公立はこだて未来大学 2022 年度 システム情報科学実習
グループ報告書

Future University Hakodate 2022 Systems Information Science Practice

Group Report

プロジェクト名

暗号とセキュリティ

Project Name

Cryptography and Secutity

グループ名

Web 班

Group Name

Web Team

プロジェクト番号/Project No.

18-B

プロジェクトリーダ/Project Leader

中村碧　Aoi Nakamura

グループリーダ/Group Leader

白井一樹　Kazuki Shirai

グループメンバ/Group Member

斉藤波平　Namihei Saitou

指導教員

白勢政明　由良文孝

Advisor

Masaaki Shirase　Fumitaka Yura

提出日

2023 年 1 月 18 日

Date of Submission

January 18, 2023

概要

本プロジェクトではセキュリティに関する知識を深め実際に体験することを目標としたプロジェクトである. 近年の IT 化に伴い増加しているサイバー犯罪や詐欺などの対策のためには対策や手口を知ることが必要である. また, コロナ禍によって急速に普及したテレワークも後押しして, 被害が増大している. そこで IPA の情報セキュリティ 10 大脅威 2022[1] などを参考にしながらサイバー犯罪や詐欺に関しての知識を習得し, セキュリティ意識向上させことを本プロジェクトの最終目標とする.

キーワード　セキュリティ, ネット詐欺, Web アプリケーション, セキュリティ意識

（※文責: 白井一樹）

Abstract

The goal of this project is to deepen knowledge of security and provide hands-on experience. It is necessary to know the countermeasures and modus operandi to prevent cyber crimes and frauds, which have been increasing with the recent shift to IT. In addition, teleworking, which has spread rapidly due to the Corona disaster, has also encouraged an increase in the number of victims. Therefore, the ultimate goal of this project is to acquire knowledge about cyber crimes and frauds and improve security awareness by referring to IPA's 10 Major Threats to Information Security 2022 [1].

Keyword security, Internet fraud, web application, Security awareness

（※文責: 白井一樹）

目次

第 1 章　はじめに

1.1　前年度の成果

近年,IT 化が進み多くの個人や組織の情報をインターネット上で扱うようになるに伴ってサイバー犯罪も増加している. また, コロナ禍によってテレワークも増え, テレワークを狙ったサイバー攻撃も増えた. それらの増大した脅威から身を守るためには正しい知識を身に着ける必要がある. そのため, サイバー攻撃に対する知識や対策, 意識の向上を図るべきだと考えセキュリティ意識を向上させる Web サイトを作成することにした. 昨年は様々なサイバー犯罪の紹介, フィッシング詐欺の疑似体験を行っている. また, 質問に答えることで回答者に向いているセキュリティソフトを紹介するページも存在している.

（※文責: 白井一樹）

1.2　前期の課題設定

前期の課題は昨年の成果物について利点や改善点について話し合いより分かりやすく気軽に学んでもらえるようなサイトを作るために Web プログラミングについて学習し, クイズページのレイアウトやセキュリティについての情報の収集, 問題作成,javascript での正誤判定の作成, 誤答した場合に解説を表示する機能の作成などを行った. 昨年のウェブページではサイバー攻撃の紹介をしているものの具体的な対策や, 予防についての記述が少なかったこと, 文字ばかりで記憶に定着しにくいという意見がでたため今年のページでは予防対応策を中心に問題を出題し, 昨年の成果物と併せることでさらなる知識の定着を図ることにした.

（※文責: 白井一樹）

1.3　後期の課題設定

後期の課題は, 現在室蘭工業大学等でも感染が確認されており被害が拡大しているランサムウェアの疑似体験をすることに決定した. ランサムウェアはファイルを暗号化し、身代金を請求するマルウェアである. コロナ禍におけるリモートワークの増加に伴い年々被害件数が増加しており, 他大学でも学生の被害が報告されているため, 知識を身につけることは必須であると考えた. ランサムウェア体験をするといっても実際にパーソナルコンピューターに被害を与えることはできないのでウェブページ上で HTML,CSS,JavaScript で演出をすることにした. また, クイズページのデザインの改善, イメージを助けるイラストの追加を行った. また, 外部評価のためのアンケートを実装した.

