公立はこだて未来大学 2021 年度 システム情報科学実習
グループ報告書

Future University-Hakodate 2021 System 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 ページ作成班

Group Name

Web page creation group

プロジェクト番号/Project No.

19-A

プロジェクトリーダ/Project Leader

今井徹雄　Tetsuo Imai

グループリーダ/Group Leader

小原賢太　Kenta Ohara

グループメンバ/Group Member

小原賢太　Kenta Ohara
松村涼　Ryo Matsumura
岩舘玲於奈　Reona Iwadate
多田龍生　Ryusei Tada
佐藤壱磨　Kazuma Sato
山崎将也　Syoya Yamazaki

指導教員

白勢政明　由良文考

Advisor

Masaaki Shirase　Fumitaka Yura

提出日

2022 年 1 月 19 日

Date of Submission

January 19, 2022

概要

本プロジェクトは、暗号化技術という観点からセキュリティに関する理解を深め、実際に活用・体験することを目的としたプロジェクトである。主に昨年度から新型コロナウイルスの影響により、オンライン授業やリモートワークの増加に伴って情報の管理が以前より重要となっている。そこで、情報を守るセキュリティ技術や、それを扱うユーザのセキュリティ意識がより大切になる。今年度の Web ページ作成班での活動は、未来大生のセキュリティ意識について調査をし、それをもとに未来大生のセキュリティ意識を向上させる Web ページの作成を目標とする。

キーワード　セキュリティ, アンケート調査, Web ページ

（文責: 小原賢太）

Abstract

This project's purpose is to deepen the understanding of security in terms of cryptographic technology and actually to utilize and experience it. Information management has become more important than before due to the increase of online lessons and remote work mainly influenced by COVID-19 since last year. Therefore, security technology that protects information and security consciousness that the user handles become more important.The activities of this year's Web page creation group will investigate the security awareness of FUN, and aim to create Web pages that improve the security awareness of FUN based on the survey.

Keyword Security, Questionnaire survey, Web page

（文責: 小原賢太）

目次

第 1 章　はじめに

1.1　背景

情報通信ネットワークの発展やスマートフォンの普及、並びに新型コロナウイルスの流行によって、在宅勤務の時間やおうち時間を楽しむ流れができ、オンラインコンテンツのニーズが高まっている。その中で、在宅勤務中に外部ネットワークに直接接続した社用パソコンがサイバー攻撃の被害に遭うなどの事例が報告されている。また、警察によるサイバー犯罪の検挙件数は、令和２年で過去最多を更新している [1]。こういった現状の中、本グループで行った未来大生を対象にしたアンケートでは、未来大生のセキュリティ意識が低いことが判明した。これは、日常的にオンラインコンテンツを利用する未来大生にとって危機的な状態である。そのため、未来大生各人がサイバー攻撃の知識を身につけ、サイバー攻撃から身を守るにはどうするべきか考える必要がある。

（文責: 小原賢太）

1.2　目的

本グループでは、Web ページを通して、未来大生のセキュリティに対する意識を向上させるという目標のもと、未来大生のセキュリティに関する知識を調べるため、セキュリティ意識調査アンケートを実施した。その結果を基に、「サイバー攻撃に関する知識が少ない」、「セキュリティに関して考える機会が少ない」という２点の未来大生の問題点を解決する Web ページの作成を目的とした。

（文責: 小原賢太）

1.3　IPA の調査について

本グループの活動は、IPA のアンケート調査 [1] に基づいている。IPA とは、Information-technology Promotion Agency の略である。日本語では、独立行政法人情報処理推進機構という。この調査は、脅威編と倫理編に分かれており、脅威編は、一般国民のサイバーセキュリティにおける脅威の認識と対策の実施状況を把握すること、倫理編は、ネットモラルに対する現状把握などを目的として実施しているものである。

（文責: 小原賢太）

1.4　前期の課題設定

はじめは、未来大生のセキュリティ意識を向上させるにはどのような Web ページの機能が必要かを話し合い、それを明確にするためにセキュリティ意識調査アンケートを実施した。その結果、前期の課題となる「サイバー攻撃に関する知識が少ない」、「セキュリティに関して考える機会が少

