

第12回全国高等学校情報教育研究会全国大会(和歌山大会)

科目「情報セキュリティ」の 授業実践

三重県立亀山高等学校
村山 佳之

新科目「情報セキュリティ」

目標

情報に関する科学的な見方・考え方を働かせ、実践的・体験的な学習活動を行うことなどを通して、健全な情報社会の構築と発展を支える情報セキュリティの確保に必要な資質・能力を次のとおり育成することを目指す。（続く）

新科目「情報セキュリティ」

目標(続き)

- (1) 情報セキュリティについて体系的・系統的に理解するとともに、関連する技術を身に付けるようにする。
- (2) 情報セキュリティに関する課題を発見し、情報産業に携わる者として合理的かつ創造的に解決する力を養う。
- (3) 情報セキュリティが保たれた情報社会の構築を目指して自ら学び、情報システムの運用と管理に主体的かつ協働的に取り組む態度を養う。

新科目「情報セキュリティ」

内容

(1) 情報社会と情報セキュリティ

ア 情報セキュリティの現状

イ 情報セキュリティの必要性

新科目「情報セキュリティ」

内容

(2) 情報セキュリティと法規

ア 情報セキュリティ関連法規

イ 情報セキュリティ関連ガイドライン

新科目「情報セキュリティ」

内容

(3) 情報セキュリティ対策

ア 人的セキュリティ対策

イ 技術的セキュリティ対策

ウ 物理的セキュリティ対策

新科目「情報セキュリティ」

内容

(4) 情報セキュリティマネジメント

ア 情報セキュリティポリシー

イ リスク管理

ウ 事業継続

授業実践

設置学科・学年 システムメディア科3年
(「情報」専門学科)

受講対象 ITシステム系列
(2018年度33名 2019年度28名)

単位数 2単位

授業実践

(1) 情報社会と情報セキュリティ

ア 情報セキュリティの現状

『実際のセキュリティ事故レポート』

【事例検証】実際のセキュリティ事故（セキュリティ事件）を考えてみよう。

- 機密性、完全性、可用性それぞれが損なわれた実例を探してみよう。
- 以下のフォルダにあるファイルを開き、いったん自分のZドライブに保存。
それから入力して、この時間中に印刷して提出。

R:\readonly\19 村山\3 年_情報セキュリティ\4 月 2 2 日\3 限目レポート作成

レポート作成時の注意

- 5W1Hに気をつけよう。ただし、すべてがそろわない場合もある。
When(いつ) Where(どこで) Who(誰が) What(何を) Why(なぜ) How(どのように)
- 単なるコピペではなく、レポートとして成立する文章にしてください。
- 出典 URL を忘れない。

授業実践

(1) 情報社会と情報セキュリティ イ 情報セキュリティの必要性

『「不正のトライアングル」レポート』

【課題】 以下の不正行為について「不正のトライアングル」を想像してみよう。

	機会	動機	正当性
高校生が お酒を飲む			
他人の物を 盗む			
他人の 情報を盗む			

授業実践

(2) 情報セキュリティと法規

ア 情報セキュリティ関連法規

『個人情報保護法について考える』

考えてみよう

1. ネットを使っていて個人情報保護法に違反してしまいそうな場面を想定しよう。

2. 1. で想定したことが起こったらどのような悪影響が起きると思うか考えよう。

3. グループで発表しよう。他の人の発表の要点を書こう。

授業実践

(2) 情報セキュリティと法規

ア 情報セキュリティ関連法規

『三重県警サイバー犯罪対策課による講演・実習』



授業実践

(2) 情報セキュリティと法規

イ 情報セキュリティ関連ガイドライン

『ガイドラインを作成する』

- ①ソーシャルメディアの使いすぎで寝不足になり、体調を崩す人が出てきた。
- ②ソーシャルメディアに悪口などを書き込まれて嫌な思いをする人が出てきた。
- ③ソーシャルメディアに個人情報を書き込まれて拡散されてしまう人が出てきた。

話し合ってみよう

- ①上記のテーマ3つにそって自分が作ったガイドラインをお互いに発表する。
- ②他の人が発表したガイドラインで、良いと思うものをレポートの該当欄に入力する。

授業実践

(3) 情報セキュリティ対策

ア 人的セキュリティ対策

『「脅威」と「脆弱性」パスワード解析』

※今後行う実習について

「情報セキュリティ」の授業で行う実習の中には、実際に悪用可能なものがあります。しかし、悪用した場合には(不正アクセス禁止法)などにより犯罪行為とされます。高校在学中に犯罪行為を行った場合には警察による補導、裁判所による刑事罰だけではなく、学校の指導・懲戒措置(謹慎、停学、退学)の対象になります。

