 ㎟以下でかつ細断幅が 6mm 以下
Level 3	細断面積が 320 ㎟以下、または細断幅が 2mm 以下
Level 2	細断面積が 800 ㎟以下、または細断幅が 6mm 以下
Level 1	細断面積が 2000 ㎟以下、または細断幅が 12mm 以下

推奨する細断面積と細断サイズは、「細断面積が160ミリ平方メートル以下且つ幅6mm以下のクロスカット」となっています。この内容に照らし合わせると、市場に多く流通している「4mm×40mm」で細断できる業務用シュレッダーは、基準を満たしている



面積で見るとマイクロカットが20平方ミリメートル、クロスカットが160平方ミリメートルと、実に8倍もの面積の差があります。
クロスカットでも上記の例よりも細かく細断出来る機種はありますが、幅4mm、長さ30～40mm程度のものが一般的です

廃棄資料を溶解対応すれば安全か？

溶解物保管場所の管理が不十分だと保管物を盗取される可能性もある・・・

サイト侵入（Incursion）

サイト侵入

- 清掃員、電気・電話工事人、警備員等になりすまし、オフィスや工場等に侵入する
- 休日に清掃や工事等を行っているオフィスに社員になりすまして入る

- 休日に清掃や工事を行っている雑居ビル入居のオフィスがあるが、平日にはドアがロックされているが、休日には、ドアを開け放したままになっている事が多い
- オフィスや重要区域の清掃では、平日の時間外のこともあり、社員の立会もないこともある
- 国内では、４月前後に大幅な異動があり、オフィスのレイアウト変更や引っ越しなどがあり、非正規社員が、机・椅子やPC、荷物を運んでおり、社員が立会していないことがある

参考：取引関係者の社内立入

- 社内に取引関係者が簡単に立ち入ることができる企業等がある
- 被害企業のセールス部門では、各人が外出時に黒板に行き先を「外出：訪問先名」と記入していた
- 出入りの印刷業者は打合等では、セールスやシステム部門の該当者の机そばに来て、打合せをしていた
- 被害企業では、見込み顧客に対し、最終段階に近づくと、必ず競合他社が入ってきた。
- 色々調べたら、この印刷業者が競合他社に情報を流していたことが判明し、業者を出入り禁止にすると同時に、黒板に担当者のスケジュールを記入することをやめた。
- 現在であれば、職場内に入ってきたら、外出している担当者がどこに行ったかを聞いて、操作PC画面を操作者と一緒に見ることができれば、同じことができるであろう

28

サイト侵入（Incursion）

サイト侵入御用達

簡単に作れる？！

- 外出時，身分証明書の内容が他人に読まれる危険性は？
  - 屋外での昼食，地下鉄車内等で，身分証明書が丸見えの人がいますが，勤務先や所属，名前などが分かる恐れは？
- 警察手帳等の偽物も販売している（*警察手帳のレプリカを販売！*）
- 弁護士の身分証明書もインターネット上で見つけることができる
  ⇒ 弁護士カードも偽造できそう・・・・
- 便利なカード作成機やIDカード作成キットもある・・・

上記の制服を調達し・・・

Frame Bridging

パイロットの服装をし、パイロットになりすました

（フランク・W・アバグネ

なりすまし実践例
（ノンフィクション）

29

セキュリティ心理学 ～ Human Element ～

のぞき見（日本語訳：Shoulder hacking）

のぞき見（shoulder surfing / visual hacking）

- 肩越しにパソコン等の画面をみて、表示されている情報、ユーザID／パスワードや重要情報を盗み見るもので、英語では、”shoulder surfing”とか、“visual hacking”と言う
- 数年前、「ショルダーハッキング」の簡単な実験を、情報セキュリティ心理学研究会の参加者（全員社会人）を対象に行ったが、画面表示の情報を覚えることは簡単でなかった
- ショルダーハッキングは、以下の方法が考えられる

1. **書き写す**
   最近は、スマーホ等のセンター持込を許可しないケースがあるが、大量の情報でなければ、ディスプレイに表示された情報を書き写すことができる。
   2015年3月 コールセンター業務委託先契約社員が、23名分の個人情報を書き写し、持ち出した
2. **記憶する**
   データの記憶方法習得者であれば、入力データが長くても記憶できる。 文字を物語り（ストーリー）として記憶する方法が使われることが多い。パスワードをみて、物語りに組み立てられれば、その物語から、パスワードを戻せる。訓練は必要
3. **写真、動画**
   人間の記憶に頼らず、電子機器を使う方法もある。最近のデジタルカメラは高倍率・高画質であり，これらを使えば長時間の訓練も不要。右図は実際に海外で撮影した写真だが、赤丸内に日本の携帯電話会社の名前があり、利用者は日本人の可能性が高い。 高倍率、高画質のスマートフォンやデジタルカメラでは動画も撮影できる。

30

セキュリティ心理学 ～ Human Element ～

のぞき見（日本語訳：Shoulder hacking）

のぞき見（Shoulder Hacking）

- 「Shoulder Hacking」は、肩越しにID/パスワード等の情報の のぞき見であるが、トラブル時等にそばにいない限り 相当の技術を要する。 こっそり、ビデオを設置し、内容を解析したり、遠方から双眼鏡等を使ってのぞき見することでないと難しいと言える。 ■
- 外出先等 公共の場でノートPC等を開いたまま離席したため、表示内容やファイルをコピーされる可能性はある ■
- サイト侵入とも関連しているが、机上に書類が山と積まれていると、重要書類を持ち去られても気づかない可能性がある。 PC画面を表示したままであったり、机上の整理整頓がなっていないと、のぞき見的な行為を行われる可能性が高い

  - 内部の会議・打合せ等でも、離席する場合には、必ずPCをログオフするセキュリティポリシーを持つ企業もあり、罰則まで備えている
  - ISMSは、「クリアスクリーン」、「クリアデスク」の実行を掲げているが、のぞき見防止にも役立つ

「クリアスクリーン」・「クリアデスク」の考え方

Clear Screen → Clear Desk → Clear Room → Clear Building → Clear Site

CPTED or/and Broken Windows Theory

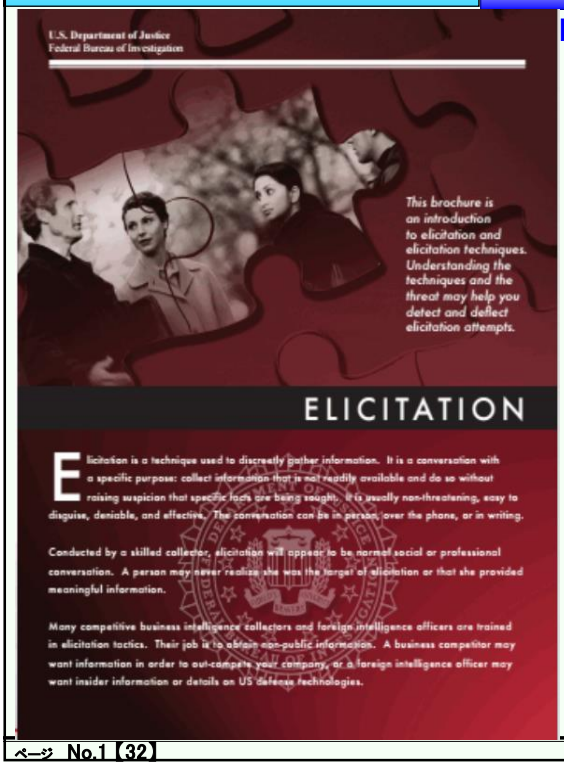
⇐ 工場の整理・整頓と同じ

「クリアスクリーン」、「クリアデスク」をこのように考えればその意義が理解できる？
重要情報保存媒体が部屋に無造作に置かれていれば、犯罪を誘発する可能性がある。

31

セキュリティ心理学
～ Human Element ～

Elicitation（誘導質問術）



Elicitation Technique（誘導質問術）とは？

- Elicitation is a technique used to discreetly gather information. It is a conversation with a specific purpose: collect information that is not readily available and do so without raising suspicion that specific facts are being sought. It is usually non-threatening, easy to disguise, deniable, and effective. The conversation can be in person, over the phone, or in writing. Conducted by a skilled collector, elicitation will appear to be normal social or professional conversation. A person may never realize she was the target of elicitation or that she provided meaningful information.
- エリシテーションとは、慎重に情報を収集するために用いられるテクニックである。特別目的の会話で、容易に入手できない情報を収集し、特別な事柄を求めていると疑われないようにすること。脅迫的でなく、偽装しやすく、否認可能で、効果的である。会話は、対面，電話、書面でも可能で，熟練者が行えば、通常の社交上／仕事上の会話に見える。被害者は、自分が対象であるとか、意味のある情報を提供したことに気づかない

https://www.fbi.gov/file-repository/elicitation-brochure.pdf/view

Katsuya Uchida uchidak@gol.com

32

セキュリティ心理学
～ Human Element ～

Elicitation（誘導質問術）

Elicitation（誘導質問術）とは？

- 誘導質問術は，慎重に情報収集するために利用される技術で，特定の目的，入手困難な情報を対象者（被害者）に疑いを抱かせずに収集すること．会話は，対面でも，電話でも，書面でも行われる．
- 高度な誘導質問術利用者にかかると，通常の会話の中でも，専門的な会話の中でも使われ，対象者は，誘導質問術の対象になっているとか，重要な情報を提供していることさえも気づかないことがある．『人々が尋問されているような感じることなく，情報収集する先約的な会話術であり，路上や電話，会議，インターネットでも行われる可能性がある』

Elicitation（誘導質問術）はなぜ機能するのか？

- 目的とする情報を収集するには，攻撃対象となる人間や文化的特性を十分理解した上で，訓練された誘導質問術者は情報収集を行う
  誘導質問術者（Elicitor）は，対象者が持ついくつかの特性を理解し，それを利用する
  具体的には，攻撃対象者（被害者）が持つ以下のような特性を利用すると考えられている．
  (1) 知らない人や初めて知った人に対してさえも，礼儀正しく，また，有用でありたいと願っている
  (2) 自分の専門的分野に関しては，よく知っていると思われたいと思っている
  (3) 重要な問題に対して，自分は評価されており，貢献していると思っている
  (4) 噂話をしたり，他人の誤りを正したいと思っている
  (5) その情報について詳しくない場合，その情報の価値を過小評価する傾向がある
  (6) 胡散臭いと思うことを嫌がり，他人は正直だと信じる傾向がある
  (7) 率直な質問をされると，事実を正直に回答する傾向がある
  (8) 誰かを自分たちの考えにしたいと思う傾向がある

Katsuya Uchida uchidak@gol.com

33

セキュリティ心理学
～ Human Element ～

Elicitation（誘導質問術）

Elicitation（誘導質問術）とは？

- 誘導質問術は，慎重に情報収集するために利用される技術で，特定の目的，入手困難な情報を対象者（被害者）に疑いを抱かせずに収集すること．会話は，対面でも，電話でも，書面でも行われる．
- 高度な誘導質問術利用者にかかると，通常の会話の中でも，専門的な会話の中でも使われ，対象者は，誘導質問術の対象になっているとか，重要な情報を提供していることさえも気づかないことがある．『人々が尋問されているような感じることなく，情報収集する先約的な会話術であり，路上や電話，会議，インターネットでも行われる可能性がある』

Elicitation（誘導質問術）はなぜ機能するのか？

- 目的とする情報を収集するには，攻撃対象となる人間や文化的特性を十分理解した上で，訓練された誘導質問術者は情報収集を行う
  誘導質問術者（Elicitor）は，対象者が持ついくつかの特性を理解し，それを利用する
  具体的には，攻撃対象者（被害者）が持つ以下のような特性を利用すると考えられている．
  (1) 知らない人や初めて知った人に対してさえも，礼儀正しく，また，有用でありたいと願っている
  (2) 自分の専門的分野に関しては，よく知っていると思われたいと思っている
  (3) 重要な問題に対して，自分は評価されており，貢献していると思っている
  (4) 噂話をしたり，他人の誤りを正したいと思っている
  (5) その情報について詳しくない場合，その情報の価値を過小評価する傾向がある
  (6) 胡散臭いと思うことを嫌がり，他人は正直だと信じる傾向がある
  (7) 率直な質問をされると，事実を正直に回答する傾向がある
  (8) 誰かを自分たちの考えにしたいと思う傾向がある

34

セキュリティ心理学
～ Human Element ～

質問方法（Open/Close）

オープンな質問とクローズドな質問（Open question & Closed question）

- オープンな質問：相手に答えを自由に考えさせる質問
- クローズドな質問：「はい／いいえ」等、制限された選択肢内の言葉で回答できる質問

事実だけを確認でき,相手の話を遮らない。ただし理由や相手の考えなどは明らかにならないため,相手の言ったことを確認するのに適している

相手が自由に回答できる問いかけ。あまり多用すると話が発散してしまうことがある。相手の話を詳しくより深く聴くのに適している

コミュニケーションスキル講座：聴く力と話す力を磨く！
http://itpro.nikkeibp.co.jp/article/COLUMN/20070529/272792/

正しい回答が得られない質問

Q：あなたのPCには最新のWindowsですか？　A：はい、最新のものを使ってます！

正しい回答を得る質問

Q：あなたのPCは、Windowsを使っていますか？　A：はい
Q：Windowsのバージョンは分かりますか？　A：はい、Windows VISTAです
Q：VISTAは最新バージョンではありませんが　A：えっ！　知りませんでした・・・

35

セキュリティ心理学 ～ Human Element ～

6つの人間の脆弱性 (Six "weapons of influence")

誘導質問術が効果的な背景

1. 返報性[Reciprocation]: 親切や贈り物、招待等で、その人にお返しをせずにいられない気持ちになる
2. コミットメントと一貫性[Commitment and Consistency]: 自分の意志でとった行動がその後の行動にある拘束をもたらす。 以下のような手法がある
   - A) ローボールテクニック: 最初にある「決定」をさせ、その決定が実現不可能である事を示し、最初の決定より高度な要求を認めさせる。 例) 特売商品を購入客に、購入手続き最中に在庫がなく当該商品の購入は無理だが、色違いの少し高価なものならあると言って高い商品を購入させてしまう
   - B) ドア・イン・ザ・フェィス テクニック: 最初に実現不可能な要求を行い、できない状況で、負担の軽い要求で、実現させる。 例) 高額借金の依頼を行い、断られたら少額の借金を申し出て，承諾させる
   - C) フット・イン・ザ・ドア テクニック: 最初に誰も断らない ごく軽い要求を行ってもらい、次により重い要求の承諾を得る。 例) 最初に簡単な署名を依頼し、その後時間がかかる調査に協力してもらう
3. 社会的証明[Social Proof]: 他人の考えにより、自分が正しいかどうかを判断する特性
4. 好意[Liking]: 好意を持っている人から頼まれると、承諾してしまう。 パーティを開いて、商品を購入させる場合、好意を持っている隣人がホスト役で販売すると、他のがホスト役より簡単に購入する
5. 権威[Authority]: 企業・組織の上司等権威を持つ者の命令に従う
6. 希少性[Scarcity]: 入手し難い物であるほど、貴重なものに思え、手に入れたくなってしまう特性

ロバート・B・チャルディーニ 著「影響力の武器」
(Robert B. Cialdini "INFLUENCE – Science and Practice") 誠信書房 より

ソーシャルエンジニアが使う説得技術は、一般の人々が日常使っているものと何等変わらない。人々は説得により 役割や信頼を築こうとし、互いに恩恵をもたらそうとする。 しかし、ソーシャルエンジニアは、これらの技術で、人を操ったり、人を欺いたり、極めて非倫理的な行為におよび、破滅的な結果を招くこともある (Dr. Brad Sagarin)