ない」の 2 点の問題の解決に向けた「サイバー攻撃の疑似体験」と「適したセキュリティソフトを推奨するクイズ」の機能を実装することとし、それに伴った機能の実装とプログラミングの学習、Web ページの作成を課題とした。

（文責: 小原賢太）

1.5　後期の課題設定

後期は、前期で集めたアンケートや中間発表のフィードバックを基にさらにどのような機能を追加するか、また、Web サイト全体をどのような形で完成させるかという 2 点を課題とした。

（文責: 小原賢太）

第 2 章　プロジェクト学習の概要

2.1　問題の設定

2.1.1　「サイバー攻撃に関する知識が少ないこと」

全世界において、情報通信技術ネットワークの発展やスマートフォンの普及により、インターネットが身近なものとなってきている一方で、サイバー犯罪の件数やトラブルの被害件数は増加している。このことから、私たちはサイバー攻撃に関する知識が少ないことが原因で被害が増えているのではないかと考えたため、この問題を設定した。

（文責: 松村涼）

2.1.2　「セキュリティに関して考える機会が少ないこと」

前期私たちが実施した、アンケートの「自分の PC のセキュリティについて考えたことはありますか？」という質問に対して「よく考える」と回答した人の割合が 5 %だったことから、私たちはセキュリティに関して考える機会が少ないのではないかと考えたため、この問題を設定した。

（文責: 松村涼）

2.1.3　通常の授業でなく、プロジェクト学習で行う利点

セキュリティに関しての講義は行われているが、あくまで対象が不特定多数ということもあり、一人一人に対して対策を練るというようなことは行われていない。また、大きな事件や重大な欠陥などの情報は得られるが、身近に潜んでいる脅威については深く掘り下げられていない。一人一人の状況に基づき、それに合った情報の提供や対策の仕方を提示するのは、講義では向かない。

（文責: 松村涼）

2.2　具体的な手順・課題設定

2.1 節で述べた課題を解決するために、前期では実際にどのような知識や情報、対策が必要なのかを考え、以下のような手順を設定した。

1. セキュリティソフトやウイルスについての調査
   Web ページの作成に向けて前提知識の調査を行った。主に、コンピューターウイルスの感染経路とその対策、セキュリティソフトの有用性について調査をした。
2. はこだて未来大学の生徒を対象にしたアンケートの実施
   未来大生がどの程度のセキュリティ意 識を持っているかを確認するため、アンケートを実施した。

3. アンケート結果の考察
   アンケートの結果を考察し、どのように Web サイトをアップグレードするか考えた。

以上の調査やアンケート結果から、未来大生のサイバー攻撃やセキュリティに関する情報の少なさやセキュリティに関する意識の低さが見られた。それらを解決するために、「サイバー攻撃の疑似体験」と「適したセキュリティソフトを推奨するクイズ」を実装することで 2.1 節で述べた課題を解決するとともに、その機能を搭載するうえで必要なプログラミングの学習、Web ページの作成を課題とした。

（文責: 松村涼）

2.3 到達レベル

1. 簡単な Web ページを作成できる
   前期に progate などで学んだ HTML や CSS の知識で Web ページのレイアウトなどを作れるようになった。
2. JavaScript のライブラリを使ってクイズを作成できる
   JavaScript のライブラリである jquery を使ってクイズを作成できるようになった。

（文責: 松村涼）

2.4 課題の割り当て

前期では、Web ページ作成のためにグループ全員が HTML および CSS について学習し、HTML および CSS を扱える環境を作成することで、実際に Web ページの作成を行った。前期で作成を開始した Web ページの内容は「ウイルス感染とその対策」と「フィッシング詐欺体験」の二つであり、これらに対してグループ内で二つの班を作成し、実際に作成にとりかかった。

- 小原：ウイルス感染とその対策を掲載するサイトに載せる文章のまとめ
- 松村：ウイルス感染とその対策を掲載するサイトに載せる文章のまとめ
- 岩舘：ウイルス感染とその対策を掲載するサイトの作成
- 多田：フィッシング詐欺体験ができるサイトの作成
- 佐藤：フィッシング詐欺体験ができるサイトの作成
- 山崎：フィッシング詐欺体験ができるサイトの作成