また、授業で扱う実習は教室内かつ授業中を前提に許される行為であることがほとんどです。悪用のつもりがなくても授業以外では決して行わないようにしてください。

授業実践

(3) 情報セキュリティ対策

ア 人的セキュリティ対策

『「脅威」と「脆弱性」パスワード解析』

【実習】「脅威」と「脆弱性」を実際に体験してみよう。

- ① グループ内でパスワードの強度を以下の中からそれぞれの人に割り当ててください。
「数字2けた」「数字3けた」「数字4けた」「英小文字3けた」「英小文字+数字3けた」
- ② エクセルを立ち上げ、A1セルに自分の名前を入れてください。
- ③ ①で決めたパスワード強度に名前を付けたファイル名をつけ、ファイルの種類を「Excel97-2003ブック」を選んで下記フォルダに保存。

授業実践

(3) 情報セキュリティ対策

ア 人的セキュリティ対策

『「脅威」と「脆弱性」パスワード解析』

④ ファイルー情報ーブックの保護ーパスワードを使用して暗号化 を選んで、自分に割り当てられたパスワード強度で好きなパスワードを設定（ただし普段使用していないもの）。

⑤ ファイルを上書き保存する。

⑥ グループ全員のファイルができたなら自分のPCのデスクトップにコピー

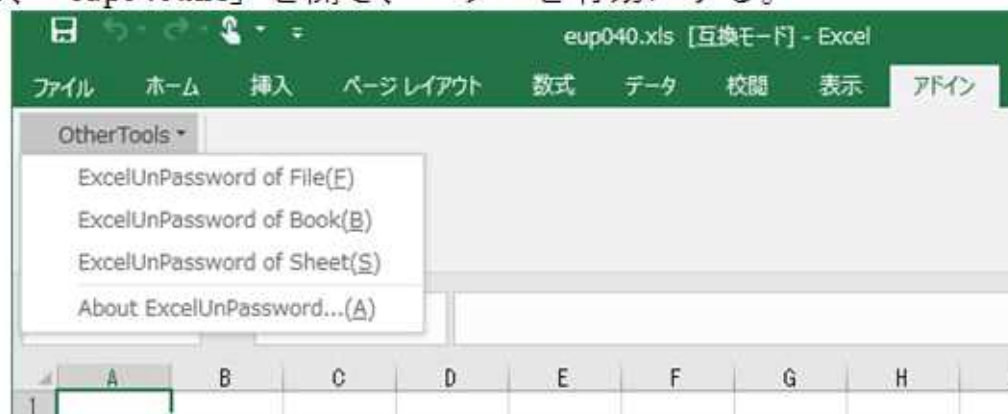
⑦ 下記のファイルを自分のPCのデスクトップにコピー

R:¥18 村山¥3 年_情報セキュリティ¥4 月 2 3 日¥4 限目実習¥eup040.xls

⑧ コピーしたファイルのうち、「eup040.xls」を開き、マクロを有効にする。

⑨ 右図のとおり操作

以降の操作は裏面を参照



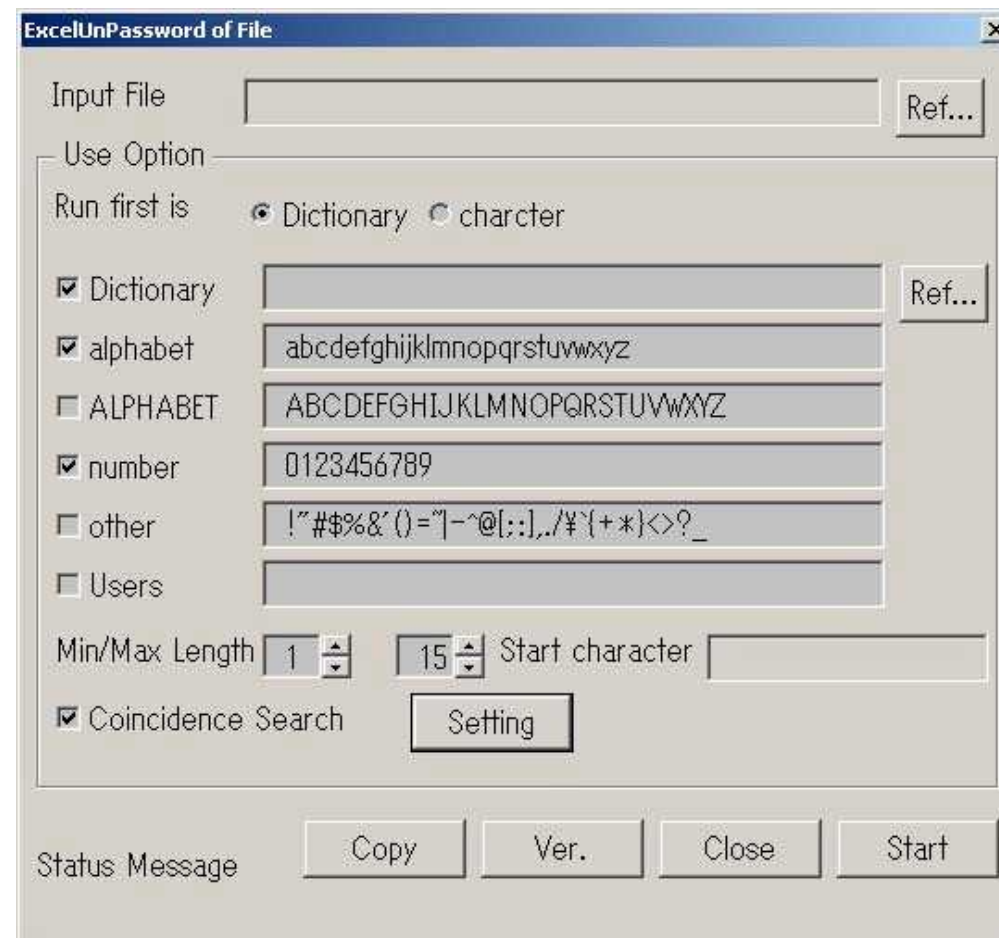
⑩ パスワードを解析するのにかかった時間を下記に記入する。

授業実践

(3) 情報セキュリティ対策

ア 人的セキュリティ対策

『「脅威」と「脆弱性」パスワード解析』





授業実践

(3) 情報セキュリティ対策

ア 人的セキュリティ対策

『標的型攻撃メール』

 murayama.yo@mxs.mie-c.ed.jp | murayama.yo@mxs.mie-c.ed.jp 2018/10
murayama.yo@mxs.mie-c.ed.jp was hacked
 このメッセージから余分な改行を削除しました。

Hello murayama.yo@

My nickname in darknet is bernhard10.

I'll begin by saying that I hacked this mailbox (please look on 'from' in your header) more than six months ago, through it I infected your operating system with a virus (trojan) created by me and have been monitoring you for a long time.

Even if you changed the password after that - it does not matter, my virus intercepted all the caching data on your computer and automatically saved access for me.

I have access to all your accounts, social networks, email, browsing history.