セキュリティ心理学 ～ Human Element ～

ソーシャルエンジニアリング 対策

(0) 基本的な対策
- セキュリティポリシーの周知(各項の背後の理由・狙い等)
- ソーシャルエンジニアの考え方を理解する
- 攻撃の可能性は全てにあることを理解させる
- 過去事例・ケース等で教育・訓練の実効を高める
- 疑わしい場合の連絡と連絡先の明確化
- セキュリティ製品の導入(Anti Virus. F/W, 脆弱性対応等)

(1) 電話でのなりすまし
- 相手の身元確認を組織で習性とする(コールバック等)
- 電話機に「防止」ステッカーの貼付
- 自分だけで判断せず、上司・同僚と情報共有する
- 部門毎に重要な情報資産を理解する

(2) ゴミ箱あさり
- 重要な資料は、溶解する
- 廃棄資料保管場所は施錠を行う

(3) サイト侵入
- 入館は「友連れ」防止を行う
- 身分証明を確実に行う
- 日常的なオフィス清掃等は勤務時間内の行う
- 休日に行う業者の作業には立会する

(4) のぞき見
- パスワード入力では、のぞき見に注意する
- 空港等 公共空間での利用は十分な注意を

(5) メール添付／埋込URL
- ウェブの管理は、外部からできない仕組みにする(イントラネット利用)
- 標的型メールの真偽の判定方法の訓練(添付ファイルのクリック前の確認も)
- 不特定多数からメールを受ける場合、ウェブ入力形式の採用を検討する
- 機密が高い情報を扱う場合には、入退館室とシステムへのログインを同期させる

(6) メール埋込
- 重要情報をメールで確認することはない

(7) メーリングリスト
- 所属が分かるようなメールアドレスをMLで利用しない
- 所属組織の課題が分かるような事柄をMLに投稿しない
- MLで質問した内容を1対1メールにしない

(8) パスワード推測
- 名前、電話番号、趣味等の関係パスワードを使わない
- 複数のシステムで同一パスワードの禁止
- リスクの高いウェブを構築しない

セキュリティ心理学 ～ Human Element ～

ソーシャルエンジニアリングへの技術 対策

実用的だろうか？

- 電話によるソーシャルエンジニアリング対応のための調査・研究：Purdue 大学 CERIAS 研究所が2005年に机上研究プロジェクトとして行ったもので，当時の技術を使えば，ソーシャルエンジニアリングを防御できるとしている。
  Hoeschele Michael D.: Rogers, Marcus K. Social Engineering Defense Architecture, http://www.cerias.purdue.edu/news_and_events/events/symposium/2005/materials/pdfs/D04-6B4.pdf
- 振り込め詐欺を電話の声で見破る技術を各社が開発している
  国立大学法人名古屋大学；富士通(株)「行動モデルに基づく過信の抑止」の研究開始について
  http://www.nagoya-u.ac.jp/research/pdf/activities/20091113_is.pdf
  ITMedia，振り込め詐欺を電話の声から見破る新技術，富士通と名大が開発，
  https://www.itmedia.co.jp/news/articles/1203/19/news082.html
  通話内容で「振り込め詐欺」を見破る、NTTが月440円で提供するAIサービスの中身
  https://xtech.nikkei.com/atcl/nxt/column/18/00001/04982/

我が家は，留守番電話（Voice maile）を20年位使っている
- 留守番電話の目的は，留守時の着信（発信者，発信日時，発信目的等）を記録すること
- 我が家は，常時 留守電状態になっている（24Hx365D）
- 有人・知人は，メッセージ内容時に，名前を言うので，留守でなければ，電話を取り，会話する
- アンケート調査，詐欺電話等は，全て諦めて，電話を切るため，電話詐欺にあうこともない
- 在宅か留守かの判断を外部からできないため，「空き巣（Burglary）」等の被害もない

セキュリティ心理学 ～ Human Element ～

ソーシャルエンジニアリング事例

実際にあったソーシャルエンジニアリング

- 最後に、ソーシャルエンジニアリングの実例をお聞かせします。 訓練やデモではありません、実践の迫力を感じることができれば・・・
- 1994年11月に開催された第21回 CSI（Computer Security Institute） Annual Conference で行われた「Meet the Enemy」（「ハッカーと語ろう」注）セッションで偶然 発生したものです
- ハッカーと情報セキュリティ専門家の電話会議に 割り込んできた電話会社のオペレータがハッカーのソーシャルエンジニアリング攻撃を受けた。何気ない会話から，オペレータのID／パスワードをハッカーが聞き出していますが，オペレータは被害を受けた自覚が全くありません。 高度なソーシャルエンジニアリング攻撃では，被害者は自分が被害を受けたことさえ分からない例です。

注）筆者の迷訳です。 Night Session として行われました
セッションモデレータの Ray Kaplan は、ケビン・ミトニックを ラスベガスで開催されたDECUS（DECのユーザ大会）に連れて行ったことで有名です。また、Kaplan は、MITのケルベロスプロジェクト（Kerberos Project）にも係わっていました

Ray Kaplan
DECUSでの対応は、ケビン・ミトニック関連の3部作の1つ（「FBIが恐れた伝説のハッカー（The Fugitive Game）」 ジョナサン・リットマン著 東江一紀訳 草思社）に詳細があります

ソーシャルエンジニアリング事例

お笑い芸人の情報収集

- 数年前テレビでお笑い芸人のMCが、二人の若い女優を相手にしていました。
- 若い女優は年齢を聞かれ、24歳と回答しましたが、年上の女優は「女性に歳を聞かないで」と。
- そこで、MCは、若い女優に「二人の関係は？」と聞き、「姉の同級生」との回答に、すかさず、「お前と姉はいくつ違う？」。
- 「3歳」との回答。このように、直接聞かなくても、情報収集ができています

医者（手術）の質問

- ① この手術であれば，生存率は 80% です
  ② この手術の失敗率は，20% です

参考 ビデオ！

女性のRougeにご注意を！

セキュリティ心理学 ～ Human Element ～

問題の発見と問題の解決

問題発見について

- **組織の機能停止や崩壊は**一瞬で起きるものでなく、**徐々に進行する**。 問題発見スキルを磨くことで、組織に大惨事をもたらしかねない脅威をあらかじめ阻止することができる
- **問題発見者になるために、リーダーが身につけるべき7つのスキルと能力**
  - ① **情報のフィルターを避ける**: リーダーの周りの部下たちは情報にフィルターをかけることがあり、それを認識する必要がある。 部下は、リーダーの貴重な時間を無駄にしたくないため、多くの場合、善意によってフィルターをかける
  - ② **人類学者のように観察する**: リーダーは、自然な環境の中で集団を観察することを学ぶ必要がある。人に質問するだけでなく、その行動を見守らなければならない。**人の発言と行動は一致しない**もの
  - ③ **パターンを探し、見分ける**: **問題のパターンを探し、見分ける**ことが、優れた問題発見者である。**過去の経験や組織の経験**をチェックする方法は問題をより早く見分けられるようになる
  - ④ **バラバラな点を線でつなぐ**: **バラバラな情報の断片から「点をつなぐ」能力**を磨く。 危機の兆候はあちこちに散らばっていることが多い。細切りの情報を多く集めることで、組織の抱える問題が見えてくる
  - ⑤ **価値のある失敗を奨励する**: 部下に**リスクを取ることを促し、失敗から学ぶ方法**を教える。失敗の中に有益なものがあり、それが学習と改善の機会になる。 しかし、リーダーは、有益な失敗とそうでない失敗を区別できなくてはならない
  - ⑥ **話し方と聴き方を訓練する**: 自分自身のコミュニケーション能力だけでなく、**組織全体のコミュニケーション能力も磨く**必要がある。部下に率直かつ効果的な話し方を教えること
  - ⑦ **行動を振り返り、反省のプロになる**: スポーツチームの偉大な監督等は、過去の試合や演技の録画をみて、自分のチームの問題だけでなく、ライバルが抱える問題からも教訓をうる。リーダーは、**反省し見直すことに熟達**し、新たな行動を効果的に練習する方法を考えなければならない

マイケル・A・ロベルト「なぜ危機に気づけなかったのか」

42

セキュリティ心理学 ～ Human Element ～

問題の発見と問題の解決

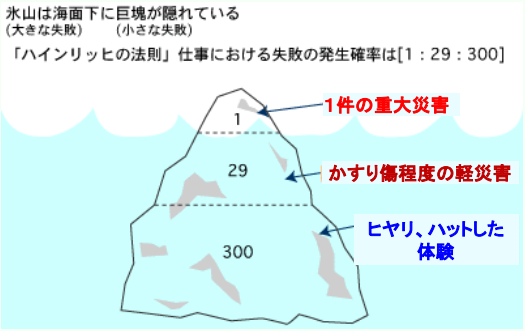
問題発見について

- **大規模な事故**は、単一の根本的な原因というより、**一連の些細な間違いや失敗から**引き起こされる
- **小さな問題の段階で適切に対処**しておけば、それは早期の警戒警報として役割を果たす。 大規模な危機は長期の潜伏期間を経て起きることが多いということは、**小さな問題が起きても、最悪の結果を回避するために手を打つ十分な時間的余裕がある**ということ
- しかし、問題が表面化しない事が多々ある。 小さな問題は局所的レベルで発生し、大きな組織の中では目につきにくい

マイケル・A・ロベルト「なぜ危機に気づけなかったのか」

ハインリッヒの法則

- 労働災害の発生確率の分析から、**1件の重大災害**の裏に、**29件のかすり傷程度の軽災害**があり、更に ケガはないが**ヒヤリ、ハットした300件の体験**がある
  更に、障害を伴うにせよ伴わないにせよ、すべての災害の下には、おそらく数千に達すると思われるだけの不安全行動と不安全状態が存在する



割れ窓理論

- **軽微な犯罪も徹底的に取り締まれば、凶悪犯罪を含め犯罪を減らせる**という**環境犯罪学**の理論
  アメリカの犯罪学者ジョージ・ケリングが提唱
  建物の窓が壊れているのを放置すると、誰も注意を払っていないと考えられ、他の窓も全て壊されるとの考え方

43

セキュリティ心理学 ～ Human Element ～

問題の発見と問題の解決

事故分析

1. やめる／なくす	エラーが発生した作業そのものをやめることはできないか？ 他の作業と統合できないか？
2. できないようにする	間違った操作をしても、機械側で操作を止めたり、決められた手順以外ではできない構造にする
3. わかりやすくする	記憶するのではなく、操作機器／場所に名称、基準となる値を表記、用紙に記録する
4. やりやすくする	作業しやすい環境にする。 机上に書類がうずたかく積まれている所で操作が邪魔されたりする
5. 知覚能力を持たせる	ある一定基準以上の感覚知覚能力を維持できるように自己管理をさせる
6. 認知・予測させる	どの様な所でエラーが発生する可能性があるかを予測させる（例：危険予知訓練 KYT）
7. 安全側に判断させる	判断に迷った時、安全側の判断を容易にできるようにする（例：分からない事は分からないと言う）
8. できる能力を持たせる	該当作業が行える基準以上の身体的能力や必要な技能を持たせる
9. 自分で気づかせる	作業終了時に、自分の仕事を確認し、自分のエラー発生の検出をさせるための工夫を考える
10. エラーを検出する	各種対策を行ってもエラーが発生した時、できるだけ早くエラーの発生を気づかせる方法を考える
11. エラーに備える	エラー発生防止／検出対策等 全てをすり抜けた時、その影響を大きくしないための方法を考える

河野龍太郎 「医療におけるヒューマンエラー」

Katsuya Uchida uchidak@gol.com

44

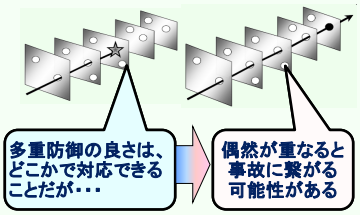
セキュリティ心理学 ～ Human Element ～

まとめ

ソーシャルエンジニアリング対策

No silver bullet

- ソーシャルエンジニアリング対応は、技術、運用、人間（教育・訓練）等を総合的に行う必要がある
- 海外では、5日間のソーシャルエンジニアリング教育・訓練が行われているが、国内では「標的型攻撃メール」の訓練は数年前から行われているが、いわゆる、ソーシャルエンジニアリング対応の教育・訓練は知らない
- 最早、セキュリティ対策は技術だけで対応できないことは明らかであり、ソーシャルエンジニアリング教育・訓練を行う必要があり、1日～2日程度の教育・訓練コースを開発し、それらの実践からも知見を得たいと考えている



カクテル・パーティ効果
- 関心のない情報は見えない、聞こえない
- 参加者が関心を持つ工夫が教育・訓練では非常に重要

- 現在の情報セキュリティ対策技術は、25～30年前の技術から余り進歩がない
- サイバー犯罪でも 100%完璧な防御は不可能で、どの様に防御し、被害を最小限にするかを考えると、「多重防御」へ行き着く。 多重防御では「人間（Human Firewall）」が重要だが、多くの人間が関係するバーチャル世界では、教育・訓練は非常に重要である

ソーシャルエンジニアリングの基本は，『心理学』と言える。 現在のセキュリティは 利用者中心を含めて考える必要がある。
利用者の管理・運用が重要になるが，それを考える中心は，『心理学』的考察であろう

Katsuya Uchida uchidak@gol.com

45

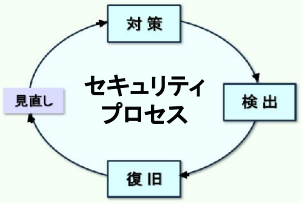
セキュリティ心理学 ～ Human Element ～

更に考えるために・・・ セキュリティ心理学入門

セキュリティ心理学の重要要素【Three Critical Issues for Security Psychology】

① 転ばぬ先の杖 Look before you leap
② 敵を知り，己を知れば Know your enemy, know yourself （Sun Tzu）
③ 性弱説 the mind being influenced by the environment （K. Uchida）

①～③を書籍【セキュリティ心理学入門】の項目（章）に当てはめてみた



はじめに ②
- 情報資産
- セキュリティ心理学について
- セキュリティ心理学
- 情報セキュリティ対策の位置付け

ヒューマンエラー ①
- 作業環境とヒューマンエラー
- ヒューマンエラーとサイバーセキュリティ
- ヒューマンエラーの誤解
- ヒューマンエラーをどの様に防ぐか

環境犯罪学 ②
- 環境犯罪学とは
- 犯罪防止を考える
- 現金より情報

ソーシャルエンジニアリング ②
- 誘導質問術
- なりすまし
- ゴミ箱漁り
- サイト侵入
- のぞき見（ショルダーハッキング）

人間の6つの脆弱性 ③
- 返報性
- コミットメントと一貫性
- 社会的証明
- 好意
- 権威
- 希少性

インテリジェンス（情報収集） ②
- インテリジェンスとは？
- 地政学的な考察
- 地政学的なサイバー攻撃

物理的セキュリティ ②
- 建物への侵入
- 重要資料を廃棄ゴミに
- 誰かが見ていた

だましの欺術 ②
- 内部統制とは？
- だましを考える：だましの9パターン

行動経済学とセキュリティ心理学 ②
- フレーミング効果（framing effect）
- アンカーリング効果（Anchoring Effect）
- 極端回避性（松竹梅の法則）
- 同調効果（社会的証明【Social Proof】）
- ナッジ（Nudge）
- ゲーミフィケーション（Gamification）