後期では、引き続き「ウイルス感染とその対策」と「フィッシング詐欺体験」についての 2 つ Web ページの作成のほかにトップページの作成を開始した。

- 小原：ウイルス感染とその対策を掲載するサイトに載せる文章のまとめ
- 松村：トップページの作成
- 岩舘：ウイルス感染とその対策を掲載するサイトの作成
- 多田：フィッシング詐欺体験ができるサイトの作成
- 佐藤：フィッシング詐欺体験ができるサイトの作成
- 山崎：フィッシング詐欺体験ができるサイトの作成

（文責: 松村涼）

第 3 章　課題解決のプロセスの概要

3.1　プロジェクト内における課題の位置付け

近年、インターネット上のサイバー攻撃やネット詐欺などは増加傾向にある。そのため、インターネットを利用する際には各個人がセキュリティに対するより高い意識を持ち、この様な行為から自らを守ることが重要である。特に、インターネットを日常的に利用する未来大生にとってこの問題は身近なものであるため、セキュリティに対する意識を高く持つ必要がある。しかし、現状において未来大生はどの程度のセキュリティ意識やサイバー攻撃などの行為に関する知識を持っているのだろうか。そこで本グループでは、未来大生のセキュリティに対する意識を調査するため、未来大生を対象としたアンケートを実施した。しかしながら、現在の社会情勢の影響により大人数でのアンケートが実施できず、回答数が少なかったため、アンケート結果が信頼性の欠けるものとなってしまった。そのため、本グループのアンケート結果とともに、IPA が行ったアンケート調査の結果を参考にして未来大生のセキュリティ意識を向上させるための Web サイトを作成することを課題とした。

（文責: 岩舘玲於奈）

3.1.1　アンケート内容と結果

本グループが行ったアンケートには全 17 個の質問があり、各質問では複数の回答から当てはまるもの 1 つを選択するという方式を取っている。前半は主にセキュリティソフトに関する質問 6 個、後半はサイバー攻撃やセキュリティ全般に関する質問 11 個から構成されている。前半の質問内容は以下のようになっている。

- 質問 1「自分の PC のセキュリティについて考えたことはありますか？」
- 質問 2「OS やソフトウェアのアップデートやパッチをすぐに適用していますか？」
- 質問 3「PC にセキュリティソフトを導入していますか？」
- 質問 4「自分が利用しているセキュリティソフトがどのような機能を持っているかを理解していますか？」
- 質問 5「フリー Wi-Fi を抵抗なく使用していますか？」
- 質問 6「以上の質問を踏まえた上で、自分の PC はセキュリティの面で安全だと思いますか？」

前半の質問 1 に対して「よく考える」「たまに考える」「あまり考えない」「考えたことはない」と回答した結果はそれぞれ 5.9%、47.1%、29.4%、17.6% であった。質問 2 に対して「すぐ適用する」「数日〜数週間たってから適用する」「適用しない（または強制的に適用されるまで放置する）」と回答した結果はそれぞれ 29.4%、41.2%、29.4% であった。質問 3 に対して「はい」と回答した結果は 64.7% であった。質問 4 に対して「よく理解している」「そこそこ理解している」「あまり理解していない」「まったく理解していない」「セキュリティソフトを導入していない」と回答した結果はそれぞれ 0%、11.8%、41.2%、23.5%、23.5% であった。質問 5 に対して「抵抗なく使用し

ている」「抵抗はあるが使用している」「抵抗はないが使用しない」「抵抗があるので使用しない」と回答した結果はそれぞれ 47.1%、17.6%、5.9%、29.4% であった。質問 6 に対して「安全である」「そこそこ安全である」「あまり安全でない」「安全でない」と回答した結果はそれぞれ 11.8%、41.2%、23.5%、23.5% であった。後半の質問内容は以下のようになっている。