（※文責: 白井一樹）

第 2 章　到達目標

2.1　本プロジェクトにおける目的

近年, 高まっているサイバー犯罪の脅威から未来大生を守るためにセキュリティ意識を向上させることが課題である. 昨年度の成果物の分析を用いてクイズやサイバー攻撃の疑似体験が出来る Web ページを企画・作成し,Web ページを通じて未来大生のセキュリティ意識向上を試みる. また,IPA(情報処理推進機構) が毎年公開している情報セキュリティ 10 大脅威に対しての対策知識を身に付ける.

（※文責: 斉藤波平）

2.1.1　通常の授業ではなく, プロジェクト学習で行う利点

本課題では Web ページ作成時に, レイアウト（css）, アルゴリズム（javascript）, 実装するプログラミング（html）を複数人で役割分担することにより, 作業効率を大幅に上げることが出来る. また,Web ページ作成時にグループでアイデアを出し合うことで創作的に行うことが出来る. 通常の授業では, 教授が多数の生徒に対して同じ内容の知識・技術を身に付ける講義・演習が行われるため, 各々の個性を発揮し創作性があるモノをうみだすことに向かない.

（※文責: 斉藤波平）

2.1.2　地域との関連性

Web ページを公開することで公立はこだて未来大学の学生に限らず地域の人々のセキュリティ意識向上につながる可能性がある. また, セキュリティ意識向上からサイバー犯罪に対する被害の抑制に効果的である. また, 中小企業のセキュリティ意識が低い傾向がある [2] ので改善が期待される.

（※文責: 斉藤波平）

2.2　具体的な手順・課題設定

2.2.1　クイズページ

セキュリティ意識の向上を目指した Web サイトを作りのために昨年度の成果物を分析し, 改善された Web ページを企画し,Web アプリケーションとサイトを製作するための Web プログラミングの学習を行い,Web サイト内に載せる情報を収集と実装をしたのちに Web ページを公開して未来大生のセキュリティ意識向上を課題とした.

1. 前年度の成果物を分析
   課題：前年度の Web ページを分析し, 良い点や改善点を挙げる.

2. サイバー攻撃の疑似体験とクイズページ作成決定
   課題：昨年度のフィッシング詐欺を疑似体験できる Web サイトを参考に別のサイバー攻撃の疑似体験が出来る Web ページ作成を企画する. 昨年度のクイズページの反省点を活かしたクイズページを企画する.
3. 現在のサイバー犯罪の脅威やそれらの対策・予防策を調査
   課題：それぞれの脅威から具体的なな被害や対策・予防策を調べる.
4. クイズ用 Web ページの大枠を作成
   サイトの目的, なぜセキュリティについて学ばなければならないのかを作成する.
   課題：HTML/CSS でクイズの問題文や選択肢, 解説を表示するプログラムを作成する.
5. クイズを実装するための関数を作成
   課題：JavaScript で正解不正解の判定を行う関数を作成する. 未回答の場合, 警告を出し正解不正解の判定を中断し解答しなおすプログラムの作成をする.
6. クイズの問題作成
   課題：IPA が公開している情報セキュリティ 10 大脅威から得た情報をもとに四択クイズを作成する.
7. クイズの解説作成（代表的なセキュリティ問題をピックアップし 6-7 の繰り返し）
   課題：不正解者に対して解説を簡潔にまとめて書く. 正解以外の間違いの選択肢に対しても根拠を説明する.
8. Web ページをローカルサーバーから公開サーバに移行
   課題：外部の端末から Web ページにアクセス可能にする

（※文責: 斉藤波平）

2.2.2 サイバー攻撃疑似体験ページ

サイバー攻撃の疑似体験をしてもらうことでサイバー攻撃の脅威と対策方法を身に着けることができ, セキュリティ意識の向上に繋がると考える.