セキュリティ教育・訓練 ①
- 教育・訓練の目的
- 一歩進んだ教育・訓練（人間での多重防御）
- 教育・訓練の難しさ
- 教育・訓練効果の評価
- 教育・訓練の誤解
- 教育・訓練事例

セキュリティ文化の確立 ①
- セキュリティ文化の確立
- セキュリティ文化のロードマップ
- セキュリティ文化推進のための教育・訓練

セキュリティ心理学 ～ Human Element ～

参 考 資 料

- 山本幸司 人はなぜ騙すのか — 狡智の文化史 岩波書店
- ロバート・チャルディーニ 影響力の武器 誠信書房
- ロバート・チャルディーニ他 影響力の武器 実践編—「イエス!」を引き出す50の秘訣 誠信書房
- ナイトメア シークレット・オブ・スーパーハッカー 日本能率協会マネジメントセンター
- ケビン・ミトニック他 欺術 ソフトバンククリエイティブ
- クリス・ハドナジー ソーシャルエンジニアリング 日経BP
- 内田勝也他 有害プログラム—その分類・メカニズム・対策 共立出版
- 内田勝也 セキュリティ心理学入門 学術研究出版
- マイケル・A・ロベルト なぜ危機に気づけなかったのか 英治出版
- マックス H.ベイザーマン 他 予測できた危機をなぜ防げなかったのか 東洋経済新報社
- リン・シャープ・ペイン バリューシフト 毎日新聞社
- シーナ・アイエンガー 選択の科学 文芸春秋
- 岡本浩一 リスク心理学 サイエンス社
- ダン・ガードナー リスクにあなたはだまされる 早川書房
- 中谷内一也 リスクのモノサシ NHKブックス No.1063
- 河野龍太郎 医療におけるヒューマンエラー 医学書院
- 日本技術士会 技術者倫理研究会 IAEA安全文化の解明
- アトゥール ガワンデ アナタはなぜチェックリストを使わないのか？ 晋遊社
- 芳賀繁 ヒューマンエラーのメカニズム （大山正・丸山康則 編「ヒューマンエラーの科学」）
- 鎌田晶子 『組織風土』とヒューマンエラー （大山正・丸山康則 編「ヒューマンエラーの科学」）
- ベライゾンビジネス データ漏洩/侵害調査報告書 2023 Data BREACH Investigations Report
  https://www.verizon.com/business/ja-jp/resources/reports/dbir/

セキュリティ心理学
～ Human Element ～

ありがとうございました

内 田　勝 也
e-mail:　uchida@iisec.ac.jp
Twitter:　@woodytokyo
Facebook: woodytokyo
http://www.uchidak.com/

Idea IT College Aso
専門学校　イデアITカレッジ阿蘇

セキュリティ担当者として知ってほしいこと

セキュリティ診断 実践

（2023/12/18）

担当講師：伴 芳龍（ ban@iica.jp ）

1

今日の流れ

1.前回講義の振り返り・質疑応答

2.本日の講義

3.まとめ

2

前回講義の振り返り

- 前回（10/30）の講義では、簡単なCapture The Flag（CTF）を皆さんに体験してもらいました。
- 講義後のアンケートでは、難しかったという意見が多かったですが問題が解けたときにやりがいを感じた、面白かったという意見もいただきました。
- 出題側としては、問題の難しさ・解き方の誘導をもう少し工夫すればより楽しんで学習してもらえるのでは、と反省しています

3

3

前回講義の振り返り

- また、オンライン参加の方（3名）がいることを想定しておらず不十分な形になってしまったのも反省点です
- 1月の講義（1/22予定）に2回目のCTFを実施予定です
  - なるべく、講義室での参加をお願いします
- アンケートの質疑応答…今回はなし

4

4

今日の流れ

今日の内容とゴール

今日の内容

- CTFの補足
  - VirusTotalの使い方、注意点
  - 解析サイトの使い方、注意点
  - メールの構造、ヘッダの見方
- メールの問題について考えてみよう
  - PPAP
  - メールのなりすまし対策

今日のゴール

- ✓ VirusTotalやWebサイトの解析を行うサイトなど、外部ツールの機能や使い方について学ぶ。
- ✓ メールのヘッダの内容や、メールに関係する問題について理解し、考えてもらう。

今日の内容

- CTFの補足
  - VirusTotalの使い方、注意点
  - 解析サイトの使い方、注意点
  - メールの構造、ヘッダの見方
- メールの問題について考えてみよう
  - PPAP
  - メールのなりすまし対策

CTFの補足

- 前回のCTFでは、授業で説明していない内容の知識を聞く問題がありました
  - メールヘッダの解読、ハッシュ値の検索、など
- 知らないことは調べながら解いてもらうという想定だったのですが、
  ヒントを次々設定したり、アドバイスしたりする形になってしまいました
- いずれもセキュリティの担当者として知っておいて損はない知識なので、
  今回の授業でそれぞれ改めて解説したいと思います

VirusTotalとは

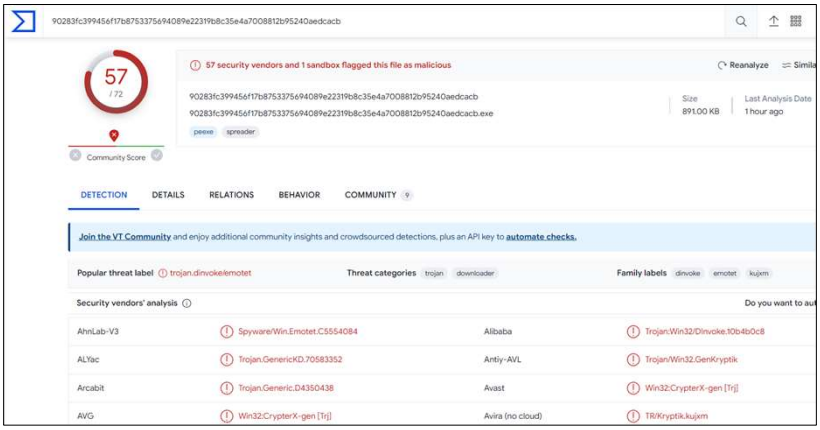
- CTFでは、マルウェアのハッシュ値から名前を調べる問題で使いました
- https://www.virustotal.com/

VirusTotalとは

- VirusTotalにファイルをアップロードすることで、
  そのファイルが「マルウェアを含むかどうか」検査ができます
- また、WebサイトのURLを指定することで
  そのWebサイトが「マルウェアを含むかどうか」検査できます
- ハッシュ値でファイルを検索し、他の人がアップロードしていた場合は
  その検査結果を確認することができます
- ただし、あくまでスキャンを行うだけです
  - マルウェアの除去はできません

VirusTotalとは

- マルウェアの検査については、約70のウイルス対策ソフトで検査をします
  - Microsoft、マカフィー、トレンドマイクロ、ESET、など…



VirusTotalの使い方

- ファイルのアップロードやURLを入力する部分がありますが、
  直感的に使えると思います。

- 講義中は、実際の画面を使って解説します。

VirusTotalの注意点

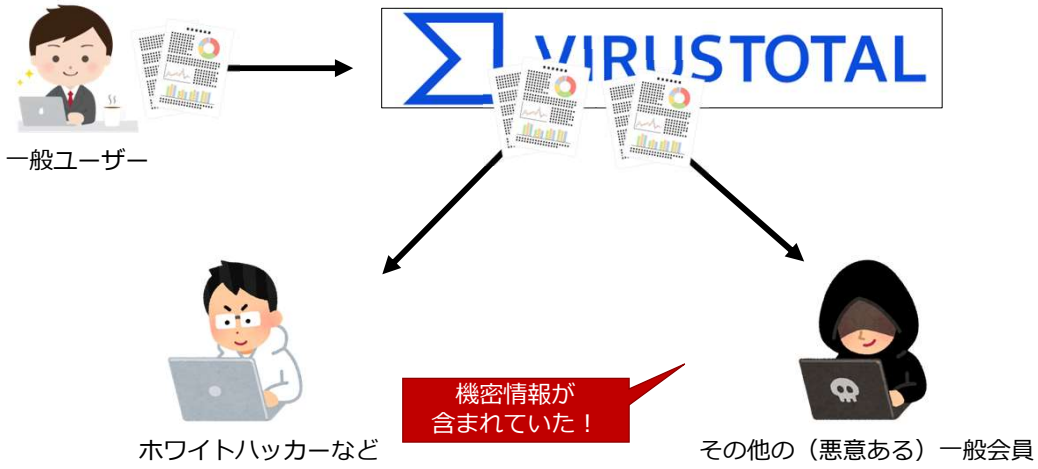
- VirusTotalの利用は無料ですが、研究目的などで有料会員になることができます

- 有料会員になると機能が追加されたり、より高度な検索ができます
  - それに加え、他のユーザーがアップロードしたファイルをダウンロード
    することができます

- この「**ダウンロードができる**」という点に注意が必要です
  - 本来は、マルウェアの検体（サンプル）をダウンロードするための
    機能だと思われます

VirusTotalの注意点

- 図で説明します



15

15

VirusTotalの注意点

- この「**ダウンロードができる**」という点に注意が必要です
  - 本来は、マルウェアの検体（サンプル）をダウンロードするための機能だと思われます

- つまり、個人情報・機密情報が含まれるファイルをアップロードしてしまうと情報漏えいを起こしてしまいます
  - 2020年には、大学職員がアップロードしたファイルに個人情報1,725件が含まれており、外部に漏えいしたとの発表がありました
  - 「ダウンロードしたファイルを自動でVirusTotalにアップロードする機能」を利用しており、誤って自動でアップしてしまったとのこと

16

16

VirusTotalの注意点

- それ以外にも、**「社外秘」「機密」などとファイル名についた、**
  外部に公開してはいけないと思われるファイルがアップロードされていたとの
  調査報告がありました

- VirusTotalにファイルをアップロードして検査する場合、そのファイルに
  「個人情報や機密情報などが含まれていないか」
  「インターネット上に公開しても問題ないか」ということを必ず確認した上で
  アップロードするようにしましょう。

17

17

解析サイトについて

- 不審なメールやフィッシングメールなどに含まれる怪しいURLですが、
  基本的にはクリックしないのが最善と説明しました

- ただ、場合によってはそのURLをクリックした場合の影響を
  確認する必要があります
  - 例えば、メールのリンクを誤ってクリックしてしまったとか

- しかし、普段使っているPC・ブラウザでそのURLを開くのは
  とても危険です

18

18

解析サイトについて

- 大学などの研究機関や企業であれば、それ専用のPC・ネット回線を用意して開くこともできます
- ただ、専用の環境を用意するのはコストがかかります
  - 一般の企業で、わざわざそんな手間はかけられないです
- 仮想環境（VirtualBoxなど）を用意する方法もあります
  - ネット回線はスマートフォンのテザリングを利用するなど…
  - ただし、通信料がかかります
- もっとも手軽なのは、解析サイトを利用することです

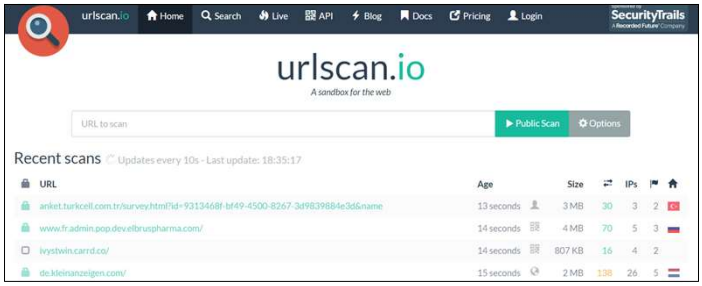
19

解析サイトについて

- 例えば、以下のようなサイトがあります

aguse.jp（日本）

https://www.aguse.jp



urlscan.io

https://urlscan.io

20

解析サイトについて

- 例えば、以下のようなサイトがあります

Hybrid Analysis

https://www.hybrid-analysis.com

SecURL（日本）

https://securl.nu

解析サイトの注意点

- 解析サイトと、調査するサイトの組み合わせによっては
  情報が正常に取得できない場合があります
  - 例えば、フィッシングサイトを調査したいような場合
    調査対象はフィッシングサイトとしたいのに、
    解析サイトはリダイレクト先の正規のページをスキャンする、など

- 上に関連して、海外の解析サイトの場合、日本狙いのサイトにやや弱い場合があります
  - 日本以外のIPアドレスからのアクセスは、別のページに
    リダイレクトするようなサイトの場合が該当
  - 日本のIPアドレスからアクセスした場合、偽サイトを表示する

解析サイトの注意点

- 解析サイトによっては、VirusTotalと同様に
  送信したURLやスキャン結果を他人に見られてしまうことがある

- URLにはメールアドレスやIDなどの情報を含んでいることがあるため、
  そのままスキャンを行うとその情報が外部公開されたり、
  攻撃者（サイトの運営者）にIDが利用されていることが知られてしまう

例：
https://hogehoge.com/CheckNew.html?TV9JRD0xNDgzOTk4MTY3Nw==（略）
&Q0lEPTAwMg==&URL=https://piyopiyo.com.br/wata/meow/dice/ban@iica.jp
というようなURLだったら…

解析サイトの注意点

例：
https://hogehoge.com/CheckNew.html?TV9JRD0xNDgzOTk4MTY3Nw==（略）
&Q0lEPTAwMg==&URL=https://piyopiyo.com.br/wata/meow/dice/ban@iica.jp

このようなURLを解析サイトで調べる場合、以下のような部分は削るか
全く別の文字列で置き換えるなどの対策が必要

- 「?」や「id=」などに続いて、文字列がある
- メールアドレスやIDがそのままURLに入っている

メールの構造

- 普段、みなさんがよく使っているメール
  - ご存知の通り、画像やWordファイルなどを添付することができます
- CTFの中で触れたかもしれませんが、実はメールでは「テキスト」の情報しか
  やり取りすることができません
- つまり、1通のメールでは以下の情報をすべてテキスト化して
  メールサーバの間でやり取りしています
  - 宛先、差出人
  - 件名、本文
  - （あれば）添付ファイル

25

25

メールの構造

- また、1通のメールは大きく以下の2つの部分に分けられます

① ヘッダ部分…宛先、差出人、件名など
  - この部分に、経由したメールサーバの情報（IPアドレス）や
    なりすまし防止の情報（後ほど説明します）が含まれます

② ボディ部分…本文、添付ファイル
  - 添付ファイルについては、Base64形式でテキストに変換されます

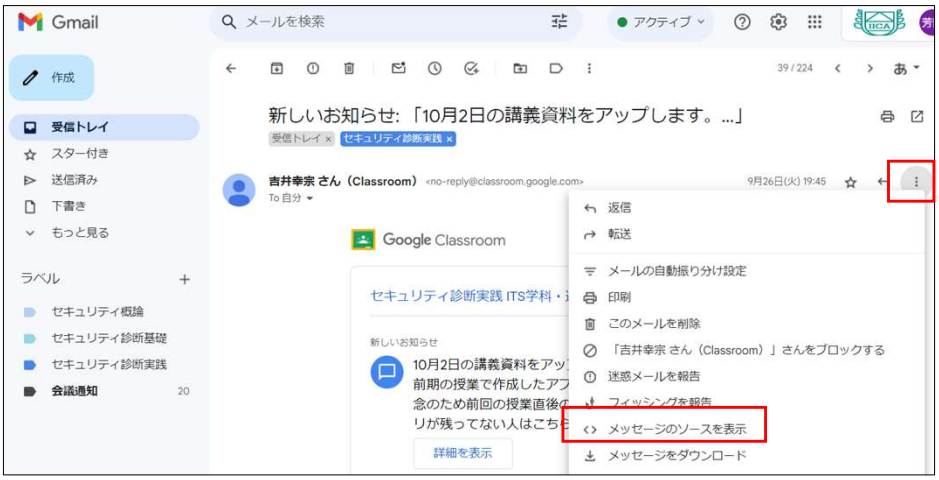
- 今回は、ヘッダ部分について詳しく取り上げます

26

26

メールのヘッダ部分（メールヘッダ）

- Gmailでは、メール返信ボタンの右にあるボタン→「メッセージのソースを表示」で、メールのヘッダ部分、ボディ部分を見ることができます。



メールのヘッダ部分（メールヘッダ）

- Gmailでは、メール返信ボタンの右にあるボタン→「メッセージのソースを表示」で、メールのヘッダ部分、ボディ部分を見ることができます。

メールのヘッダ部分（メールヘッダ）

- ヘッダ部分にはさまざまな項目がありますが、
  経験上、主に以下の項目を見ることが多いです。
  - Date：メールの送信日時
  - To：宛先のアドレス
  - From：差出人のアドレス
  - Return-Path：メールが配送されなかった場合のエラーの通知先
  - Received：メールが中継されたサーバ（機器）の情報と、その時刻