- 質問 7「サイバー攻撃に関する知識を持っていますか？」
- 質問 8「サイバー攻撃に対して危機感を持っていますか？」
- 質問 9「サイバー攻撃の被害にあったことはありますか？」
- 質問 10「以下のサイバー攻撃（マルウェア、フィッシング詐欺、パスワードリスト攻撃、DoS 攻撃、トロイの木馬、セッションハイジャック、ランサムウェア）に関してあなたはその攻撃内容を知っていますか？」
- 質問 11「以下のサイバー攻撃（マルウェア、フィッシング詐欺、パスワードリスト攻撃、DoS 攻撃、トロイの木馬、セッションハイジャック、ランサムウェア）に関してあなたはその対策方法を知っていますか？」
- 質問 12「フィッシング詐欺に遭遇したことがありますか？」
- 質問 13「二段階認証はしていますか？」
- 質問 14「USB などの外部記憶媒体を人目につく場所で保管していますか？」
- 質問 15「USB などの外部記憶媒体を廃棄する際、中身のデータをすべて削除していますか？」
- 質問 16「SNS 上に自分または知人の個人情報を特定することができるような情報を載せていますか？」
- 質問 17「Web サイトのドメイン名、URL に着目して Web サイトにアクセスしていますか？」

後半の質問 7 に対して「持っている」「そこそこ持っている」「あまり持っていない」「持っていない」と回答した結果はそれぞれ 11.8%、17.6%、41.2%、29.4% であった。質問 8 に対して「持っている」「そこそこ持っている」「あまり持っていない」「持っていない」と回答した結果はそれぞれ 17.6%、35.3%、17.6%、29.4% であった。質問 9 に対して「ある」と回答した結果は 94.1% であった。質問 10 に対しては、各攻撃について「知っている」と回答した結果はそれぞれ 52.9%、64.7%、41.2%、70.6%、64.7%、5.9%、23.5% であった。質問 11 に対しては、各攻撃について「知っている」と回答した結果はそれぞれ 41.2%、41.2%、23.5%、17.6%、41.2%、5.9%、23.5% であった。質問 12 に対して「ある」と回答した結果は 11.8% であった。質問 13、14、15 に対して「している」と回答した結果はそれぞれ 64.7%、82.4%、29.4% であった。質問 16 に対して「載せている」と回答した結果は 35.3% であった。質問 17 に対して「している」と回答した結果は 29.4% であった。

（文責: 岩舘玲於奈）

3.1.2　利用した IPA のデータ

先述の通り、現在の社会情勢の影響から本グループが行ったアンケートでは回答数が少なく、その結果が信頼性の欠けるものとなってしまった。そのため、Web サイトを作成するに当たって、IPA がインターネット利用者を対象に行った「2020 年度情報セキュリティの脅威に対する意識調

査」[2][3] の結果を参考にした。また、クイズ班では IPA が提示している「日常におけるセキュリティ対策」[4] を基にして Web サイトの作成を行った。以下の図に、参考にした IPA のデータを示す。