Accordingly, I have the data of all your contacts, files from your computer, photos and videos.

I was most struck by the intimate content sites that you occasionally visit.
You have a very wild imagination, I tell you!

授業実践

(3) 情報セキュリティ対策

ア 人的セキュリティ対策

『標的型攻撃メール』

イ メールはどこから来たのか

実習 2] メールのヘッダを確認して、送信元のIPアドレスを確認。

電子メールのヘッダには、さまざまな情報が含まれている。

- 1 : Received: from mail.mrac.jp (mail [123.45.67.89]) by mrac.jp (8.12.7/8.12.7) with ESMTP id HWM1Wwnc020178 for <goro@mrac.jp>; Wed, 24 Oct 2012 10:32:58 +0900 (JST)
- 2 : Received: from mail.flo.jp (ms [87.66.43.21]) by mail.mrac.jp (8.11.6p2/3.7W-hub) with ESMTP id HWM1Wwnc01617 for <goro@mrac.jp>; Wed, 24 Oct 2012 10:32:58 +0900 (JST)
- 3 : Date: Wed, 24 Oct 2012 10:23:10 +0900 ←受信日時
- 4 : From: "Harako" <harako@f10.or.jp> ←送信者 (メールアドレス)
- 5 : Reply-To: allmember@f10.or.jp ←受信者のメールアドレス
- 6 : Subject: 会議のお知らせ ←件名
- 7 : To: "太郎さん" <goro@mrac.jp> ←受信者 (メールアドレス)
- 8 : Cc: "子-ア" <chie@f10.or.jp> ←CC (Distribution List) のみで表
- 9 : Message-Id: <001b01c96836d132b301c9703a10@new.furumaww.or.jp> ←メッセージID (メッセージIDを照会すると元のメール)

上の例の1-2は、メッセージ送信に利用したサーバ名とその日時を示している。経由したサーバ1つに対し、1つのReceived行が記される。経由したサーバが増えれば、Receivedの数も増える。下から上が増えていくため、経由したサーバの経路には、Receivedフィールドを下から上に参照する。

	怪しいメール1	怪しいメール2	怪しいメール3
IPアドレス			

実習 3] 確認した送信元IPアドレスをWHOISを使ってどこから来たか調べる。

	怪しいメール1	怪しいメール2	怪しいメール3
国名			

授業実践

(3) 情報セキュリティ対策

ア 人的セキュリティ対策

『ひろげよう情報モラル・セキュリティコンクールへの応募』

ひろげよう情報モラル・セキュリティコンクール

ホーム お問い合わせ **IPA**

コンクールについて 募集要項 受賞作品 情報セキュリティ美術館 コンクール制作のヒント

第15回 IPA 「ひろげよう情報モラル・セキュリティコンクール」2019

作品募集中!!