- 中でも、一番よく使うのが「Received」ヘッダになります。

Receivedヘッダとは

- 「Received」ヘッダには、メールが中継された際の情報が記録されます。

例：

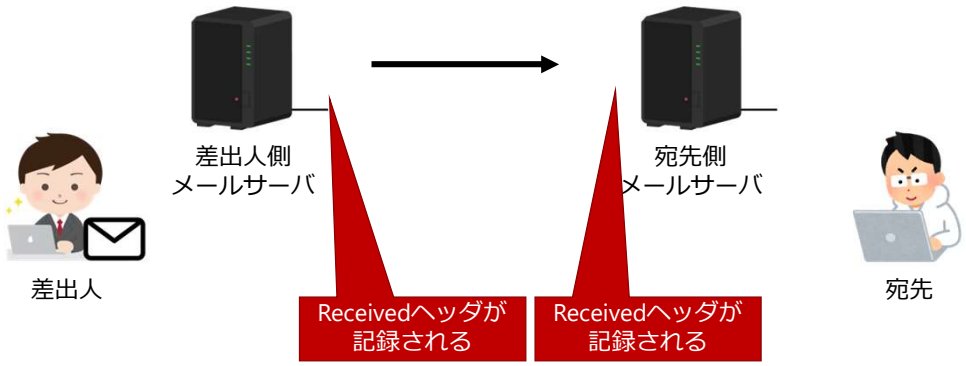
Received: from mail002.b-2.jp (mail002.b-2.jp. [219.99.184.60])
by mx.google.com with SMTP id u17-20020a631411000000b00585999a38a6(略)
for <ban@iica.jp>;

- from：送信元のサーバの名前　（例では、mail002.b-2.jp）
- by：メールを受け取ったサーバの名前　（例では、mx.google.com）
- for：メールの宛先アドレス

つまり、「mail002.b-2.jp」から「mx.google.com」にメールが中継されたということ。

Receivedヘッダとは

- 「Received」ヘッダには、メールが中継された際の情報が記録されます。
- 基本的に、メールは宛先に届くまでに複数のサーバを経由します。
  - サーバを経由するたびに、Receivedヘッダが付与されます。

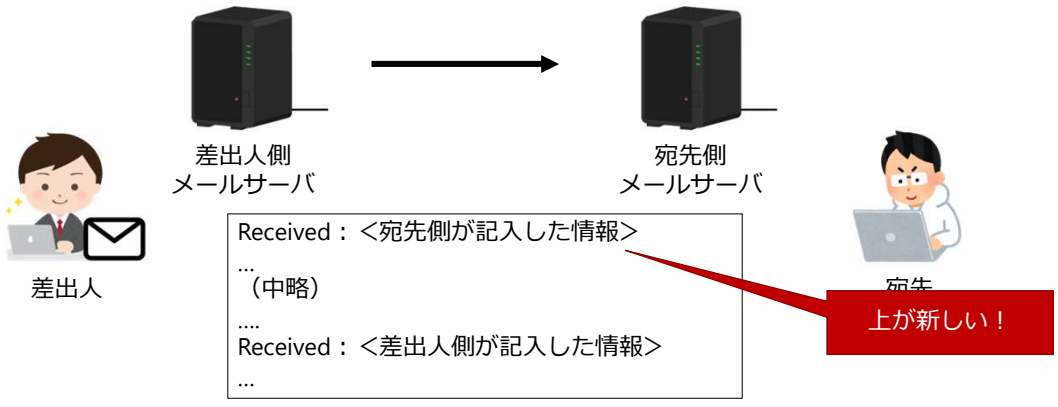


31

31

Receivedヘッダとは

- なお、これらのヘッダは上にいくほど新しい情報になります。
- つまり、メールの経路をたどる場合には、Receivedヘッダを下から追うことになります



32

32

今日の内容

- CTFの補足
  - VirusTotalの使い方、注意点
  - 解析サイトの使い方、注意点
  - メールの構造、ヘッダの見方
- メールの問題について考えてみよう
  - PPAP
  - メールのなりすまし対策

メールの問題について考えてみよう

- 先ほど説明したように、メールはみなさんもよく使うツールです
- また、仕事でもメールは欠かせないものとなっています
  - SlackやTeamsなどのコミュニケーションツールはありますが、
    お客さま・取引先との連絡は基本的に電話かメールです
- ここまで普及し、一般的に使われているメールですが
  実はいくつか問題を抱えています
  - 今回はみなさんにその問題について知ってもらおうと思います

PPAPとは

- メールで添付ファイルを送るときに、盗み見などを防ぐため
  暗号化して（パスワードをかけて）送るというケースがよくありました
  - 個人情報が含まれるファイルなどが対象
  - パスワードは、別のメールで送ります

- 暗号化する（パスワードをかける）ことで、盗み見（盗聴）だけでなく
  誤送信対策もできる、というメリットがよくあげられていました
  - パスワードを知らない限り、そのファイルを開くことができない、という理屈

- しかし、このパスワード付きファイルを送ることが、
  セキュリティ上問題であるということがここ数年で話題になっています

PPAPとは

- この方法の何が問題なのか？
  - ウイルススキャンをすり抜ける
    パスワードがかけられたZipファイルは、ウイルス対策ソフトや
    アンチスパムなどで検査することができない
  - メールボックスなどが盗み見されていたら、そもそも無意味
    メールを見られるのであれば、Zipファイル本体も、
    パスワードの通知メールも盗むことができる（保護できない）
  - Zipのパスワードそのものが脆弱になってきている
    以前紹介したように、オフラインであればGPUなどを利用して
    総当たり攻撃を現実的な時間で仕掛けることができる

などといった問題があると言われています

PPAPとは

- この方法は、
  - PasswordつきZipファイルを送ります
  - Passwordを書いたメールを送ります
  - Angoka（暗号化）
  - Protocol（プロトコル）

の頭文字をとり、「PPAP」と呼ばれるようになりました。

※数年前に流行した、とある芸能人（リンゴとペンを持った）も
　このネーミングに影響していると思います

37

37

PPAPの解決策

- では、このPPAPの運用をやめたい（が、安全にファイルを送りたい）と
  なったら、どのような手段があるでしょうか

- 実際に考えてみましょう

38

38

メールのなりすまし対策

- メールは、その仕組み上なりすましが簡単にできてしまいます。
  - 実は、Fromアドレスを自由に設定することが可能です
- そもそも、メールの仕組みができた当時は、なりすましなどを想定しておらず
  なりすましを防ぐ方法もなかったと思われます。
- その結果（？）フィッシングメールや迷惑メール、Emotetなどで
  なりすましが多くなってしまったのは皆さんも知っての通りです

メールのなりすまし対策

- メールのなりすましを防ぐには、以下のような方法があります

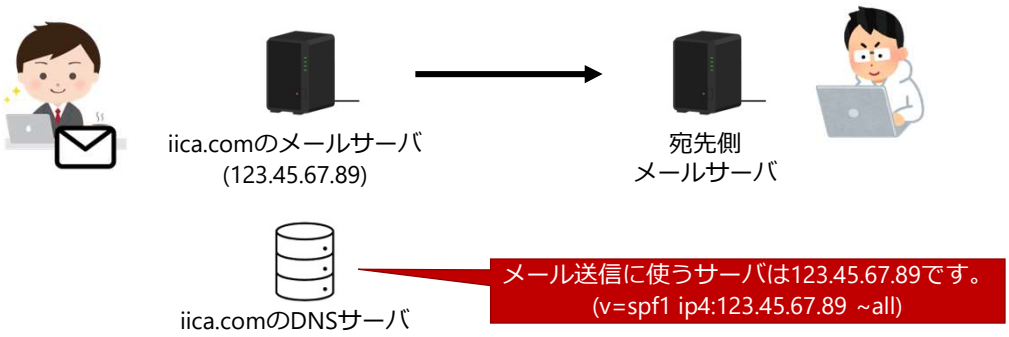
① SPF（Sender Policy Framework）…メール送信に使うサーバを事前に登録する

② DKIM（DomainKeys Identified Mail）…送信メールに電子署名を付加する

- 上記の2つの方法について、それぞれ解説します

SPF（Sender Policy Framework）

- SPF（Sender Policy Framework）…メール送信に使うサーバを事前に登録する
- 例えば、「iica.com」のメールサーバが「123.45.67.89」というIPアドレスだったら、DNSサーバに「メールサーバは123.45.67.89です」という情報を登録します

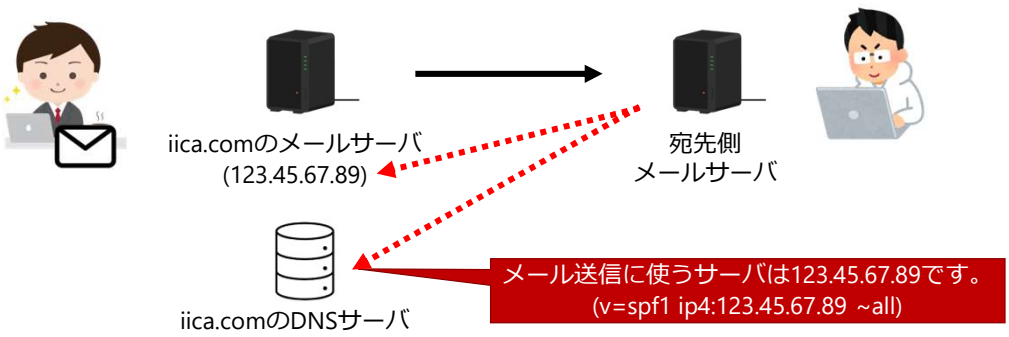


41

41

SPF（Sender Policy Framework）

- メールを受け取ったメールサーバは、
  メールを送ってきたサーバのIPアドレスと、差出人のドメインのDNSサーバの情報を
  比較して、IPアドレスが一致すれば本物だと判断します。

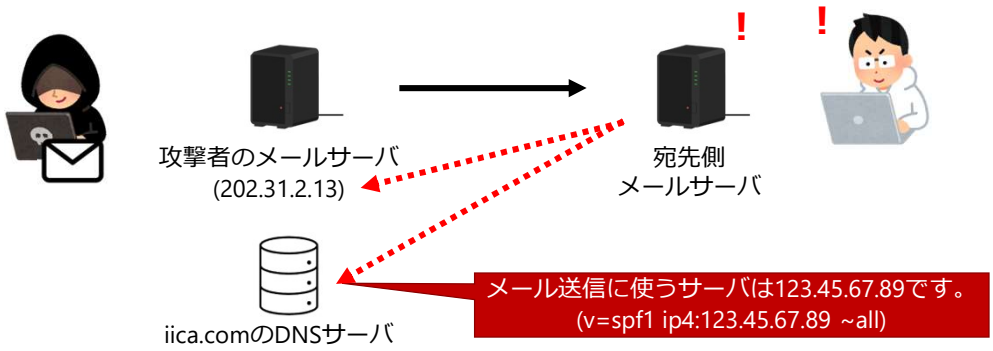


42

42

SPF（Sender Policy Framework）

- 攻撃者が、差出人を変えることでiica.comになりすましたメールを送ってきても
  メールサーバのIPアドレスが登録されたIPアドレスと異なるため、
  なりすましたメールだと判断することができます。



SPF（Sender Policy Framework）

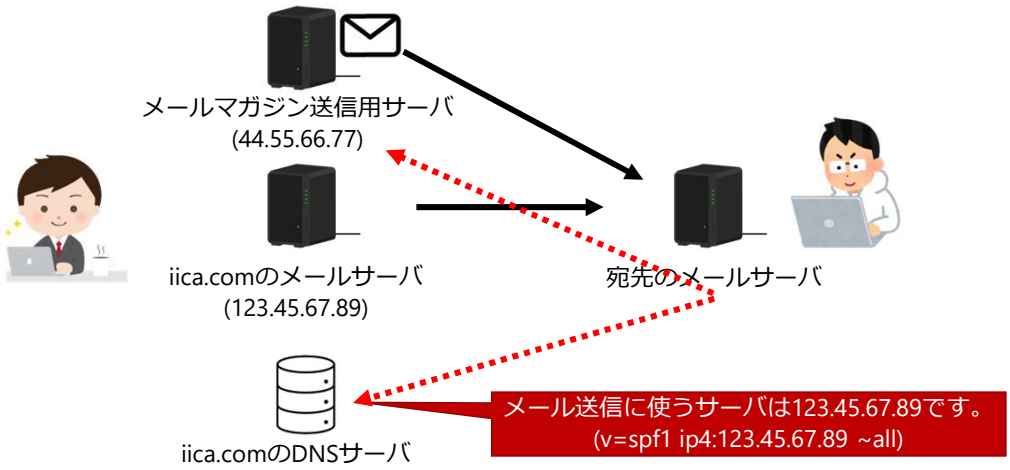
- SPF（Sender Policy Framework）…メール送信に使うサーバを事前に登録する

- メールマガジンを送ったり、自社以外のサーバからメールを送るような場合は
  そのサーバの情報もDNSサーバに登録する必要があります。
  - 登録を忘れると、本当に必要なメールなのになりすましと判定されて
    迷惑メール扱いされたり、宛先に届かない場合があります