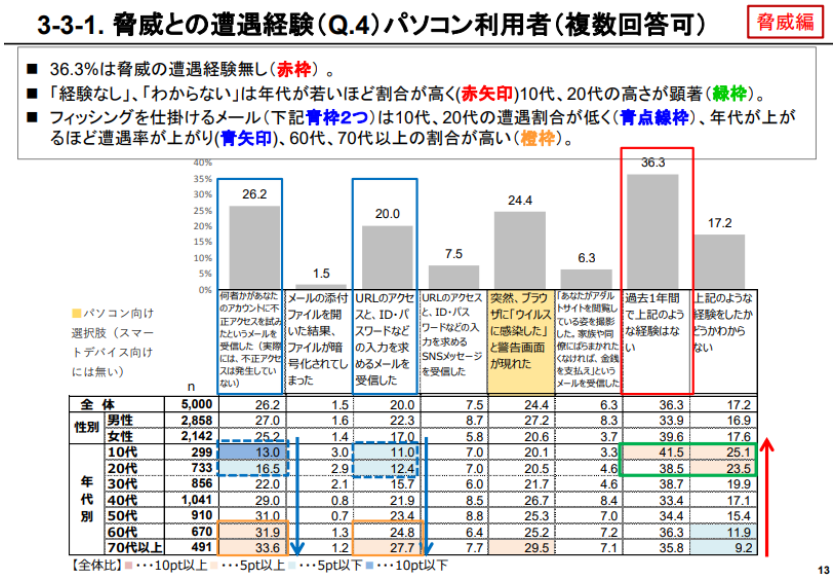


図 3.1　2020 年度情報セキュリティの脅威に対する意識調査 概要報告書 13p

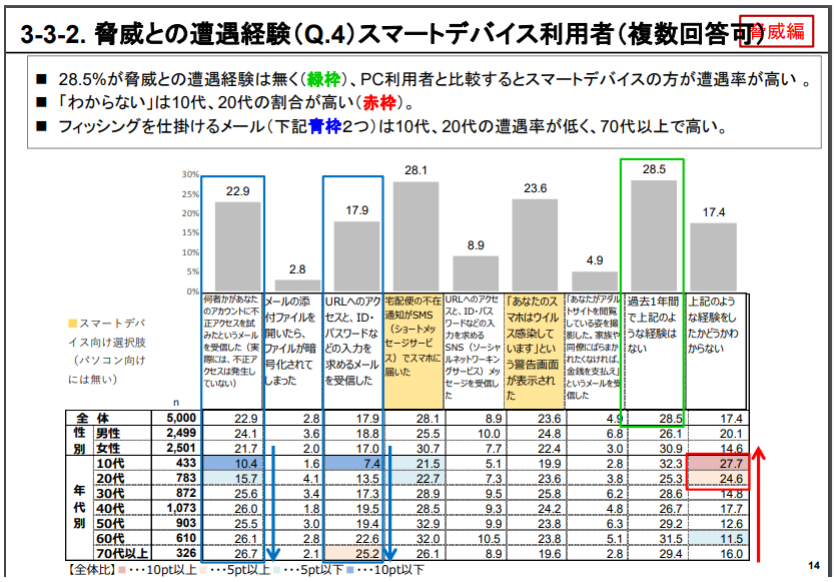
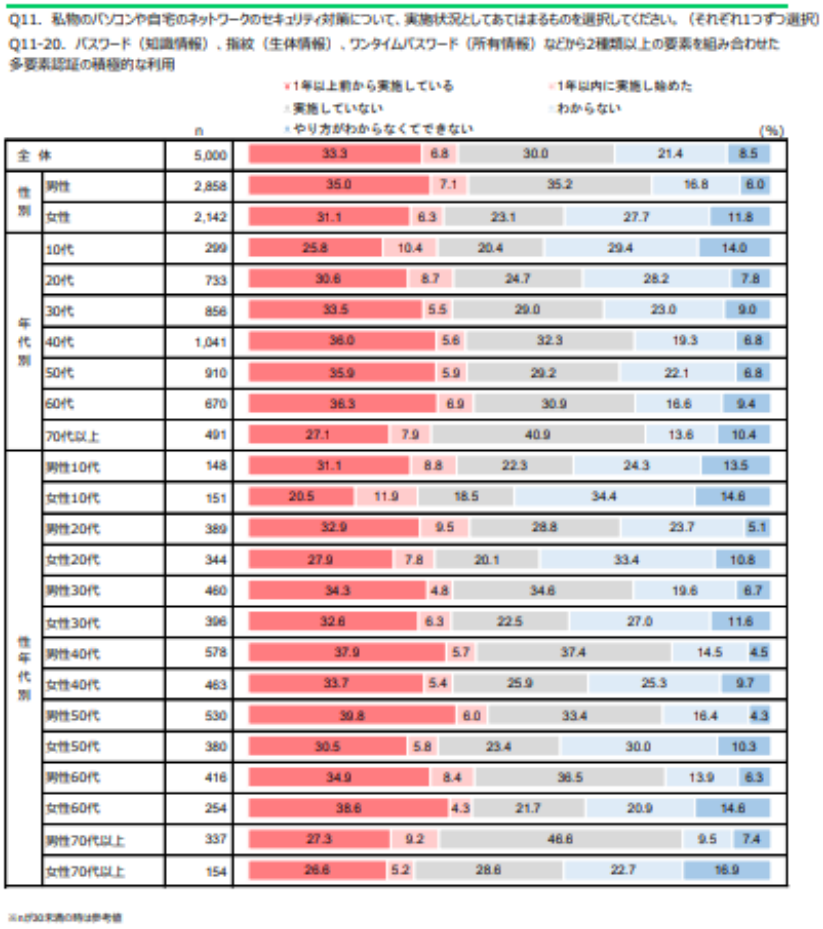