募集期間 ▶ 2019年 7月1日 月 ~ 9月13日 金 必着

今年もみんなの力作をいっぱい募集します!!

2018年の受賞作品

標語部門 最優秀賞

つぶやきが
自分をおいて
一人旅

郷司 篤希 さん
大阪府 桃山学院高等学校 2年

ポスター部門 最優秀賞

咲くはるなさん

鹿児島県立川内商工高等学校 3年

4コマ漫画部門 最優秀賞

阿部 遥香 さん
東京都 筑波大学付属中学校 1年

授業実践

(3) 情報セキュリティ対策

イ 技術的セキュリティ対策

『利用者認証(生体認証)』

実習 手のひら静脈の認証装置を用いて、静脈パターンの登録と認証を行う。

①向かって右側が6組、左側が7組の実習用PCです。

②先生の指示に従って出席番号順に静脈パターンの登録を行ってください。

なお、登録は連続して3回行います。

③各クラスごとに、自分以外のユーザ名でログイン出来ないか試す。

もしログイン出来たら先生に報告すること。

④自分のユーザ名でログインする。

授業実践

(3) 情報セキュリティ対策

イ 技術的セキュリティ対策

『利用者認証(生体認証)』



授業実践

(3) 情報セキュリティ対策

イ 技術的セキュリティ対策

『暗号技術』

ア 共通鍵暗号方式

共通鍵暗号方式では、暗号文にする暗号化鍵と、元に戻す復号鍵は(同一)のものを使用する。通信相手ごとに(別々の)共通鍵が必要であるが処理は(高速)である。

実習 1 共通鍵暗号の一種である「バーナム暗号」で暗号化と復号を行う。

バーナム暗号…ビット列に変換した平文と鍵の排他的論理和を暗号文とする。

例 平文 = B₍₁₆₎
鍵 = C₍₁₆₎

①	ビット列に変換して XOR				
暗	平文	1	0	1	1
号	鍵	1	1	0	0
化	暗号文	0	1	1	1

暗号文 = (7)₍₁₆₎

②	暗号文	0	1	1	1
復	鍵	1	1	0	0
号	平文	1	0	1	1

授業実践

(3) 情報セキュリティ対策

イ 技術的セキュリティ対策

『暗号技術』

RSA暗号(受信者)

[役割選択に戻る](#)

鍵作成

素数 p 隠す
 素数 q 隠す
 公開鍵 e

 公開鍵 n
 公開鍵 e
 秘密鍵 d 隠す

p, q, e はそれぞれ異なる数。
 鍵を生成したら、送信者に n と e を伝えてください。

復号

公開鍵 n
 秘密鍵 d 隠す
 暗号文

 暗号文の数値化
 数値の復号
 平文

送信者から受け取った暗号文を入力して復号してください。

授業実践

(3) 情報セキュリティ対策

イ 技術的セキュリティ対策

『暗号技術』

RSA暗号(送信者)

[役割選択に戻る](#)

暗号化

公開鍵 n	<input type="text"/>
公開鍵 e	<input type="text"/>
平文	<input type="text"/> <input type="checkbox"/> 隠す
<input type="button" value="暗号化"/>	<input type="button" value="クリア"/>
平文の数値化	<input type="text"/>
数値の暗号化	<input type="text"/>
暗号文	<input type="text"/>

受信者から教えられた n と e を入力して、平文を暗号化してください。
平文は英大文字で5文字以下。

授業実践

(3) 情報セキュリティ対策

イ 技術的セキュリティ対策

『暗号技術』



授業実践

(3) 情報セキュリティ対策

イ 技術的セキュリティ対策

『暗号技術』

暗号解読実習

- ① 右隣の人から暗号文と暗号化に使った公開鍵 n 、公開鍵 e を聞く。

公開鍵 n	
公開鍵 e	
暗号文	

- ② R:¥18 村山¥3 年_情報セキュリティ¥9 月 3 日¥01_リンク 内にある「素因数分解 - 高精度計算サイト」のショートカットを開く。

<https://keisan.casio.jp/exec/system/1161228771>

- ③ 「整数」テキストボックスに、公開鍵 n を入力し、**計算** ボタンをクリック。
あとはどうすれば暗号文が解読できるか自分で考えてみよう。

考察 実際に使われている RSA 暗号はなぜ解読されないのでしょうか。

授業実践

(3) 情報セキュリティ対策

イ 技術的セキュリティ対策

『暗号技術』

 素因数分解

ホーム / 数学公式集 / 方程式

指定した整数を素因数に分解します。

Prime factorization
ex. $360 = 2 \times 2 \times 2 \times 3 \times 3 \times 5$
 $= 2^3 \times 3^2 \times 5^1$