- また、メールが転送されたような場合にはIPアドレスが変わってしまうため
  なりすましと判定されることが（仕組み上）あります

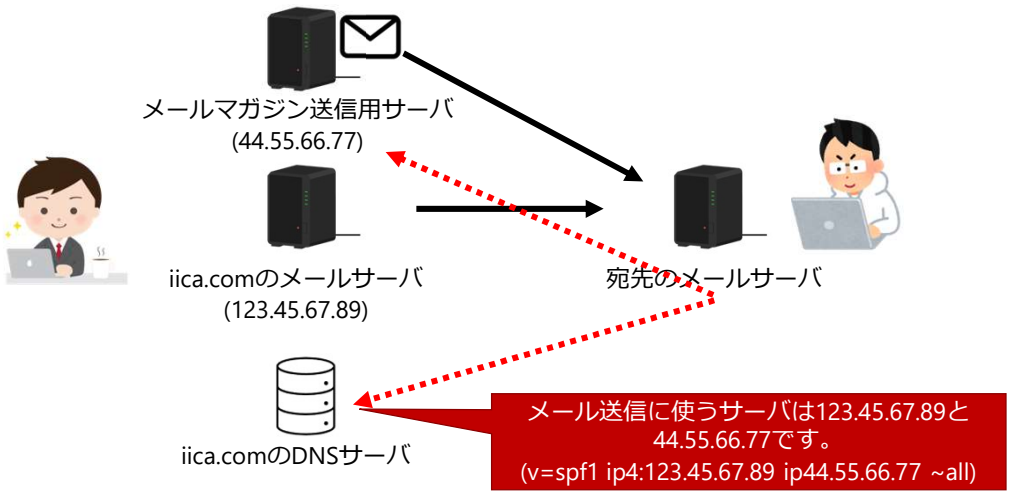
SPF（Sender Policy Framework）

- メールマガジンの例



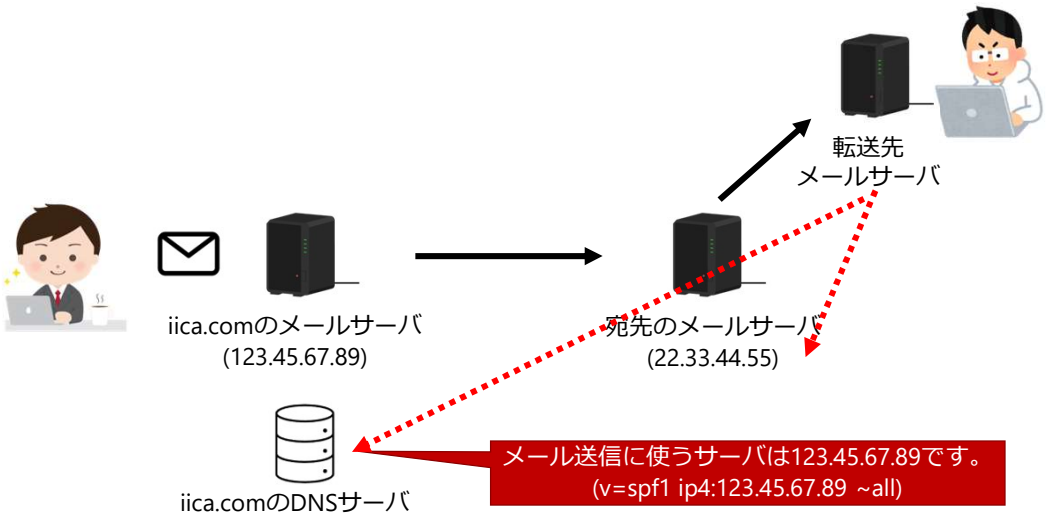
SPF（Sender Policy Framework）

- こういった場合には、メールマガジン送信用サーバの情報も登録する必要があります。



SPF（Sender Policy Framework）

- 転送の例



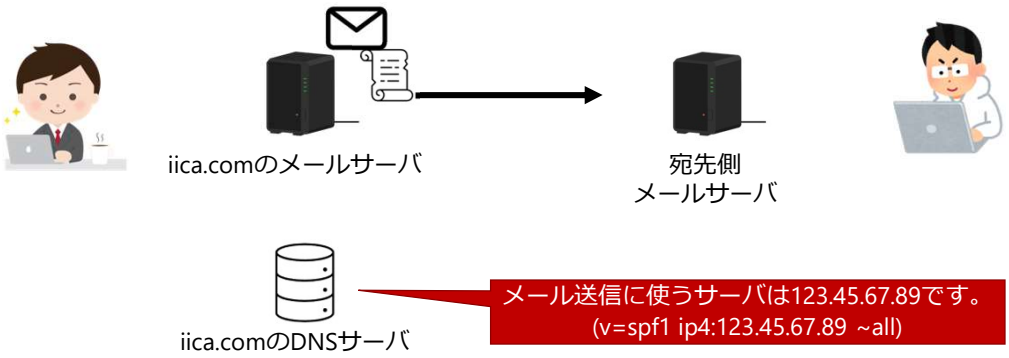
SPF（Sender Policy Framework）

- SPF（Sender Policy Framework）…メール送信に使うサーバを事前に登録する
- 以前解説した、nslookupコマンドでこの登録内容を見ることができます。
  - コマンドプロンプトで「nslookup」と入力
  - set type=TXT と入力
  - 確認したいドメイン名（iica.jp）などを入力

```
権限のない回答:
iica.jp text =

        "v=spf1 include:_spf.google.com ~all include:crmstyle.com ~all include:_spf.lolipop.jp ~all"
```

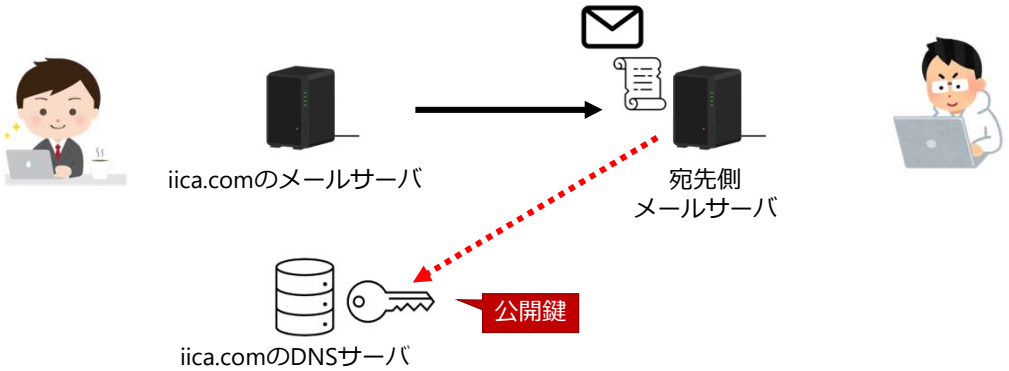
DKIM（DomainKeys Identified Mail）

- DKIM（DomainKeys Identified Mail）…送信メールに電子署名を付加する
- メールサーバでは、送信するメールに電子署名を付与します



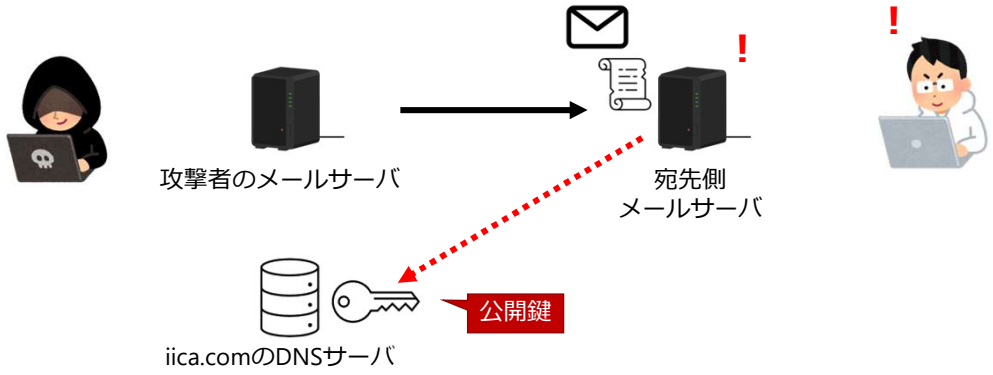
DKIM（DomainKeys Identified Mail）

- メールを受け取ったメールサーバは、メールに付与された電子署名を
  差出人ドメインのDNSサーバに公開されている公開鍵で検証します。
- 検証に成功すれば、そのメールはなりすましされておらず、改ざんもされていない
  ことが判断できます。



DKIM（DomainKeys Identified Mail）

- 攻撃者がなりすましメールを送ろうとしても、攻撃者はなりすまし先ドメインの秘密鍵を持っていないので、正しい電子署名を作ることができません。
- そのため、メールサーバでは電子署名の検証に失敗します。



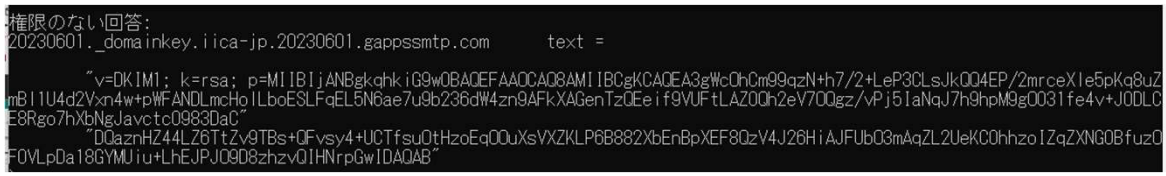
DKIM（DomainKeys Identified Mail）

- DKIM（DomainKeys Identified Mail）…送信メールに電子署名を付加する
- メールのヘッダ部分で、付与された電子署名の情報を見ることができます