図 3.2　2020 年度情報セキュリティの脅威に対する意識調査 概要報告書 14p

（文責: 岩舘玲於奈）



Q11. 私物のパソコンや自宅のネットワークのセキュリティ対策について、実施状況としてあてはまるものを選択してください。（それぞれ1つずつ選択）
Q11-20. パスワード（知識情報）、指紋（生体情報）、ワンタイムパスワード（所有情報）などから2種類以上の要素を組み合わせた多要素認証の積極的な利用

		n	1年以上前から実施している	1年以内に実施し始めた	実施していない	わからない	やり方がわからなくてできない
全体		5,000	33.3	6.8	30.0	21.4	8.5
性別	男性	2,858	35.0	7.1	35.2	16.8	6.0
	女性	2,142	31.1	6.3	23.1	27.7	11.8
年代別	10代	299	25.8	10.4	20.4	29.4	14.0
	20代	733	30.6	8.7	24.7	28.2	7.8
	30代	856	33.5	5.5	29.0	23.0	9.0
	40代	1,041	36.0	5.6	32.3	19.3	6.8
	50代	910	35.9	5.9	29.2	22.1	6.8
	60代	670	36.3	6.9	30.9	16.6	9.4
	70代以上	491	27.1	7.9	40.9	13.6	10.4
性年代別	男性10代	148	31.1	8.8	22.3	24.3	13.5
	女性10代	151	20.5	11.9	18.5	34.4	14.6
	男性20代	389	32.9	9.5	28.8	23.7	5.1
	女性20代	344	27.9	7.8	20.1	33.4	10.8
	男性30代	460	34.3	4.8	34.6	19.6	6.7
	女性30代	396	32.8	6.3	22.5	27.0	11.6
	男性40代	578	37.9	5.7	37.4	14.5	4.5
	女性40代	463	33.7	5.4	25.9	25.3	9.7
	男性50代	530	39.8	6.0	33.4	16.4	4.3
	女性50代	380	30.5	5.8	23.4	30.0	10.3
	男性60代	416	34.9	8.4	36.5	13.9	6.3
	女性60代	254	38.6	4.3	21.7	20.9	14.6
	男性70代以上	337	27.3	9.2	46.6	9.5	7.4
	女性70代以上	154	26.6	5.2	28.6	22.7	16.9

※nが30未満の時は参考値

図 3.3　2020 年度情報セキュリティの脅威に対する意識調査 性年代軸報告書 90p

3.1.3　未来大生含む若者のセキュリティ意識

本グループが未来大生を対象として行ったアンケート調査の結果によると、「サイバー攻撃に関する知識をもっている」という人は 3 割程度であり、サイバー攻撃に関する知識の少ない未来大生が多数であることが分かる。また、「自分の PC のセキュリティについて考えたことがある」という人は 5 割程度、「自分が利用しているセキュリティソフトがどのような機能を持っているかを理解している」という人は 1 割程度であり、セキュリティに関して考える機会のない未来大生が多数であることが分かる。

次に、IPA がインターネット利用者を対象に行った「2020 年度情報セキュリティの脅威に対する意識調査」の結果によると、フィッシング詐欺の遭遇経験があると回答した人は約 7 割であった。また、そもそもフィッシング詐欺の遭遇経験があるか分からないと回答した人の割合は 10 代と 20 代が最も高く、ともに 3 割程度であった。さらに、10 代と 20 代のセキュリティ対策をしている割合が男女ともに 5 割以下であった。

これらから、未来大生を含む若者のセキュリティに対する意識は総じて高くないことが分かる。特に、フィッシング詐欺の遭遇経験があるか分からないと回答した人の割合が全体で最も多かったことからは、この様なサイバー攻撃に関する知識が少ない若者が多いことが考えられる。また、男女ともにその半数がセキュリティ対策をしていないことからは、自らのセキュリティについて考えていない若者が多いことが考えられる。しかしながら、現代では多種多様なサイバー攻撃が増加し