1. 前年度の成果物を分析
   課題：前年度の Web ページを分析し, 良い点や改善点を挙げる.
2. サイバー攻撃の疑似体験とクイズページ作成決定
   課題：昨年度のフィッシング詐欺を疑似体験できる Web サイトを参考に別のサイバー攻撃の疑似体験が出来る Web ページ作成を企画する. 昨年度のクイズページの反省点を活かしたクイズページを企画する.
3. 近年, 勢力を増している攻撃を調べ, 警察庁のデータより疑似体験のテーマをランサムウェアに設定
   ランサムウェアの特徴, 被害の大きさをわかりやすく伝える.
4. ランサムウェアの特徴を調べ, 疑似体験のシナリオと攻撃の方法を設定する.
   疑似体験での実装方法について考える.
5. ランサムウェアの説明をしたウェブサイトを作成する. 事前に知識を身に着けた状態で体験をすることで確かな知識の定着を目指す.
   概要を説明するが, この後の疑似体験のネタバレにならないようにする.
6. 疑似体験シナリオのウェブページを作成する. 今回のシナリオでは攻撃を受け改ざんされラ

ンサムウェアを仕込まれた広告が表示されたサイトにアクセスしてしまいドライブバイダウンロード攻撃を受けてしまった. という設定である.
ページのデザイン, 構成, 内容を考える.

7. 疑似体験終了後の説明ページを作る
   ランサムウェアの対策について調べる.
8. GitHub に移行, 実装する
   GitHub 用に調整をする.

（※文責: 白井一樹）

第 3 章　課題解決のプロセスの概要

3.1　プロジェクト内の課題の位置づけ

近年,IT 化が進み多くの個人や組織の情報をインターネット上で扱うようになった. その結果, 個人や組織の情報を盗む犯罪も増加した. これらの手口は昔からあるものから新たに生み出された巧妙なものまで様々だ. これらの犯罪に巻き込まれないための対策や被害を最小限にするための正しい対応を 身に付けるためにセキュリティについて学ぶ必要がある. そして, 日々開発される新たな手口のサイバー攻撃やインターネットを利用した詐欺から身を守るために定期的に自身のセキュリティ知識をアップデートする必要がある. そのためにはセキュリティ意識を常に高く維持する必要がある. そこで,Web サイトを作成し, セキュリティに関する知識をゲーム感覚で提供することでセキュリティに意識を向けるきっかけとなるサイトを作成しセキュリティに関する知識を広めることを課題とした.

（※文責: 白井一樹）

3.1.1　身に着けるべきセキュリティに関する知識

実際に身に着けるべき知識の参考として IPA の情報セキュリティ 10 大脅威 [1] を参考に事例の多い被害について知識を身に着けることで実際に活かせる可能性が高くなると考えたため, それらの被害に関する知識をテーマにすることにした.

（※文責: 白井一樹）

3.1.2　コロナ禍による被害拡大

コロナ禍によってリモートワークが急速に発達したがそこを狙ったサイバー攻撃が急増している. また,Emotet を初めとしたランサムウェアも勢力を増している. 特に Emotet などのランサムウェアは室蘭工業大学 [3] や京都大学大学院 [4] などでも感染が確認されていることから, 未来大生も狙われる可能性がある. このことからランサムウェアをテーマとしたサイトを作成することにした.

（※文責: 白井一樹）

3.2　課題解決の方法

3.2.1　身に着けるべきセキュリティに関する知識

インターネット上の犯罪に巻き込まれないためのセキュリティ知識を身に付けるためにクイズ形式で不足しているセキュリティ知識を補うことが出来る Web ページを作成した.

（※文責: 斉藤波平）

3.2.2 コロナ禍による被害拡大

ランサムウェアの感染事例を調査し, 事例を参考にランサムウェア感染の疑似体験する Web サイトを作成した. また, 体験した内容の詳しい解説の他にそれ以外のランサムウェアの感染方法や対策方法などを細かく解説する Web ページを作成した.