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=iica-jp.20230601.gappssmtp.com; s=20230601; t=1696210886; x=1696815686; darn=iica.jp;
        h=cc:to:subject:message-id:date:from:mime-version:from:to:cc:subject
         :date:message-id:reply-to;
        bh=YNMZhfyTuS9cWcwDSd/iMdtBaFpacb6/kO6dDOXoyyc=;
        b=fDttNBumNNHA7Qi6qKxhKF1YGwPOpGQNaxqwb9unNWMuudOgrnTBm4n5jF8yH+eQiy
         4OREFaZcOPZPdenaO3OaAaORDdcAi9Rk6Y8mYJvdY4daQ/ChvwD4KyawVOcdQqmKKORS
         vUEBqCnIdHAM26x/N47fh1taZJrapwNmyRPsTg6gJgj2nddjgdeK8Os9NNXPc6fVFuyW
         97cs7OzcaLwkQssJXuty4V2/AEIOuIIJWhRO9PhPFc5VOd4SnU6G7TZBXCRjP8de3nGI
         3pqmHwvOS+QCIc1ROk+f+IPjX32g7dqVUUYOwYoxoXjSrV6+Z4fGfuaJMh1z6aLZAzOd
         J3IQ==
```

DKIM（DomainKeys Identified Mail）

- DKIM（DomainKeys Identified Mail）…送信メールに電子署名を付加する
- また、nslookupコマンドでDNSサーバに登録された公開鍵の情報を
  調べることができます。



メールのなりすまし対策（DMARC）

- また、SPF・DKIMとは別にDMARCという仕組みもあります。
- SPFやDKIMは「送信元が正しいかどうか」を判別する仕組みです
- DMARCは、SPFやDKIMとセットで利用します
  - SPFとDKIMの両方と組み合わせて使うことも可能です
- DMARCでは「SPFやDKIMの認証に失敗した場合、メールをどう扱うか」を
  送信元で宣言することができます
  - DMARCなしの場合、認証に失敗したメールの扱いは
    受信者側の判断に任せられています

メールのなりすまし対策（DMARC）

- DMARCでは「SPFやDKIMの認証に失敗した場合、メールをどう扱うか」を
  以下の3つから送信者が宣言することができます
  - 受信拒否(reject)
  - 隔離(quarantine)
  - 何もしない(none)

- それに加えて、メール受信元からSPF・DKIMの認証結果について
  詳細なレポートを受け取ることができます
  - その結果、SPFなどの設定漏れ（正しいメールが認証に失敗していないか）、
    自ドメインのなりすましメールが送られていないか、などを
    知ることができます

メールのなりすまし対策

- これらのなりすまし対策について、ユーザー側で確認する必要はなく
  メールソフトやGmailなどで自動で処理してくれています
  - ゆえに、ユーザーはこれらの対策を意識することがあまりないですが
    GmailではSPF・DKIMのチェック結果を確認することができます

メールのなりすまし対策・まとめ

- Googleは、これらのなりすまし対策がされていないメールについて
  対応を厳しくしていくことを表明しています
  - 具体的には、個人で利用しているGmailに対してメールを送る場合
    受信を拒否したり、迷惑メールとして扱うなど
  - 特に、1日で5,000件以上のメールを送るような送信元はより厳しくなります
- Gmail以外にも、メールのセキュリティを強化する動きは活発化すると思われます

- 今後、みなさんが就職・起業するにあたってメールは必ず使うことになります
  - 起業する場合はドメイン取得やメール設定も必要になると思います
  - その際に、お客さまにメールが送れない・届かないといったトラブルを避けるため
    今日説明した内容が役に立てば幸いです

今日の振り返り

今日のキーワード

VirusTotal、メールヘッダ
SPF、DKIM、DMARC

今日のゴール

- ✓ VirusTotalやWebサイトの解析を行うサイトなど、
  外部ツールの機能や使い方について学ぶ。
- ✓ メールのヘッダの内容や、メールに関係する問題について
  理解し、考えてもらう。

課題について

今日の課題

- Google Classroomにアップします。
- 提出期限：12/22（金）17:00

59

59

質疑応答

- 本日の講義の中で、わからなかったこと、気になったことがあれば
  ぜひ質問してください。
- また、授業後の課題（アンケート）、メールでも質問OKです。
  次回の私の講義にて回答します。

60

60

Idea IT College Aso
専門学校　イデアITカレッジ阿蘇

Webアプリ脆弱性診断2

セキュリティ診断実践
(2024/1/15)

担当講師：吉井 幸宗（ yoshii@iica.jp ）

Ver.1.1.0

今日の内容とゴール

今日の内容

- 前回のおさらい
  - 画面遷移図
- Webアプリ脆弱性診断
  - 診断作業の流れ
  - 診断を実施するための準備
  - 診断する

今日のゴール

- ✓ Webアプリ脆弱性診断作業の流れを知る
- ✓ 診断作業の準備をする
- ✓ 実際に診断をやってみる

前回のおさらい

画面遷移図

5

画面遷移図

- 脆弱性診断業務の流れ

対象サイトの全体をざっくりと把握	診断対象となるページを決める。 全機能の診断はコストや期間から合理的ではないため。
↓	
診断対象ページの機能を把握	正常な挙動、各パラメータや必要な事前条件などを確認し **画面遷移図**としてまとめる
↓	
実際に診断作業を行う	ツールによる自動診断と手作業での手動診断を組み合わせる 見つかった点をメモし報告書にまとめる
↓	
報告書の提出、報告会など	わかりやすい報告 場合によっては修正後の再診断なども

6

画面遷移図

- 画面遷移図とは何か？
  - 診断対象のWebサイトを調査・整理し、Webサイトが動作する際に送信される各種リクエスト（通信）を一覧表にまとめて記載したもの
  - 診断対象のリクエストと診断対象外のリクエストを明確にする

Webアプリ脆弱性診断

診断作業の流れ

診断作業の流れ

- 脆弱性診断業務の流れ

対象サイトの全体をざっくりと把握	診断対象となるページを決める。 全機能の診断はコストや期間から合理的ではないため。
↓	
診断対象ページの機能を把握	正常な挙動、各パラメータや必要な事前条件などを確認し 画面遷移図としてまとめる
↓	
実際に診断作業を行う	ツールによる自動診断と手作業での手動診断を組み合わせる 見つかった点をメモし報告書にまとめる
↓	
報告書の提出、報告会など	わかりやすい報告 場合によっては修正後の再診断なども

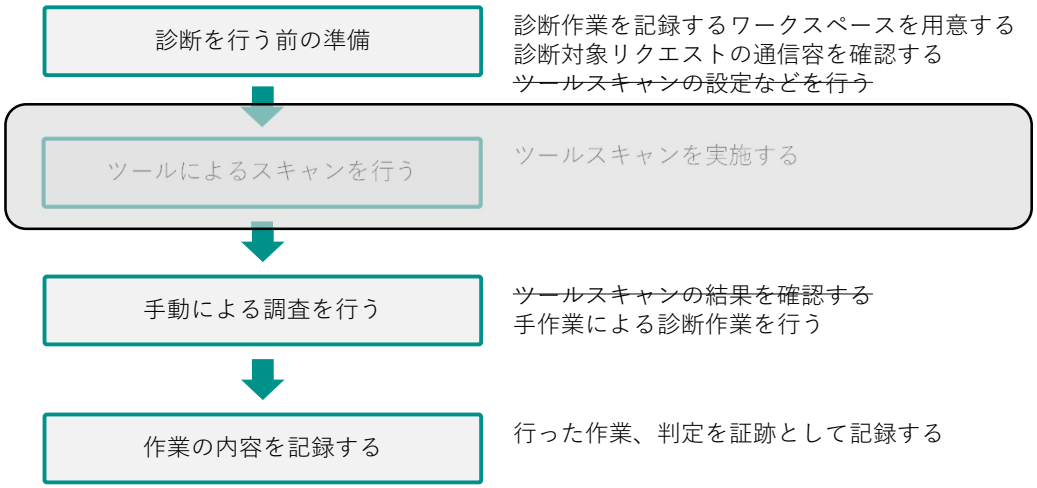
診断作業の流れ

- 実際に診断作業を行う

診断を行う前の準備	診断作業を記録するワークスペースを用意する 診断対象リクエストの通信容を確認する ツールスキャンの設定などを行う
↓	
ツールによるスキャンを行う	ツールスキャンを実施する
↓	
手動による調査を行う	ツールスキャンの結果を確認する 手作業による診断作業を行う
↓	
作業の内容を記録する	行った作業、判定を証跡として記録する

診断作業の流れ

- 実際に診断作業を行う



11

診断作業の準備

12

診断作業の準備

- 診断記録用のワークスペースを用意する
  - recordフォルダ
    - 00_テンプレート.adoc
    - common.adoc
  - 診断記録はAsciiDocで行う
    - VSCodeで開く
      - Extension「AsciiDoc」をインストールするとプレビューが表示できる

診断作業の準備

- 診断記録ファイルを作る
  - 診断対象リクエストごとに1ファイルを作成
    - 03_ログイン.adoc
    - 06_検索.adoc
    - 07_検索（任意の書籍を選択）.adoc
    - …
  - サイト全体で共通する診断
    - common.adoc

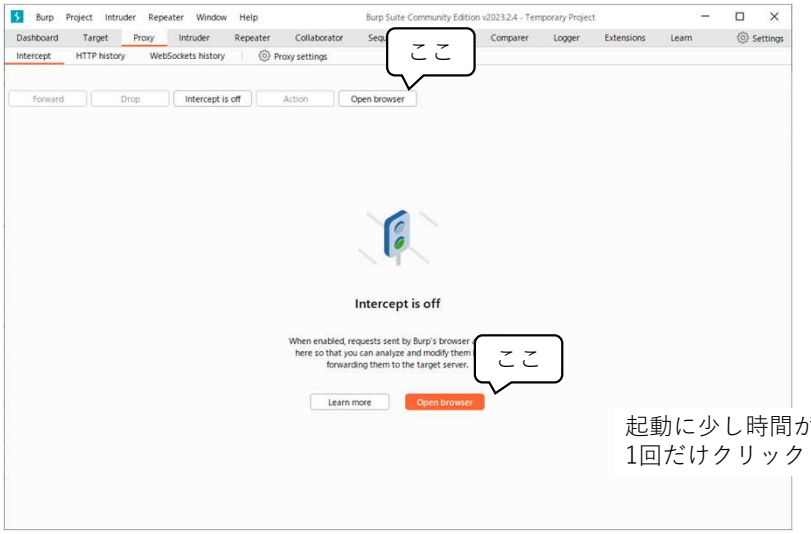
診断作業の準備

- 診断項目のピックアップ
  - 診断対象のリクエストについて必要な検査を見極める
  - そのために以下を調査して記録する
    - そのリクエストがもつ機能
    - リクエスト・レスポンスの特徴
    - パラメータの値と役割
    - その他

診断作業

診断作業

- Burpのビルトインブラウザを起動



起動に少し時間がかかるので
1回だけクリックして待つ

17

診断作業

- Bad図書館サイトにアクセス
  - https://badlibrary.vuln-demo.net/
  - Basic認証
    - iica2023/iica2023

18

診断作業

- ログイン機能を検査してみる
  - 03_ログイン.adoc
    - 機能概要などを記入する
    - 診断項目をピックアップする
    - 各診断項目を検査して記録する

診断作業

- リクエストの概要を調査
  - 概要
    - リクエストが持つ役割や、注意事項などを記載する
  - Req
    - リクエストの内容や特徴を記載する
  - Res
    - レスポンスの内容や特徴を記載する
  - パラメータ解釈
    - パラメータ名と値、役割を記載する
  - その他メモ
    - その他なにか記載事項があれば記載する

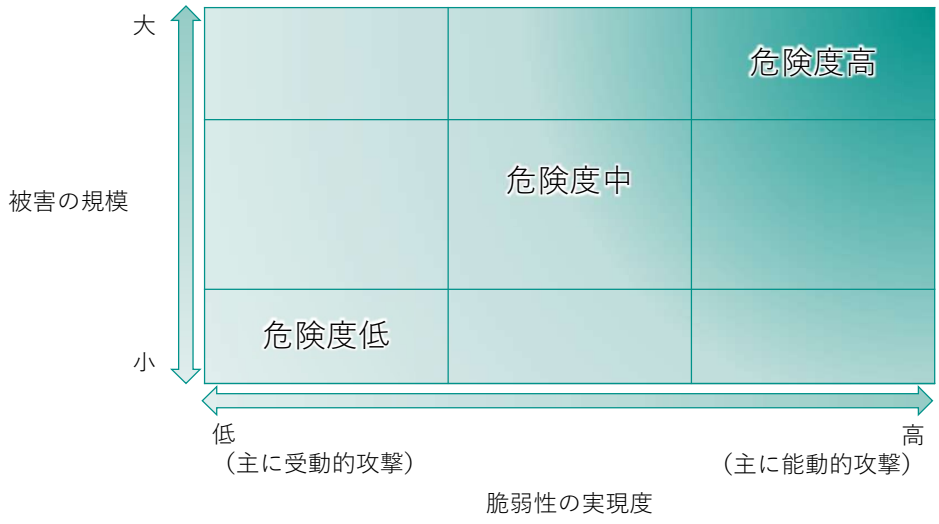
診断作業

- 診断項目の検査
  - 脆弱性の探し方
    - AppGoatで学んだやり方
    - 別冊：「ウェブ健康診断仕様」
      - https://www.ipa.go.jp/security/vuln/websecurity/about.html
  - 検査結果を記録する
    - 「なに」を「どう」したら「どうなった」から、「どう判断したか」「脆弱性があるかないか」が明確にわかるように記載すること

21

診断作業

- 危険度について



22

診断作業

- BurpのRepeaterについて
  - 脆弱性を検査するためには何度もリクエストを送信してトライ＆エラーを繰り返す必要がある
  - そのたびに画面を操作するのは面倒なので、リクエスト再送するBurpの機能を使用する

診断作業

- 脆弱性を発見した場合
  - エビデンスを残す
    - 通信内容（リクエスト・レスポンス）をテキストファイルにする
    - 画面のスクリーンショット

報告書を作成する際に必要な資料を残しておきます

診断作業

- 脆弱性診断は検査をしたら終わりではない
  - 発見した脆弱性を報告するまでが診断業務
    - ただ報告すればいい訳ではなく、脆弱性を理解してもらうことが大事
    - 最終的には問題を修正・対応して脆弱性をなくしてもらうことが目標
- 依頼者が理解しやすい報告書を作成する

25

診断作業

- 診断を進めてください
  - 授業で扱っていない検査観点もあるのでスキップしてよい
  - まずはわかるところを一人でやってみる
    - 他の人と協力して進めてもよい
    - commonの検査項目もわかりそうなところはトライしてよい
- 今後の授業
  - 発見した脆弱性を報告書にまとめる

26

診断項目の説明

診断項目の説明

- セッションの固定化
  - ログイン前後でセッションIDが変わらない場合など、セッションの固定化ができないか
- 不適切な承認(セッションIDの推測)
  - セッションIDが固定だったり、推測が可能だったりしないか
- 情報漏えい(GETでの重要情報送信)
  - GETメソッドのリクエストで重要情報を送信していないか
- 不適切な承認(HTTPでもアクセスが可能)
  - HTTPSのサイト、リクエストがHTTPでもアクセスできないか

診断項目の説明

- 情報漏えい(HTTP接続での重要情報送信)
  - 重要情報を送信するリクエストがHTTPSかどうか
- 登録済みのログインIDが判明
  - ログインIDを送信するリクエストで他者のログインIDが判明しないか
- 不適切な承認(権限のないデータの利用)
  - パラメータを操作して権限のないデータを閲覧、修正できないか
- 不適切な承認(権限のない機能の利用)