つつあり、またセキュリティ技術の進化に伴ってその脆弱性を利用した犯罪も増加しつつある。このような状況の中で自らの安全を確保するためには、まずサイバー攻撃について知っておくことや、自らのセキュリティが十分に安全なものであるかなどを考える機会を持つことが重要である。よって本グループでは、「サイバー攻撃に関する知識が少ない」「セキュリティに関して考える機会が少ない」という 2 点の問題点を解決する Web ページの作成を課題とした。

（文責: 岩舘玲於奈）

3.2 課題解決の方法

3.2.1 サイバー攻撃に関する知識が少ない点について

まずは文献やインターネットでサイバー攻撃に関する調査を行い、その特徴や対処法をまとめた。また、そこから課題解決に必要な Web サイトの機能を考案し、「サイバー攻撃の疑似体験」の機能を実装する事に決定した。

（文責: 岩舘玲於奈）

3.2.2 セキュリティに関して考える機会が少ない点について

まずは文献やインターネットを用いてコンピュータウイルスやセキュリティソフトなどに関する調査を行い、それぞれまとめた。また、そこから課題解決に必要な Web サイトの機能を考案し、「適するセキュリティソフトを推奨するクイズ」の機能を実装することに決定した。

（文責: 岩舘玲於奈）

3.2.3 課題解決の方法 (サイバー攻撃疑似体験班　レイアウトについて)

レイアウトについては各自で様々な文献を参考にし、レイアウト構成を確認した。レイアウトを学習するにあたって、インターネットで、どのようなレイアウト構成が基本なのか、どのようにすることで、より相手の情報が伝わりやすくなるかなどを追求したうえでレイアウト構成について学習した。また学習以外にも、フィッシング詐欺の疑似体験ページにおいてはよりリアルさを追求するため、実際に使われている「web mail」などのレイアウトを参考にしてメール受信画面や、メール本文のレイアウトを作成した。特に個人情報入力画面においては、実際に起きたサイバー犯罪のモデルを参考に、「メールアドレス」や「パスワード」入力画面などを作成し、リアル感の向上につなげた。また、最終ページでは、内容が多いため、タイトルやトピックなどを明確に分けたうえで、全体的に見やすいレイアウト構成にした。

（文責: 山崎将也）

3.2.4 課題解決の方法 (サイバー攻撃疑似体験　使用した言語、環境について)

使用した言語については前年度同様、HTML、CSS 言語を用いた。しかしメンバー全員がほとんど使用した経験がなかったため、前期の活動で progate というプログラム学習ページを用いて基

本的なプログラムを学習した。学習期間は 5 月から 7 月の間で学習を行なった。学習に関しては、無料プランで行い、progate 内の「HTML & CSS 初級編」を使用し、ヘッダーの構造や、フッターのレイアウト構成、お問い合わせフォームの作成を行った。その後、後期では前期で確認した内容を用いて web ページ作成に当たった。また、基本的なもの以外の知識・技術に関しては、その都度インターネットで確認しプログラムを行った。環境に関しては、Atom を用いてプログラムを作成し、GitHub で実装を行った。Atom に関しては複数人での同時編集が可能であるが、各自で作業を行った。作業はメンバー個人で行っていたので、進捗度合の確認の際はファイルの共有や、実際にプログラムをしたページを GitHub の web ページに実装し、完成度の具合や、不具合などがないかを確認した。また、GitHub アカウントの管理に際しては、サイバー攻撃疑似体験班のアカウントを作成し、アカウント管理は代表してグループリーダーの山崎が管理を行った。Web ページの変更の際は変更点を確認したうえで GitHub にログインし変更を行った。

（文責: 山崎将也）

3.2.5　課題解決の方法 (サイバー攻撃疑似体験班　ページ内の内容について)

今回作成したページの特徴としては、実際のフィッシング詐欺に近い体験をすることができるページとなっている。実際のフィッシング詐欺を体験することで、フィッシング詐欺の内容を理解することができるほか、どの点に気を付ければよいかなどを確認することができる。また、レイアウトやストーリーなどを工夫したので、よりリアルに近い web ページを作成した。それによりインターネットによる犯罪などセキュリティ意識の向上につながると考える。