（※文責: 斉藤波平）

3.2.3 クイズページ

- 昨年度の成果物の分析
  解決過程: 昨年度の成果物をプロジェクトメンバー全員で閲覧した. その後, 良い点や改善点を挙げて今年度に実現できる案を厳選した.
- クイズページの企画
  解決過程: 昨年度の成果物の分析結果をもとに Web サイトの構成や内容を決定した. 去年の成果物の違いとしてサイバー犯罪に対する具体的な対策・予防策に焦点をあてて Web ページを企画した.
- 現在のサイバー犯罪の脅威やそれらの対策・予防策を調査
  解決過程:IPA が公開している情報セキュリティ 10 大脅威 2022 から情報収集した. その後, クイズの問題文や解説文を作成した.
- クイズ用 Web ページの大枠を作成
  解決過程: 去年の成果物から Web ページの構成や仕組みを参考にしながら HTML でを作成した. その後,CSS で文字の配置やサイト全体の色などのデザインを作成した.
- クイズを実装するための関数を作成
  解決過程:JavaScript で 1 つ 1 つの機能を正確に追加しながら作成した. 具体的に, クイズの正誤判定をする機能や未回答か判定する機能や解説を表示する機能などを順番に追加して完成させた.
- クイズの問題作成
  解決過程: 実践的なサイバー犯罪の予防策・対応策を学んでもらうため過去に被害があったサイバー犯罪の事例を参考に問題を作成した.
- クイズの解説作成
  解決過程: 選択肢が正解か不正解かを示す根拠を示してから解説を作成した. また, 昨年度の成果物に対する分析結果の反省点から難しい専門用語はなるべく使わない（使う場合は補足説明を行う）ようにした.
- Web ページをローカルサーバーから公開サーバに移行
  解決過程:github で公開サーバーに HTML/CSS,JavaScript ファイルをアップロードした. その後, ローカルサーバーから公開サーバーに移行したことで発生したエラーの解消を行った.

（※文責: 斉藤波平）

3.2.4 疑似体験ページ

- 疑似体験ページの企画
  解決過程: 現在大学生にも影響が出ているランサムウェアをテーマとすることで体験者に危機感を抱かせることができると考えた.
- ランサムウェアの調査
  IPA が公開している情報セキュリティ 10 大脅威 2022[1] や警察庁 [5] , トレンドマイクロ社 [6] などから情報収集を行った. その結果被害件数がコロナ禍以降増大していることを確認した.
- ランサムウェアのシナリオ, 攻撃手法の設定
  ランサムウェアの攻撃手法には大きく分けてメールの添付ファイルから攻撃する方法と脆弱性のあるウェブサイトや広告から感染する方法の 2 パターンがあるが, 今回はウェブサイトでの疑似体験ということと,html,css,javascript のみだということを考慮して後者を選択した. それに伴い, シナリオを「攻撃を受けランサムウェアに感染させる可能性のある広告を表示しているウェブサイトに訪れたところランサムウェアに感染した.」というものに決定した.
- シナリオに沿ったデザイン, ウェブページの作成
  決定したシナリオに沿ったウェブページを制作した. その際体験者の理解度を高めるために, 事前にランサムウェアの概要について説明をしこれから体験することは実際には体験者のパーソナルコンピューターに被害を与えないことを説明する. その後, 検索エンジンを模したウェブページから脆弱性のあるウェブページに訪れることができる.
- スクリプト作成
  脆弱性のあるウェブページからウイルスに感染した旨を伝える脅迫画面に強制的に遷移し, 前のページに戻れなくなるスクリプトを作成した.

（※文責: 白井一樹）

3.2.5 アンケート

アンケートを実施することでこの活動の外部評価を得ることができ, さらなる改善が期待できる.

1. セキュリティ意識の変化
   この体験を通じてセキュリティに対する意識に変化があったかを 5 段階で調査する. その後, ユーザのセキュリティにとって大事なセキュリティソフトの導入について, すでに導入しているか. これから導入しようと思うか, を質問する. また, 脆弱性に対応するために OS やソフトのアップデートは必須である. そのためこれから OS やソフトのアップデートを頻繁に行うか質問する. 最後にランサムウェアや, その他さまざまなサイバー攻撃の対応策を学ぶことができたかを調査し回答をもとにウェブページの改善を行う.

（※文責: 白井一樹）

第 4 章　課題解決のプロセスの詳細

4.1　各人の課題の概要とプロジェクト内における位置づけ

白井一樹の担当課題は以下のとおりである.

5 月　昨年度の成果物の分析.IPA が公開している情報セキュリティ 10 大脅威から情報収集 [1].
6 月　クイズページの作成.
7 月　中間発表スライド作成.
8 月　疑似体験ページの作成.
9 月　公開サーバへ移行.
10 月　疑似体験ページの改良.
11 月　クイズページの改良.
12 月　報告書, 発表資料作成.