  - ユーザごとに異なる権限機能、認証をしないと使用できない機能が利用できないか

診断項目の説明

- 不適切な承認(クロスサイトリクエストフォージェリ)
  - データの変更を行うリクエストにおいて、CSRFが可能か
- クロスサイトスクリプティング (2nd order xss)
  - 蓄積型のXSSがないか
- 機能の悪用(パスワードを平文で表示)
  - パスワード入力フォームがマスクされているか
- クロスサイトスクリプティング
  - 反射型のXSSがないか

診断項目の説明

- SQLインジェクション
  - 意図しないSQLが実行できないか
- OSコマンドインジェクション
  - 意図しないOSコマンドが実行できないか

診断項目の説明

common

診断項目の説明

- 不適切な承認(CookieのSecure属性)
  - httpsでアクセスする場合、セッションのCookieにSecure属性がついているか
- 不適切な認証(サーバ証明書の警告)
  - 無効なサーバ証明書を利用していないか
- 不適切なセッションの期限(タイムアウトが存在しない)
  - 一定時間でセッションが切れるか
- 不適切なセッションの期限(ログアウト機能)
  - ログアウト後にサーバ側でセッションが無効になるか

診断項目の説明

- 不適切なセッションの期限(ログアウトボタンが存在しない)
  - ログアウトボタンが存在するか
- 情報漏えい(HTMLファイルのコメント)
  - 重要情報を含むコメントが残っていないか
- HTTPとHTTPSが混在
  - HTTPSのサイトにHTTPのコンテンツが混在していないか
- X-Content-Type-Optionsヘッダの指定について
  - 診断対象のリクエストにおいて、レスポンスヘッダに「X-Content-Type-Options: nosniff」の指定があるか

診断項目の説明

- 情報漏えい(システム情報)
  - サーバ・ソフトウェアのバージョンなどのシステム情報がレスポンスに含まれていないか
- 機能の悪用(現在のパスワードを記載)
  - 画面上やソースコードにパスワードが出力されていないか
- 不要と思われるWebコンテンツ
  - Webアプリに無関係のファイルが存在しないか

今日の振り返り

今日のキーワード

診断項目のピックアップ、危険度の判定

今日のゴール

- ✓ Webアプリ脆弱性診断作業の流れを知る
- ✓ 診断作業の準備をする
- ✓ 実際に診断をやってみる

Idea IT College Aso
専門学校　イデアITカレッジ阿蘇

CTF(Capture The Flag)2回目

セキュリティ診断 実践
（2024/1/22）

担当講師：伴 芳龍（ ban@iica.jp ）

1

今日の流れ

1.前回講義の振り返り

2.セキュリティ関連のトピック紹介

3.CTF

4.CTFの解説

2

今日の流れ

今日の内容とゴール

今日の内容

- セキュリティ関連のトピック
- CTFの説明
- CTFの登録
- 実践
- 問題の解説

今日のゴール

- ✓ CTF（Capture The Flag）について知る。
- ✓ 実際にCTFを行い、前期で学習した内容や

  その他セキュリティで気をつけることなどについて考える。

前回講義の振り返り

- 前回（12月）の講義では、CTFの補足として以下の便利なツールの説明をしました
  - VirusTotal
  - 解析サイト（urlscan.io、aguse.jp　など）
- また、メールの構造やヘッダの内容の見方、
  そしてメールにまつわる問題について考えてもらいました
  - PPAP
    - どうやって安全にファイルを送ればよいのか？
  - メールのなりすまし対策（SPF、DKIM、DMARC）
    - Gmailでは2月からこれらの対策が重要になります

今日の内容

- セキュリティ関連のトピック
- CTFの説明
- CTFの登録
- 実践
- 問題の解説

セキュリティ関連のトピック

- Gmailのセキュリティ強化
- 偽セキュリティ警告の体験サイト
- CyberChef

Gmailのセキュリティ強化

前回（12月）の講義でも触れましたが、Gmailが「メール送信者のガイドライン」を2024年2月以降適用することを発表しました。

「メール送信者のガイドライン」の要件	
全てのメール送信者の要件	1日当たり5000件以上のメール送信者の要件
送信ドメイン認証のSPFまたはDKIMに対応する	送信ドメイン認証のSPFとDKIMの両方に対応する
送信元のドメインまたはIPアドレスに、有効な正引き及び逆引きDNSレコード（PTRレコード）を設定する	
メールの送信にTLSを使用する	
受信者から報告される迷惑メールの割合を0.1%未満に保ち、0.3%を超えないようにする	
Internet Message Format標準（RFC 5322）に準拠する	
送信者アドレス（ヘッダーFrom）をGmailのメールアドレスに偽装しない	
	送信ドメイン認証のDMARCに対応する
	DMARCをパスする
	【マーケティングメッセージや購読メッセージ】ワンクリックでの登録解除に対応し、メール本文に登録解除のリンクを分かりやすく表示する

（出所：米グーグルの「Email sender guidelines」を基に作成）

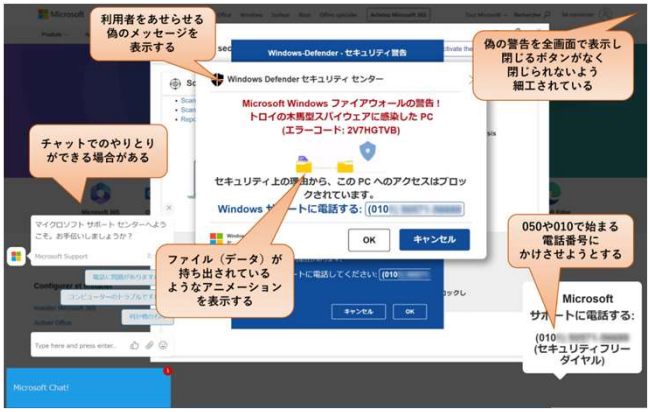
https://xtech.nikkei.com/atcl/nxt/column/18/00001/08712/ より引用

Gmailのセキュリティ強化

- 利用者としての立場では、より安全にメールが利用できるような変更
- メールマガジンを送るような企業では、対応が必須
  - Gmailにメールを送らないということは、現実的にまずない
- Gmailはそれ以前から、適切に設定がされていないような送信者に厳しい
  - SPF/DKIMや、MXレコードの設定などから判断
  - 神奈川県の高校入試出願システムで、Gmailにメールが届かないという事例が最近話題になっていました
  - システムで利用していたメールサーバについて、MXレコードの設定がおかしかったのが原因ではないかという意見があります

偽セキュリティ警告の体験サイト

講義の中で何回か紹介した「偽警告」について、
IPA（情報処理推進機構）が「画面の閉じ方体験サイト」を公開しました。



偽警告の一例とその特徴（IPAサイトより）

偽セキュリティ警告の体験サイト

実際にこの偽セキュリティ警告を体験してみましょう。

https://www.ipa.go.jp/security/anshin/measures/fakealert.html

にアクセスし、以下のボタンをクリック。

※音が鳴ります

偽セキュリティ警告の体験サイト

全画面表示の警告の閉じ方ですが、

- 「Esc」キーを3秒間ほど長押しする　（IPAのサイトで紹介されています）
- 「Alt」キーと「F4」キーを同時に押す
- 「Ctrl」「Shift」「Esc」キーでタスクマネージャーを開き、
  Webブラウザを選択して終了する

などの方法があります。

13

13

CyberChef

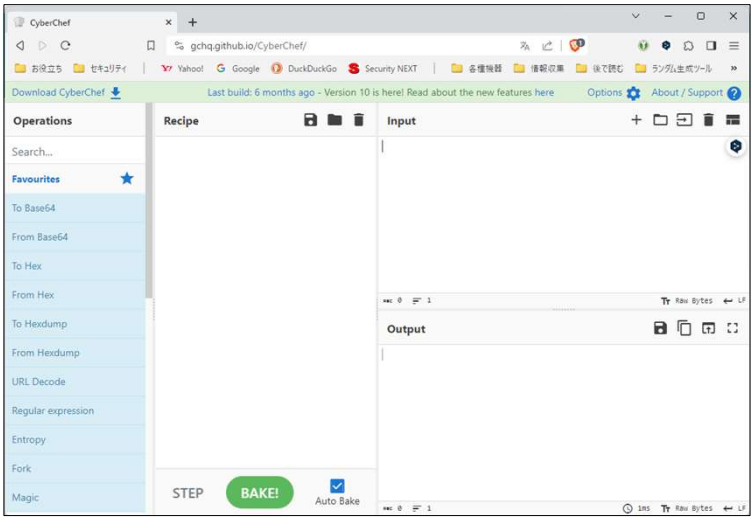
- イギリスのGCHQ（英国政府通信本部）が開発した、無料のWebアプリ
- https://gchq.github.io/CyberChef/
- さまざまな形式のデータを相互変換するために使う
- プログラムコードを書くことなく、複雑な変換が行える
  - また、オフライン環境でも実行可能

14

14

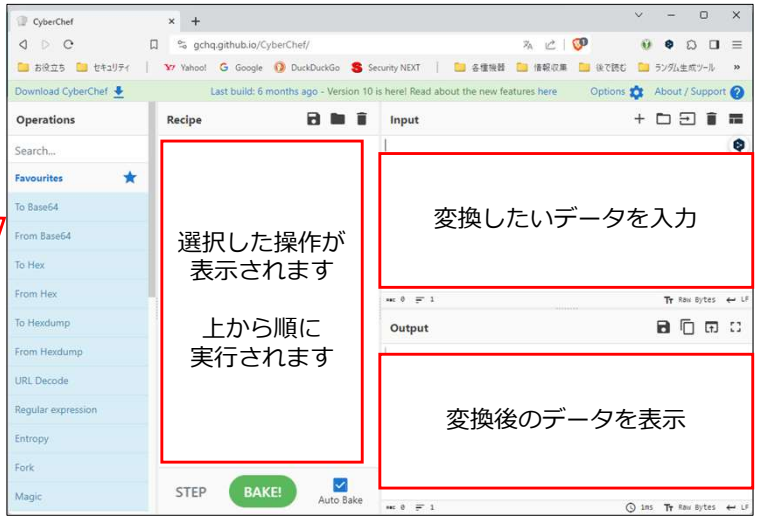
CyberChef

- CyberChefの画面構成



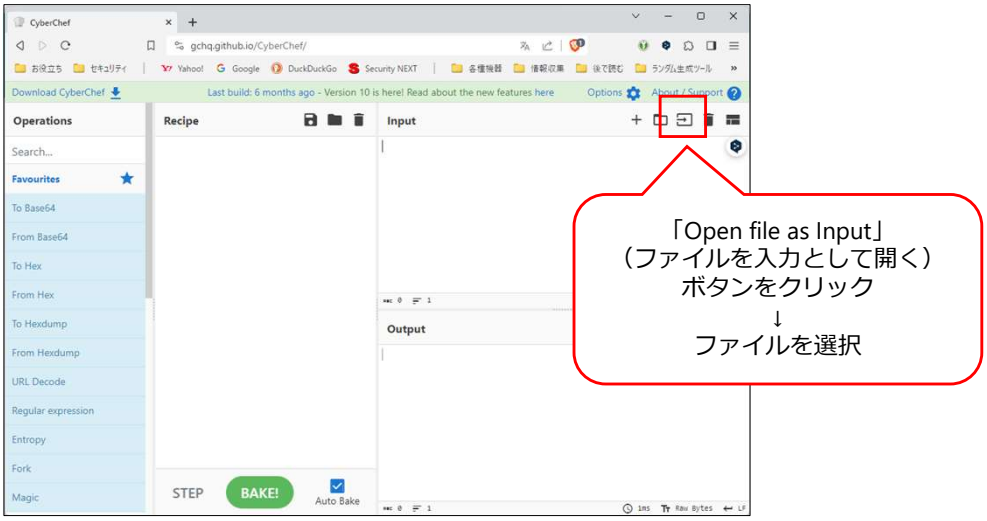
CyberChef

- CyberChefの画面構成



CyberChef

- 例えば、ファイルのハッシュ値を求めたい場合

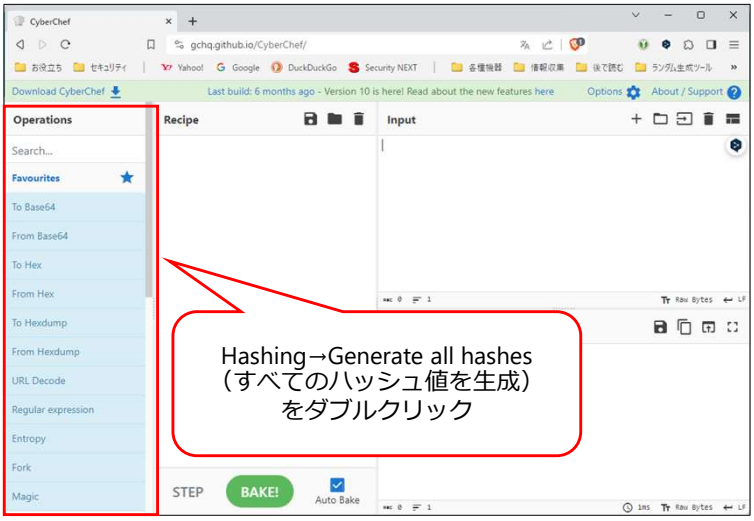


17

17

CyberChef

- 例えば、ファイルのハッシュ値を求めたい場合

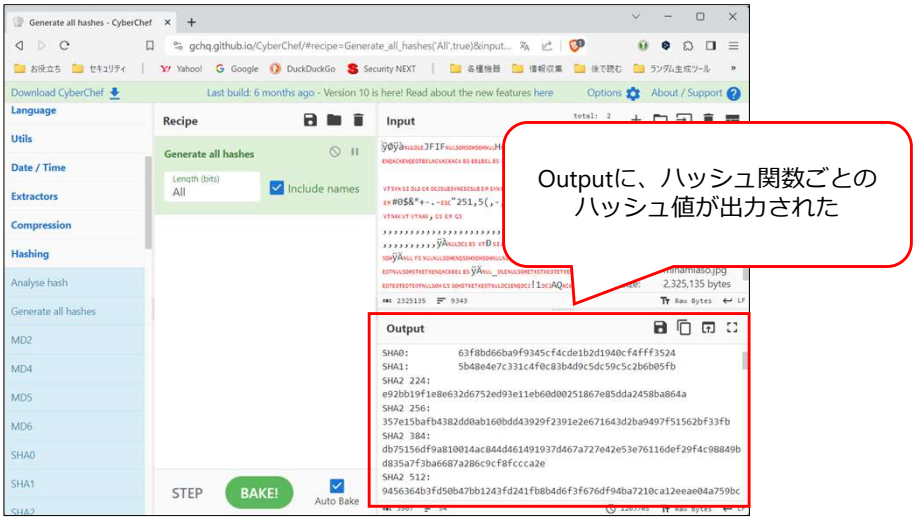


18

18

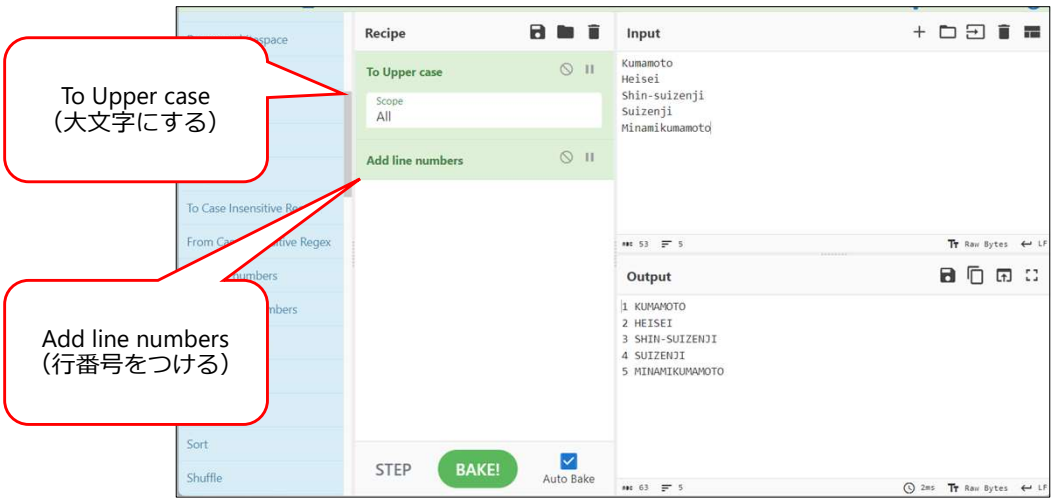
CyberChef

- 例えば、ファイルのハッシュ値を求めたい場合



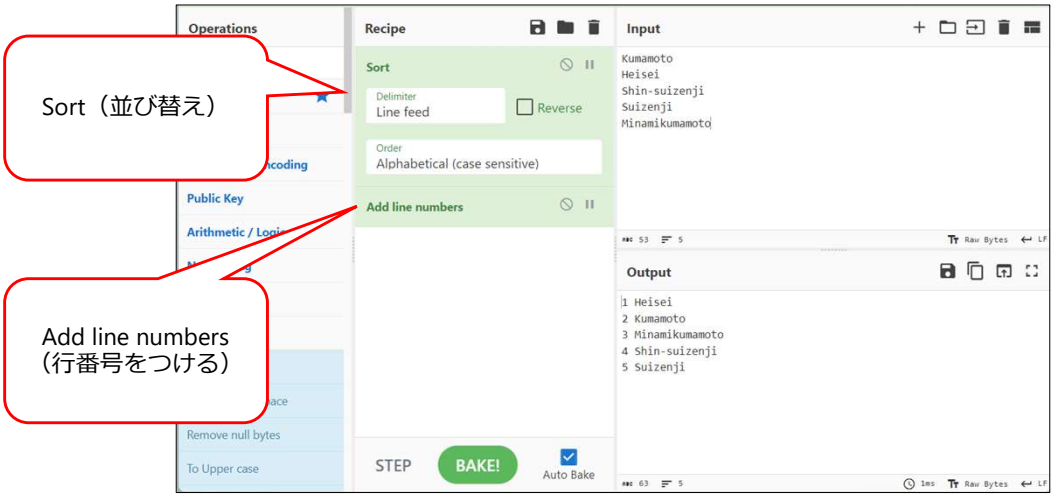
CyberChef

- 複数の処理を連続させるような例



CyberChef

- 複数の処理を連続させるような例



CyberChef…実際に使ってみよう

- 例題１：以下の文章を逆から書いてみましょう。

The quick brown fox jumps over the lazy dog.

- 逆から変換するレシピは「Utils」→「Reverse」

CyberChef…実際に使ってみよう

- 例題２：以下の2進数を10進数に変換してください。

100110100110101011011111010

- ◯進数から、10進数に変換するレシピは「Data format」→「From Base」
  - 「Radix」がデフォルトで36になっているので、2にする
- なお、10進数から◯進数に変換する場合は「To Base」を使います

CyberChef…実際に使ってみよう

- 問題１：以下の2進数を10進数に変換してください。

100110100110101011011110101

- 問題２：以下の2進数を16進数に変換してください。

100100011010001010110011111000

今日の内容

- セキュリティ関連のトピック
- CTFの説明
- CTFの登録
- 実践
- 問題の解説

CTF（Capture The Flag）とは

CTF（Capture The Flag） … 答えとなるFlagを探す、セキュリティのコンテスト

クイズのように行われる形式（Jeopardy）、
サーバやアプリケーションに含まれるフラグを（脆弱性を突くことで）
奪取する形式など、複数の形式があります。

Jeopardy形式では、問題を解くことで得られるFLAG{xxx}という形式のデータを
回答させることが多いです。

CTF（Capture The Flag）とは

CTF（Capture The Flag） … 答えとなるFlagを探す、セキュリティのコンテスト

日本ではSECCON（Security Contest）が
年に1回大規模な大会を開催しています。

それ以外にも、民間でCTFを開催されることが
あります。

https://west-sec.com/vs　など…

「SECCON CTF」が3年ぶりにリアル開催 - 1点差の接戦も

2月11日、12日と浅草橋ヒューリックホール＆カンファレンスで国内最大級のCTFイベント「SECCON CTF 2022」の決勝戦が開催された。カンファレンスイベントなども併催され、3年ぶりとなる現地開催は盛り上がりを見せた。

SECCONは、セキュリティの知識や技術を競うコンテスト。2012年にスタートし、今回で11回目。2021年からは総額100万円の賞金も出ている。新型コロナウイルス感染症の影響で前々回、前回とオンライン開催となったが、3年ぶりに現地開催が戻ってきた。

CTF会場の様子。落ち着いた雰囲気で選手が競技に集中している

11月に開催された予選では、1843人がエントリーし、726チームが得点を獲得。決勝大会は予選上位10チームによる「国際決勝」と、国内に限定した上位12チームによる「国内決勝」にわかれて争った。「国際決勝」には国内から東京大学の学生チーム「TSG」も参戦している。

https://www.security-next.com/143843　より引用

今回実施するCTFについて（ルール）

- 今回は、個人戦形式です。
- 試験とは違い、Googleなどでの検索はOKです。
  - むしろ、分からないことを調べるスキルを身につけてほしいです。
  - ただし、ChatGPTなどのAI利用はNGとします。
- ほとんどの問題は、解答数に制限はありません。
  何回でも挑戦できます。
  - 一部の問題は、入力回数を制限します。

今日の内容

- CTFの説明
- CTFの登録
- 実践
- 問題の解説

今回実施するCTFについて（登録方法）

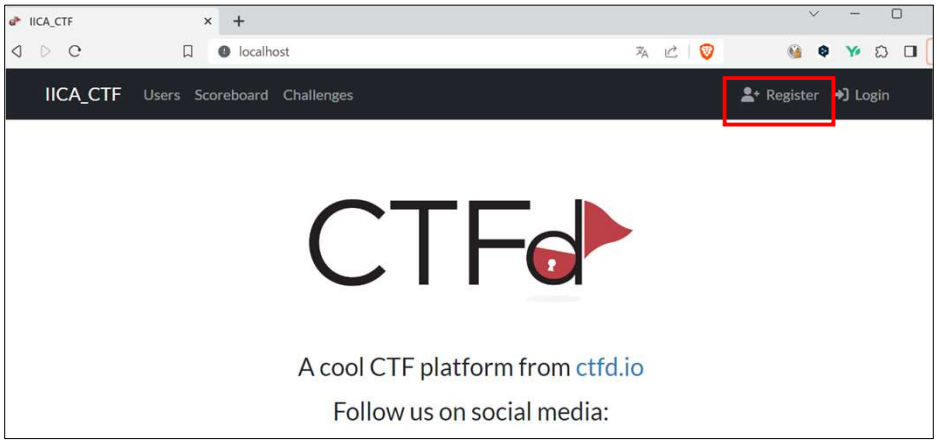
- IICA-Student　に接続します。
- Webブラウザを開き、以下のURLにアクセスしてください。

http://xxx.xxx.xxx.xxx:8000

※URLは講義当日に連絡します。

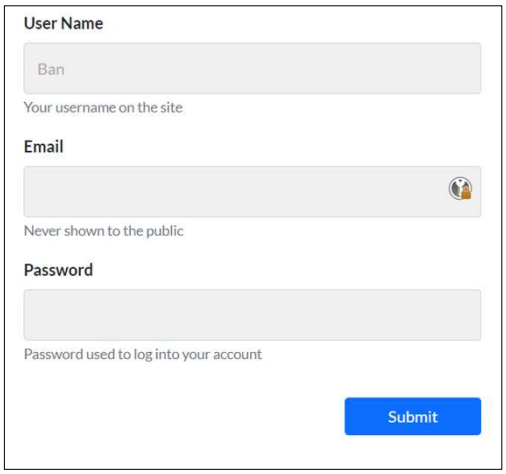