整数

素因数
2
2
2
3
3
5

授業実践

(3) 情報セキュリティ対策

イ 技術的セキュリティ対策

『マルウェア・不正プログラム』

各製品共通テストウイルス

テストウイルス EICAR

このファイルはThe EICAR(European Institute of Computer Anti-virus Research)の [Webサイト](#)にて公開されているワクチンソフトの動作テスト用のファイルです。

このファイルはワクチンソフトにて“EICAR-TEST-FILE”としてあたかもウイルスのように検出されますが、あくまでワクチンソフトの検出用のテストファイルであり、ウイルスではありません。

このファイルは“駆除”しようとしても“失敗”しますが、ファイル自体は無害であり、感染・潜伏・発病といった動作は行いませんのでご安心ください。

当ファイルはユーザーの責任の元でダウンロードしてお使いください。
このファイルによって発生した一切の損害に関しては当社は責任を負いかねます。

[他のバージョンを見る](#)

その他

オペレーティングシステム: **Any Platform**

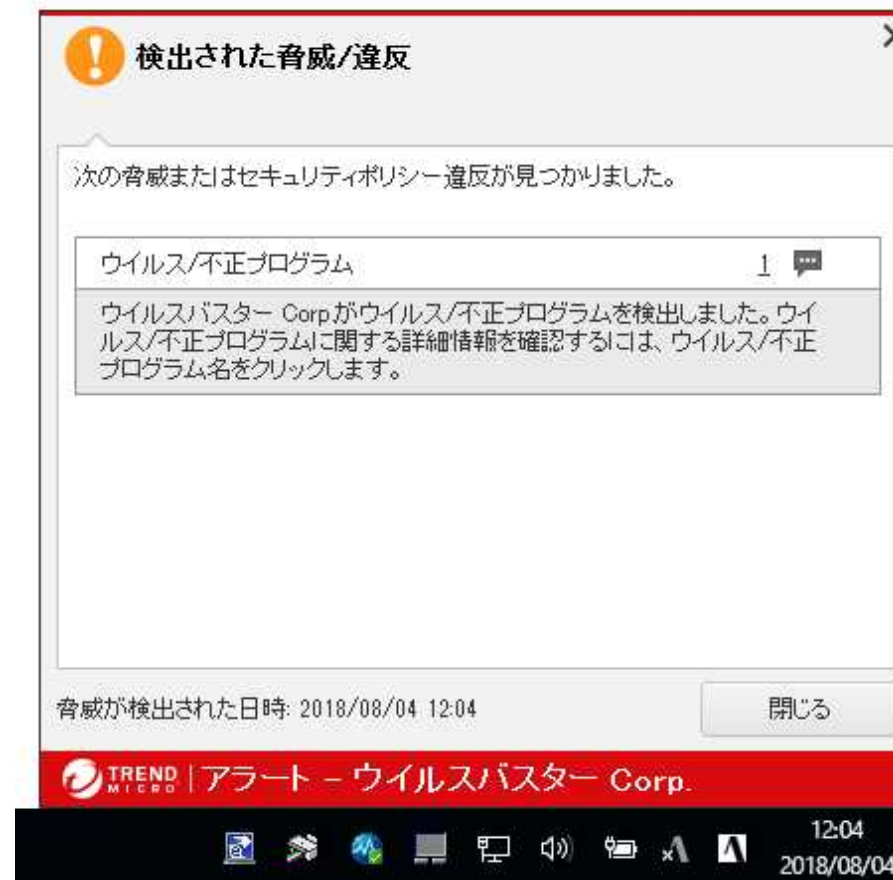
ダウンロード内容	リリース日付	ファイル名	サイズ (MB)
ツール/ユーティリティ English	0000-00-00	eicar.com	0

授業実践

(3) 情報セキュリティ対策

イ 技術的セキュリティ対策

『マルウェア・不正プログラム』



授業実践

(3) 情報セキュリティ対策

イ 技術的セキュリティ対策

『クロスサイトスクリプティング』 他

脆弱性体験学習ツール AppGoat

最終更新日：2017年11月30日

■お知らせ(更新日時：2017/11/30)

AppGoat V3.0を活用し、高校や大学での講義、組織の新人教育等で効果的な集合教育を効率良く実施する上で必要な段取りや注意点をまとめた、「脆弱性体験学習ツール「AppGoat」を用いた集合教育実施の手引き」を公開しました。

また、AppGoatを用いて集合教育を実施する際、講師側で補助資料を用意することで学習者の理解を助けることができます。その補助資料のサンプルとして3種類の脆弱性解説資料をあわせて公開しました。