（※文責: 白井一樹）

斉藤波平の担当課題は以下のとおりである.

5 月　昨年度の成果物の分析.IPA が公開している情報セキュリティ 10 大脅威から情報収集.
6 月　Web プログラミングの学習, クイズの問題作成.
7 月　ポスターの作成.
8 月 9 月　疑似体験ページの作成.
10 月　クイズページの改良.
11 月　疑似体験ページの改良.
12 月　報告書, 発表資料作成.

（※文責: 斉藤波平）

4.2　担当課題解決過程の詳細

4.2.1　白井一樹

5 月　昨年度の成果物を見ながら改善点を話し合い, その際に専門的な用語が多いことや文字が多いことからわかりにくいサイトになっているという意見が出ていたため今年は見た人にわかりやすい, セキュリティ意識の向上を図ることができるサイトを作ることを決定した. また, 去年の Web サイトを参考に html,css を習得した.
6 月　わかりやすいサイトをつくるにあたってクイズページの作成, 攻撃の疑似体験をできるサイトを作成することにした. クイズページ作成の際に javascript の技術を習得した.
7 月　中間発表の際, 発表用の原稿を作る中で限られた時間内で効果的に伝える方法を身に着けた.
9 月　疑似体験ページ作成の際に,Javascript によるタイマー機能, 静的にページを移動させる機能, 元のページに戻れなくする機能を身に着けた.

10 月　疑似体験ページ作成の際に, フレームワークの利用方法を学んだ.

11 月　GitHub でウェブページを作成する方法,GitHub で共同で作業する方法を学んだ.

（※文責: 白井一樹）

4.2.2　斉藤波平

5 月　昨年度の成果物を分析し改善点を話し合い, 改善点を考えた. その結果, 難しい専門用語が多く内容が理解しにくい事や文章量が多すぎて隅々まで目を通すのが大変であることから効率的にセキュリティ知識を知ることが出来るクイズページの企画をした. また, プログラミング言語学習サイトや去年のサイトを参考に html,css の技術を習得した.

6 月　クイズページの問題作成にあたって必要な情報を IPA が公表しているセキュリティ 10 大脅威 2022 から情報収集し, 問題と解説を作成した. また,Web ページにクイズ問題と解説を表示する機能を実装した. そこで,html で javascript の関数を実装するを方法を学んだ.

7 月　中間発表の資料作成する中で誰でも理解することが出来る文章や見やすい発表スライドのデザインを学ぶことが出来た. また, 発表練習と発表後の評価から反省点を見つけて発表技術向上につながった.

9 月　サイバー攻撃疑似体験サイトの企画と作成を協力して行うことでプロジェクトチーム内でのグループで貢献できるように協調性を身に付けた.

10 月　css を用いた Web ページ内のボタンのデザインやテキストボックスなどの強調などを実装する中で css の実践的な技術を高めた.

11 月　GitHub でウェブページを共同で作成する方法を学んだ.

12 月　成果発表の際に注意すべきことや発表スライドの作成方法を学んだ.

（※文責: 斉藤波平）

第 5 章　結果

5.1　プロジェクトの結果

未来大生のセキュリティ意識向上させるために 2 つの Web ページを制作した.1 つ目はクイズページというクイズ形式でサイバー攻撃の具体的な対策・対応方法を学ぶ Web サイトを制作した. 問題は IPA が公表している情報セキュリティ 10 大脅威 2022 から具体的なサイバー犯罪の事例を参考に作成した. サイトの内容としては, クイズが 10 問用意されており 1 問づつ解答と答え合わせを行い間違えた場合にのみ詳しい解説が表示される.2 つ目は疑似体験ページを制作した. 疑似体験ページではサイバー攻撃の脅威を知ってもらう事やこれらの脅威に対して危機感を意識してもらうためにランサムウェア感染の疑似体験が出来る Web ページを制作した. また, 体験後にランサムウェアの詳しい解説サイトに移行すると具体的な仕組みや本体験以外のランサムウェアの感染方法や対策・対応を知ることが出来る. これらの成果物はサイバー犯罪の具体的な予防・対応策を中心に学習できるので去年の成果物と合わせるとよりセキュリティ知識が深まるように制作した.