今回実施するCTFについて（登録方法）

- CTFの画面が表示されますので、右上の「Register」をクリックします。



今回実施するCTFについて（登録方法）

- フォームに入力して、「Submit」をクリックします。



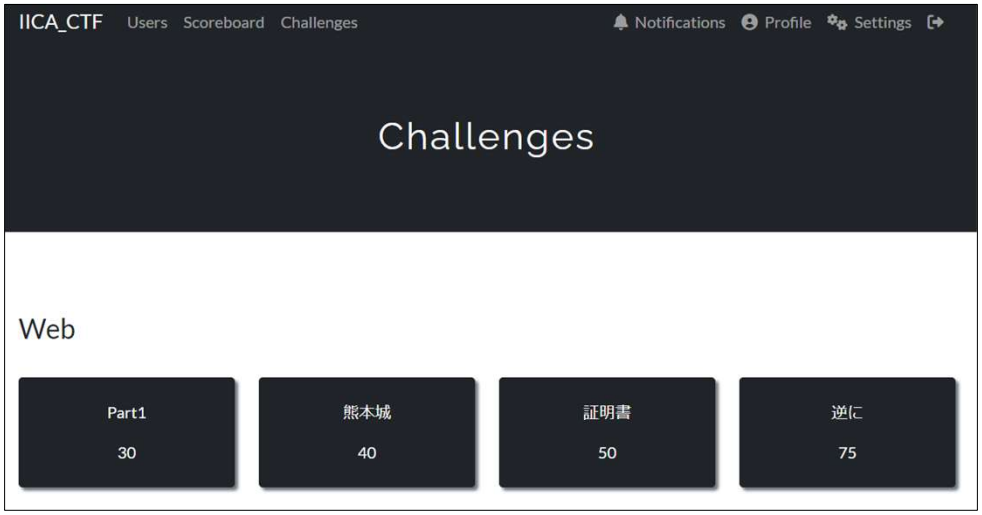
Name：名前を入力します（アルファベット）

Email：aaa@aaa.com　のように、
適当なアドレスを入力します。

Password：好きなパスワードを入力します。

今回実施するCTFについて（登録方法）

- Challenges（問題）が表示されます。



33

33

今回実施するCTFについて（問題について）

- 解きたい問題をクリックすると、以下の画面が表示されます。

34

34

今回実施するCTFについて（問題について）

- 解きたい問題をクリックすると、以下の画面が表示されます。

今回実施するCTFについて（問題について）

- 解きたい問題をクリックすると、以下の画面が表示されます。

今回実施するCTFについて（問題について）

- 問題によっては、以下のような形でFlagが書いてあります。
  - Flag is ○○
  - Flag is “○○”
  - Flag{○○}

  このような場合は、”、{}、isといった部分を含まずに
  ○○　**だけ入力して解答すればOKです**。

- 一部の問題は、得点を使ってヒントを見ることができます。

37

37

今日の内容

- CTFの説明
- CTFの登録
- 実践
- 問題の解説

38

38

実践

- それでは、実際にCTFに挑戦してみましょう。

http://xxx.xxx.xxx.xxx/

制限時間は○○分（～12:00）とします。

今日の内容

- CTFの説明
- CTFの登録
- 実践
- 問題の解説

問題の解説

- 実際のCTFでは問題の解説（答え合わせ）がされることは少ないです。
  - 参加者がWrite-Upという、自分なりの解答をネットに公開することはあります。
- 今回は講義なので、解答できた人が少なかった問題を中心に正解と解き方を解説します。

今日の振り返り

今日のキーワード

CyberChef、CTF

今日のゴール

- ✓ CTF（Capture The Flag）について知る。
- ✓ 実際にCTFを行い、前期で学習した内容やその他セキュリティで気をつけることなどについて考える。

課題について

今日の課題

- Google Classroomにアップします。
- 提出期限：1/29（月）9:00

質疑応答

- 本日の講義の中で、わからなかったこと、気になったことがあれば
  ぜひ質問してください。
- また、授業後の課題（アンケート）、メールでも質問OKです。

Idea IT College Aso
専門学校　イデアITカレッジ阿蘇

Webアプリ脆弱性診断3

セキュリティ診断実践
(2024/1/29)

担当講師：吉井 幸宗（ yoshii@iica.jp ）

Ver.1.0.0

1

今日の内容とゴール

2

今日の内容

- 前回のおさらい
  - 脆弱性診断のやり方
- Webアプリ脆弱性診断
  - 診断作業の続き
  - 診断報告書についての説明

今日のゴール

- ✓ 脆弱性診断を行う
- ✓ 診断報告書について知る
- ✓ 脆弱性診断のゴールをイメージできるようになる

前回のおさらい

脆弱性診断のやり方

脆弱性診断のやり方

- 診断記録ファイルを作る
  - 診断対象リクエストごとに1ファイルを作成
    - 03_ログイン.adoc
    - 06_検索.adoc
    - 07_検索（任意の書籍を選択）.adoc
    - …
  - サイト全体で共通する診断
    - common.adoc

脆弱性診断のやり方

- 診断項目のピックアップ
  - 診断対象のリクエストについて必要な検査を見極める
  - そのために以下を調査して記録する
    - そのリクエストがもつ機能
    - リクエスト・レスポンスの特徴
    - パラメータの値と役割
    - その他

脆弱性診断のやり方

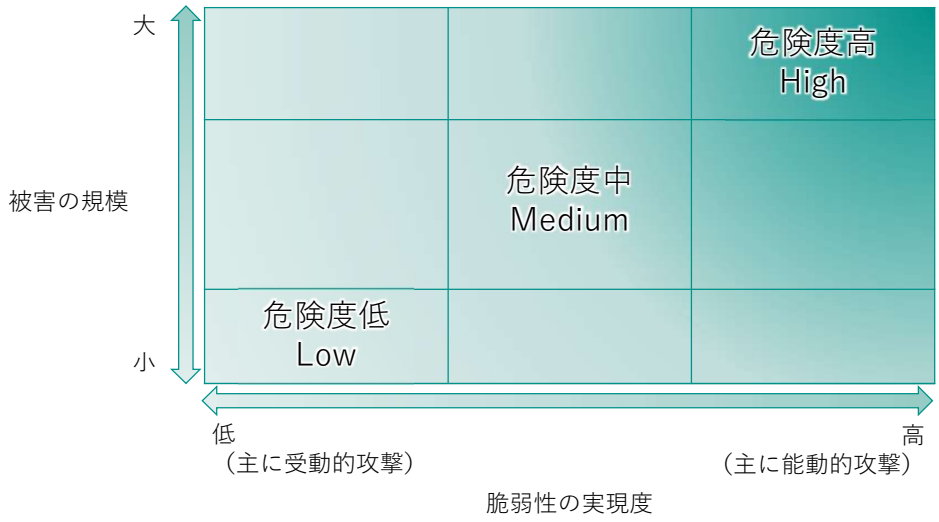
- リクエストの概要を調査
  - 概要
    - リクエストが持つ役割や、注意事項などを記載する
  - Req
    - リクエストの内容や特徴を記載する
  - Res
    - レスポンスの内容や特徴を記載する
  - パラメータ解釈
    - パラメータ名と値、役割を記載する
  - その他メモ
    - その他なにか記載事項があれば記載する

脆弱性診断のやり方

- 診断項目の検査
  - 脆弱性の探し方
    - AppGoatで学んだやり方
    - 別冊：「ウェブ健康診断仕様」
      - https://www.ipa.go.jp/security/vuln/websecurity/about.html
  - 検査結果を記録する
    - 「なに」を「どう」したら「どうなった」から、「どう判断したか」「脆弱性があるかないか」が明確にわかるように記載すること

脆弱性診断のやり方

- 危険度について



脆弱性診断のやり方

- 脆弱性を発見した場合
  - エビデンスを残す
    - 通信内容（リクエスト・レスポンス）をテキストファイルにする
    - 画面のスクリーンショット

報告書を作成する際に必要な資料を残しておきます

診断報告書

診断報告書

- 診断報告書とは？
  - 診断で検出された脆弱性、注意事項を報告するための正式な文書
  - 正式な納品物となるもの
- 全体の説明は次回に
  - 今回は発見した脆弱性を報告する際に記載が必要な情報を説明

診断報告書

- 記載する内容の説明
  - 脆弱性名
  - 危険度
    - High、Medium、Low
  - 脆弱性の概要
    - どのような脆弱性なのかの説明を記載する
  - 発生箇所のURLとパラメータ
    - 脆弱性が検出されたURL、パラメータ名、Cookie名などを記載する
    - 基本的には画面遷移図に記載のURLと一致する

診断報告書

- 記載する内容の説明
  - 脆弱性発生状況
    - 検出した脆弱性の再現方法を記載する
    - どこで、どのような操作（パラメータ改ざんなど）を行った時、どのような現象が発生するのかを順序立てて説明する
  - 想定される脅威
    - この脆弱性を利用された時に、どのような問題が発生するのかを記載する

15

15

診断報告書

- 記載する内容の説明
  - 想定される被害
    - 脆弱性悪用の実現度
      - 実際にこの脆弱性を利用されて攻撃される度合いを説明する
    - 想定される被害
      - 攻撃された場合に起こりうる被害を記載する
  - 対策
    - 対策方法について説明を記載する
  - 参考情報
    - その他、参考にできる情報があれば記載する。なければ削除

16

16

診断報告書

- 注意事項
  - 脆弱性ではないが、Webサイトをよりセキュアにするために対策を推奨するもの

診断する

診断する

- 診断を進めてください
  - 授業で扱っていない検査観点もあるのでスキップしてよい
  - まずはわかるところを一人でやってみる
    - 他の人と協力して進めてもよい
    - commonの検査項目もわかりそうなところはトライしてよい
- 質問があれば随時声をかけてください
  - Meetチャットやメールなどの文章でもOK

19

19

診断する

- Burpのビルトインブラウザで Bad図書館サイトにアクセス
  - https://badlibrary.vuln-demo.net/
  - Basic認証
    - iica2023/iica2023

20

20

今日の振り返り

今日のキーワード

Web診断報告書

今日のゴール

- ✓ 脆弱性診断を行う
- ✓ 診断報告書について知る
- ✓ 脆弱性診断のゴールをイメージできるようになる

Idea IT College Aso
専門学校　イデアITカレッジ阿蘇

Webアプリ脆弱性診断4

セキュリティ診断実践
(2024/2/19)

担当講師：吉井 幸宗（ yoshii@iica.jp ）

Ver.1.1.0

1

今日の内容とゴール

07:29

2

今日の内容

- 質問と回答
- 診断報告書
  - 診断報告書についての説明
  - Bad図書館の診断報告書を作成する
- 次回の授業について

07:29

3

今日のゴール

✓ 診断報告書を作成する

07:29

4

質問と回答

07:29

5

質問と回答

- 課題に点数はあるか？提出が遅れたら？
  - 期限内に提出していれば100点
  - 期限後に提出したら少し減点

07:29

6

診断報告書

07:29

7

診断報告書

- 診断報告書とは？
  - 診断で検出された脆弱性、注意事項を報告するための正式な文書
  - 正式な納品物となるもの

07:29

8

診断報告書

- Bad図書館の診断報告書を作成してください
  - 形式は自由です
    - word、pdf などなんでもよい
    - サンプル報告書、ネットで検索など
  - 脆弱性が見つからなかった場合
    - 脆弱性はなかったという報告書を作成してください

07:29

9

診断報告書

- 作成した報告書を提出してください
  - ファイル名
    - 学生番号_名前_診断報告書
  - 提出先
    - メールに添付して送信してください
    - yoshii@iica.jp
    - 件名
      - セキュリティ診断実践2月19日課題

07:29

10

診断報告書

- 診断報告書の記載内容
  - Web診断サンプル報告書.pdf

07:29

11

診断報告書

- 作成した報告書を提出してください
  - ファイル名
    - 学生番号_名前_診断報告書
  - 提出先
    - メールに添付して送信してください
    - yoshii@iica.jp
    - 件名
      - セキュリティ診断実践2月19日課題

07:29

12

次回の授業について

07:29

13

次回の授業

- 成果発表グループワーク
  - 1年間（特にセキュリティ診断実践の授業）で学んだことをまとめて発表してください
    - 詳細は次回の授業にて
  - グループ分け
    - 依頼中、3グループくらいを予定
  - 日程
    - 2月26日：発表資料作成
    - 3月4日：発表

07:29

14

おまけ

Bad図書館に存在する脆弱性

07:29

15

おまけ

- Bad図書館に存在する脆弱性
  - ログイン画面にSQLインジェクション
  - 貸し出し履歴画面にSQLインジェクション
  - 書籍情報画面にブラインドSQLインジェクション
  - 貸し出し履歴画面に反射型XSS
  - 404エラーページにDOM-based XSS
  - セッションの固定化
  - お問い合わせの内容のログが閲覧可能
  - お問い合わせログのディレクトリインデックス
  - 管理画面にアクセス可能
  - 管理画面での書籍登録でXXE
  - お問い合わせ画面等でCSRF

07:29

16

今日の振り返り

今日のキーワード

Web診断報告書

今日のゴール

- ✓ 診断報告書を作成する

07:29

Idea IT College Aso
専門学校　イデアITカレッジ阿蘇

成果発表グループワーク

セキュリティ診断実践
(2024/2/26)

担当講師：吉井 幸宗（ yoshii@iica.jp ）

Ver.1.0.0

今日の内容とゴール

今日の内容

- 成果発表グループワーク
  - 説明
  - 発表資料作成

3

今日のゴール

✓ 成果発表資料を作成する

4

成果発表グループワーク

5

成果発表グループワーク

- 成果発表グループワーク
  - 1年間（特にセキュリティ診断実践の授業）で学んだことをまとめて発表してください
    - 個人的に聞きたいこと
      - 印象に残った脆弱性
      - Bad図書館の診断で発見した脆弱性
  - 発表資料の形式は自由です

6

成果発表グループワーク

- 日程
  - 2月26日：発表資料作成
  - 3月4日：発表＋伴さんの講義
    - 1グループあたり15分程度

7

成果発表グループワーク

- グループわけ
  - 当日発表

8

今日の振り返り

今日のキーワード

グループワーク

今日のゴール

✓ 成果発表資料を作成する

振り返りとまとめ

❑ Webアプリケーションの脆弱性とその脅威について

理解し、その指摘・報告手順を実践する。