詳細は下記URLの「資料のダウンロード」からご参照ください。

<https://www.ipa.go.jp/security/vuln/appgoat/classroom.html#download>

[トップ](#) | [個人学習向けツール概要](#) | [集合学習向けツール概要](#) | [FAQ](#) |



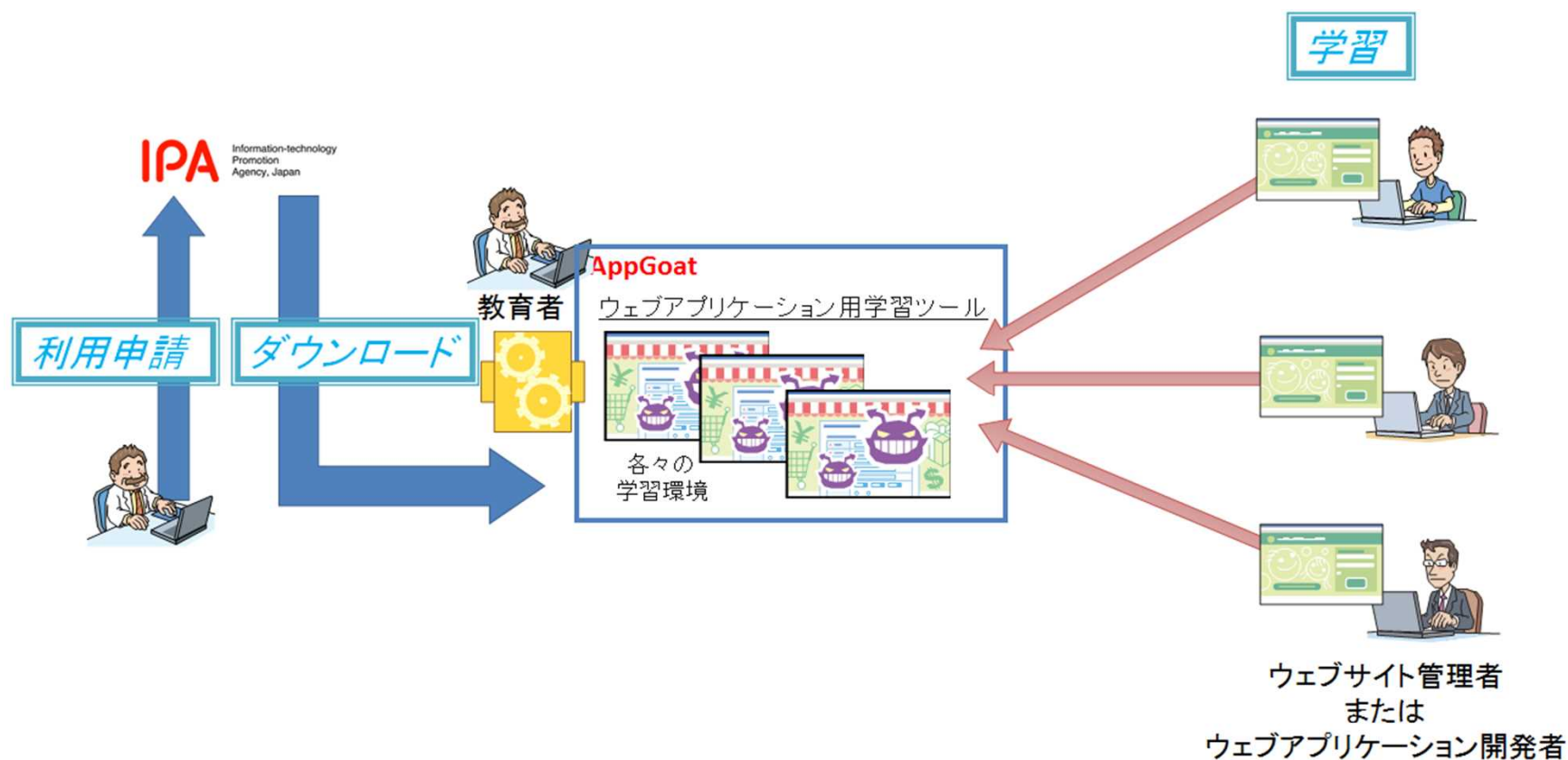
<https://www.ipa.go.jp/security/vuln/appgoat/index.html>

授業実践

(3) 情報セキュリティ対策

イ 技術的セキュリティ対策

『クロスサイトスクリプティング』他



<https://www.ipa.go.jp/security/vuln/appgoat/classroom.html>

授業実践

(3) 情報セキュリティ対策

イ 技術的セキュリティ対策

『クロスサイトスクリプティング』他

(様式)

誓約書

私は、この度、貴校が「脆弱性体験学習ツール AppGoat」を用いて実施する授業を受講者の一人として受講するに当たり、教師等から受ける注意事項等を誠実に遵守するとともに、下記各項を誓約します。