（※文責: 斉藤波平）

5.2　成果の評価

プロジェクト全体の成果として体験が終わった方にアンケートをお願いしましたが, 母数が集まらなかった. 理由として, ウェブサイトの周知方法が分かりにくかったことが挙げられる. 今回ウェブサイトの周知方法として 3 年生全体にメールを送ったが, セキュリティの観点から URL を直接載せることはせず,HOPE のプロジェクト学習のページからアクセスするようにした. だが, それが体験の敷居を上げてしまったと考えられます. 改善案として, 購買など人目のつくところにも QR コードを張らせてもらうことが挙げられる.

（※文責: 白井一樹）

5.3　担当分担課題の評価

5.3.1　白井一樹

- 疑似体験ページのテーマ決定

  疑似体験については IPA が公開している情報セキュリティ 10 大脅威 2022 より, 被害が多く報告されている攻撃について作成することにより, 実践的なページを作成することができたが攻撃の詳しい手口については技術力や倫理の問題から, 再現することができなかった.
- 疑似体験ページの作成

  疑似体験ページにおける javascript, シナリオ制作を行った.javascript を画像に埋め込む計画だったが作業日数の関係で断念した. シナリオはセキュリティに詳しくない人でも理解できるよう専門的な用語を極力減らし, シンプルな構成にした.

- クイズページの添削
  制作された問題や選択肢を精査し, 情報ソースを明記することの徹底と, わかりやすい表現にすることなどを行った.
- アンケートの作成
  制作したウェブページの外部評価を行ってもらうためのアンケートを制作した. このアンケートでは今回の体験を通じてセキュリティ意識やセキュリティに関する知識が向上したかを 10 ほどの質問によって評価する.
- 完成したページの広報
  完成したページを体験してもらうためにはどのような方法が適しているかを班員, 担当教員を交えて話し合った. 完成したリンクを直接メールに貼る行為はセキュリティの観点から好ましくないため HOPE のプロジェクト学習にある 18 暗号とセキュリティの説明欄にリンクを記載し, そのことを 3 年生全体にメールで周知した. だがこの方法だと体験に訪れる人が例年に比べて少なかったため, 購買や食堂の壁に QR コードを貼るなど, 他の方法で周知させるべきだったと考える.

（※文責: 白井一樹）

5.3.2 斉藤波平

- 昨年の成果物の分析
  昨年の成果物から良かった点や反省点をまとめることで今年の成果物のテーマ決定や Web ページの方針などを決めることが出来た. ただし, グループメンバーの人数が二人ということもあり, 全てのアイデアを生かすことが出来なかった.
- クイズページの問題作成
  IPA が公開している情報セキュリティ 10 大脅威 2022 からサイバー犯罪の事例を参考にクイズを作成したことで実践的なサイバー犯罪の予防・対策を学ぶことが出来る. しかし, クイズの難易度が極端に高いものがあり学習しにくい事や問題数が 10 問のみで少ないことで多種多様な手口のサイバー犯罪の対策を学びきることが出来ないという反省点が挙げられる.
- ポスターの作成
  中間発表に向けたポスターの作成では去年のポスターを参考に課題設定の背景や成果物について簡潔にまとめることが出来た. 反省点としては見直しなどのチェックが足りずに誤字が見られたところが挙げられる.
- 疑似体験ページの作成
  疑似体験内のスタート画面や偽検索画面の HTML/CSS を制作した. 色やテキストボックスなどで強調などして分かりやすくした. 一方で Web ページ全体のデザインが悪いとアンケート結果から指摘をされた.
- クイズページの改良
  公開サーバーに移行するために隅々までチェックを行った. 具体的に Web サイトを見やすくするために文字のフォントの修正やページ移動のボタンを追加や誤字・脱字の修正を行った. 反省点としてはデザインなどの修正は客観的な視点で評価し修正する必要があるのでプロジェクト内の他のグループに相談するなど多くの人に見せてから修正などを検討するべきだった.

- 疑似体験ページの改良
  Web ページを閲覧中にランサムウェアに感染するというストーリーだったのでより現実的な体験を演出するために検索画面が必要と考えて,google の検索画面を参考に作成した. 反省点としては次に進むためにクリックしてほしい場所への誘導が去年と比べて分かりずらくなっている事が挙げられる.