記




1. 上記授業において上記学習ツール AppGoat (以下「AppGoat」といいます)を利用する場合、教師から明示的に使用の許可を受けた機能及び情報、又は AppGoat が明示的に受講者に提示する機能及び情報のみを使用することとし、その他の機能等については、それらを探索せず、また、何らかの事情でそれらを知り得たとしても、それらを決して使用せず、また他の受講者を含めて決して他人に開示・漏洩しません。
2. 上記授業における AppGoat の利用によって知り得た他の受講者や貴校に関する情報は、上記授業の実施目標実現のための、かつ当該授業の現場限りにおける利用のみに限ることとし、決して他の目的に利用せず、また他人に開示・漏洩しません。
3. AppGoat の利用によって学んだ知識や情報は、上記授業の終了後であっても、私の正当な業務の遂行のためにのみ利用することとし、その他の目的への利用(正当な業務以外で、他人のコンピュータシステムに侵入したり、同システム内で情報を閲覧・書き換え・消去・外部送信等したり、ウイルスへの感染その他その正常な動作に支障を生ぜしめたり、又はそれらを試みる行為を含みます)は決して行いません。

授業実践


(3) 情報セキュリティ対策

イ 技術的セキュリティ対策

『クロスサイトスクリプティング』他

[手順1]   

入力フィールドに様々な値を入力する



演習の手順

HTMLタグを入力して、脆弱な箇所を発見してみましょう

- 掲示板の複数の入力欄に「`>"><hr>」を入れて、水平の罫線が引かれているところを探しましょう。


ウェブブラウザ上の表示

```
13 `>"><hr>title : `>"><hr>name 2013年07月05日 17:22 削除
`>">
comment
```

- 「本文」を入力する箇所で、入力した値がそのまま使われていることが確認できます。

HTMLソース

```
<div class="comment">
```



Copyright © 2017 独立行政法人情報処理推進機構

15

授業実践

(3) 情報セキュリティ対策

イ 技術的セキュリティ対策

『クロスサイトスクリプティング』 他

The screenshot shows a web browser window displaying a training page for Cross-Site Scripting (XSS). The browser address bar shows the URL: `http://localhost/main.php?scenario=Scenario1111&stage=stage4`. The page title is "脆弱性の概要および発見演習".

Left Navigation Menu:

- テーマ一覧
- 表示中のページ
 - 基礎
 - クロスサイト・スクリプティング
 - Level1
 - 脆弱性の概要および発見演習
- 基礎
 - クロスサイト・スクリプティング
 - イントロダクション
 - クロスサイト・スクリプティングとは
 - Level1
 - 脆弱性の概要および発見演習
 - Level2
 - アンケートページの改ざん(反射型)
 - 入力情報の漏えい(反射型)
 - 提示欄に埋め込まれるスクリプト(格納型)
 - ウェブページの改ざん(DOMベース)
 - Level3
 - 不完全な対策
 - ヘッダ要素へのスクリプト
 - 習熟度テスト
 - テスト問題 全問
 - +SQLインジェクション
 - +CSRF(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

Main Content Area:

脆弱性の概要および発見演習

← 戻る 次へ →

→ テーマ概要説明 → 原理解説 → 脆弱性の発見手法 → **演習(発見)** → 影響解説 → 動作確認

演習(発見)

チャレンジ

【脆弱登録画面】にはクロスサイト・スクリプティングの脆弱性があり、スクリプトを送信すると確認画面で実行してしまいます。クロスサイト・スクリプティングの検査方法を用いて脆弱性を発見してみましょう。

検査

次の手順にしたがって、検査を進めていきましょう。

- ❶ 名前に「0x×h×h」と入力します。
- ❷ 住所と性別に値を入れて登録ボタンを押します。

次のページでは脆弱性の影響を見ていきます。

脆弱登録画面 最初のページに戻る

URL: `http://localhost/Users/sec01/Web/Scenario1111/VulSoft/form.php` GO

名前:

住所:

性別: 男 女

登録

授業実践

(3) 情報セキュリティ対策

イ 技術的セキュリティ対策

『クロスサイトスクリプティング』 他

検査

次の手順にしたがって、検査を進めていきましょう。

- ① 名前に「><hr>」と入力します。
- ② 住所と性別に値を入れて登録ボタンを押します。

次のページでは脆弱性の影響を見ていきます。

脆弱登録画面

最初のページに戻る

URL

名前

住所

性別 男 女

授業実践

(3) 情報セキュリティ対策

イ 技術的セキュリティ対策

『クロスサイトスクリプティング』 他



URL

Congratulations!!演習の目標を達成しました。

登録内容

名前	'>">
住所	a
性別	男

授業実践

(3) 情報セキュリティ対策

イ 技術的セキュリティ対策

『SQLインジェクション』

SQL Editor(匿名ユーザ) ログアウト

接続しているデータベース：なし

履歴表示 履歴削除

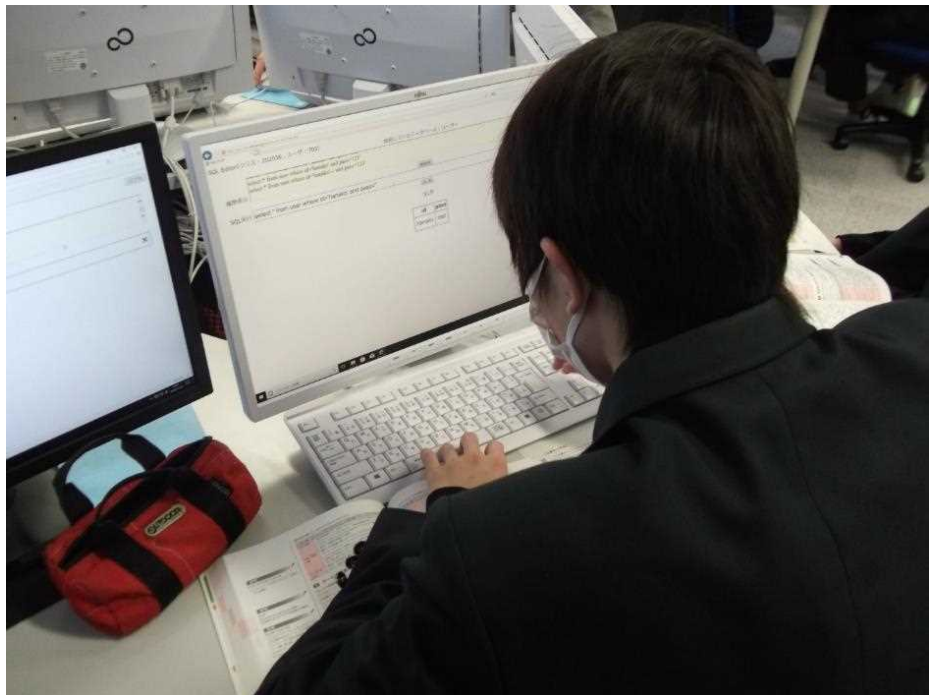
SQL実行 送信

授業実践

(3) 情報セキュリティ対策

イ 技術的セキュリティ対策

『SQLインジェクション』



授業実践

(3) 情報セキュリティ対策

イ 物理的セキュリティ対策

『トラッシング・窃視』

※授業以外では決して行わないように

《実習1 トラッシングは可能なのか》

[各班に配られる用紙の原型]

亀山高等学校
△△△△△△

先のように学校名とパスワードが書かれた紙
△には英小文字か数字が入る

実際に解読してみよう

① びりびりに手で破かれたもの

② シュレッダーに横で入れられたもの

③ シュレッダーに縦で入れられたもの

④ ほかのゴミと混ぜてびりびりに手で破かれたもの

授業実践

(3) 情報セキュリティ対策

イ 物理的セキュリティ対策

『トラッキング・窃視』



授業実践

(3) 情報セキュリティ対策

イ 物理的セキュリティ対策

『トラッキング・窃視』

《実習2 ショルダーハッキングは可能なのか》

各グループ交代で、入力する人が入力するキーだけをみて疑似パスワードを盗む。

[注意] 実際に使用しているパスワードを使わないこと。

- ①パスワードを入力する人がキーボードの前に座る。
- ②パスワードを盗む人は入力する人の視界に入らないところから盗む。
入力する人は視界に入る人がいたら見えることを伝える。
- ③実際に入力する。盗む人はいったんすべての桁を覚えてからメモをとる。
- ④入力した人は答え合わせをする。

①数字のみ4桁

②数字のみ6桁

③数字のみ8桁

④英小文字のみ4桁

⑤英小文字のみ6桁

⑥英大小文字混ぜて4桁

授業実践

(3) 情報セキュリティ対策

イ 物理的セキュリティ対策

『トラッキング・窃視』



授業実践

(3) 情報セキュリティマネジメント

『リスク管理』

机上演習

前提…皆さんはCSIRTの一員です。日頃から自社で起こるセキュリティインシデントへの対応や、リスク軽減のための活動を行っています。

ある日、3つのインシデントがほぼ同時に発生したとの連絡を受けました。今のところ表面上のことしか分からず、全体像ははっきりとしません。

それでも対応策の案を作って会社役員の承諾を得なければいけません。役員が納得する状況説明とその対応策を支給考えることができるでしょうか。

授業実践

(3) 情報セキュリティマネジメント

『リスク管理』



授業実践

(3) 情報セキュリティマネジメント 『リスク管理』



最後に

- 生徒は情報セキュリティに関する関心・意欲が高く、実習内容にも意欲的に取り組んでいた。
- 授業の実施に向けて実習内容を考えて準備するには多くの時間が必要であった。
 - －実習内容の共有が必要。
- 生徒が授業で情報セキュリティに関する知識を得ると同時に、その悪用を防ぐためにモラル面での指導について必要性を感じている。
- 評価に関する研究も進めていきたい。