（※文責: 斉藤波平）

第 6 章　今後の課題と展望

前期の活動では IPA の「情報セキュリティ 10 大脅威　2022」を参考にクイズを作成した. クイズを用いてセキュリティの知識が不足している人に対して詳しく説明することで, 効率的なセキュリティ意識向上を目指した Web サイトを作成した. 後期からはサイバー攻撃疑似体験サイトとして現在, 被害が拡大しているランサムウェア感染の疑似体験を制作した. その後, クイズページの改善を行い github でローカルサーバーから公開サーバーに移行した後に Hope に URL を公開し未来大生がアクセスすることを可能にしたことでセキュリティ意識向上に役立たせることが出来るようにした. 今後の展開としては, 成果物を宣伝しより多くの未来大生に Web ページを利用してもらうことで未来大生全体のセキュリティ意識向上に繋がることが期待できる. また, 未来大生以外でも成果物の Web ページを公開することでセキュリティ意識向上に役立たせることが出来ると考えられる. 改善すべき点としては, アンケートの指摘より Web ページ全体のデザインが良くなかったことが挙げられた. また, セキュリティの観点から電子メールに URL を添付しアクセスすることが危険であることから Hope で公開したため学部 3 年のプロジェクト学習 2022 を登録している学生, または最終発表当日のスライド内にある QR コードからアクセスした人のみが利用できる状態であることから未来大生全体に周知することが出来ず独自で用意したアンケートに協力してもらうことが出来なかった事は改善を試みたい. 具体的にプロジェクト内の予算を使いアンケート回答者に謝礼を払うなどの工夫を行い協力をお願いすることで回答数を増やす. これらの改善によって, 多くの人に成果物である Web ページを訪れてセキュリティ意識向上に役立ててもらうことが出来る. また, アンケート結果から未来大生のセキュリティ意識の現状の調査から改善点を見つけることでさらに効果的なセキュリティ意識向上を目指した Web ページ作成に役立たせることが期待できる.

（※文責: 斉藤波平）

付録 A　新規習得技術

- html
- css
- javascript

（※文責: 斉藤波平）

付録 B　活用した講義

講義名　情報機器概論活動内容　ウェブサイト作成時,HTML の記述を活用した.

（※文責: 斉藤波平）

付録 C　相互評価

C.1　白井一樹

斉藤波平: クイズページに関してはクイズの問題作成と正誤判定のプログラミングをしてもらいました. 2 人で相互評価することでミスが減り, 新しいアイデアが生まれました. 疑似体験ページではトップページの作成とデザインの修正などをしてもらいました. 一人だと手が回らない部分をフォローしてくれたので自分はスクリプトの制作に集中することができました.

（※文責: 白井一樹）

C.2　斉藤波平

白井一樹: クイズページに関してはトップページの作成とプログラミングをしてもらいました. 作業を効率的に分担できたことでスムーズにクイズページ作成を取り組むことが出来ました. 疑似体験ページに関しては全体の構想や解説などを考えて実装してもらいました. 私は細かいデザインの修正や目次, ページ間のリンクの繋ぎなど細かい機能の追加を担当することが出来ました. また, ローカルサーバーから公開サーバーに移行する際に gidhub の仕組みや使い方などを教えてもらいながら作業できたので効率よく作業を進めることが出来ました.

（※文責: 斉藤波平）

参考文献

[1] 報セキュリティ 10 大脅威 2022
https://www.ipa.go.jp/files/000096258.pdf 2022/5/13
[2] 2021 年度 中小企業における情報セキュリティ対策に関する実態調査」報告書
https://www.ipa.go.jp/files/000097060.pdf 2022/5/20
[3] ルウェア感染が原因と思われる本学メールアドレスを悪用したメール送信のお詫びについて
https://muroran-it.ac.jp/guidance/info/post-40565/ 2022/6/22
[4] 大大学院の教職員が Emotet 感染, 不審メール確認される
https://cybersecurity-jp.com/news/67529 2022/6/22
[5] ンサムウェア被害防止対策
https://www.npa.go.jp/cyber/ransom/index.html 2022/9/30
[6] ンサムウェア
https://www.trendmicro.com/ja/jp/security-intelligence/research-reports/threat-solution/ransomware.html 2022/9/30