詳しい内容に関しては、はじめは『注意書きページ』から始まる。ここでは、今後進めていくと。実際にメールアドレスやパスワードを入力する画面が表示されるが、疑似体験者が入力する情報は、記録されない旨を伝え、また架空のメールアドレスやパスワードを使用するように呼び掛けている。次のページに進むと、プロローグということで、どのような経緯でストーリーが始まるかが書かれている。プロローグを追加することで、あたかも自分が実際にメール受信を確認しなければならない気持ちにさせ、疑似体験を開始するという目的がある。メール本文に関しては、実際にフィッシング詐欺で使われたメール本文と同様にし、リンクアドレスがあたかも実際に存在する通販会社に似た URL を使用している。その後、アカウントの情報を更新するためという名目で個人情報を入力させる。これに関しても実際に起きたフィッシング詐欺の内容をもとにしている。その後背景が黒塗りで、個人情報が掲載され、『攻撃者はすでに上記の個人情報を盗んでいます。』と表記しているページに飛ぶ。このページでは、疑似体験者に対して驚きや焦りを与えるため、背景を黒塗りにし、危険性のあるページに仕上げた。また、最終ページに関しては、フィッシング詐欺のほかにトロイの木馬などのサイバー犯罪や、どのような点に気を付ければよいか、またサイバー犯罪に関する統計値などが載せられているので、フィッシング詐欺意外にも学習可能なページとなっている。内容としては、まず疑似体験の振り返りというページを設けている。そもそもフィッシング詐欺の定義は何なのか、疑似体験で起きたことの注意すべきポイントなどが掲載されている。画像を張り付けてあるので、わかりやすいものとなっている。またアンケートに関しては、情報処理推進機構 (IPA) が公表した「情報セキュリティ 10 大脅威 2021」を掲載し、どのような点に注目すればよいのかが書かれている。中にはセキュリティ以外にも『SNS での誹謗中傷』について書かれているので、セキュリティ意識の向上以外にも、情報モラルについて考える必要がある点にも触れている。

（文責: 山崎将也）

3.2.6 課題解決の方法 (サイバー攻撃疑似体験班　サイバー攻撃の疑似体験ページ作成のプロセス)

まず初めに、どのサイバー攻撃の疑似体験を作成すべきか、班員同士で話し合いをした。その結果、最も被害件数が多く、年々脅威が増加しているサイバー攻撃を選ぶべきという判断に帰着した。IPA のデータなどから、上の条件に合うサイバー攻撃を探したところ、フィッシング詐欺の疑似体験を作成すべきとなった。フィッシング詐欺を扱うと決まったあとは、班員各々でフィッシング詐欺についての知識を得る作業に移った。コーディングに移る前に、どのような流れの疑似体験にするか話し合った。流れを決めるにあたっては、過去のフィッシング詐欺被害のケースを参考に決めた。流れが決まった後、ページに書く文章、デザイン、ページの動きを決めた。　ある程度設計が決まった後、HTML で文章を書き、デザインに合わせてタグ付けを行った。そして、すべてのページが完成したあと、Javascript を用いてページのリンク、文字自動書き起こし、スイッチの反応、などの機能を付けた。全ての HTML , CSS, Javascript を記述したあと、デバッグ作業に移った。はじめに考えたフィッシング詐欺疑似体験ページの設計通り動いているか、一ページごと班員全員で確認作業を行った。班員の確認が終わり次第、他班の人にもバグがないか確認していただいた。デバッグ作業のなかで、新しい意見などがでたため、その追加などを行い、再度デバッグを行い、サイバー攻撃疑似体験ページの作成が完了した。

（文責: 多田龍生）

3.2.7 課題解決の方法 (クイズ班 トップページ)

トップページは、1 年間の本プロジェクトの活動内容や、本プロジェクトの概要、成果物などをまとめたページにした。また、前期に未来大学の生徒を対象にして行ったセキュリティ意識に関するアンケート結果の代わりに IPA が行った調査を掲載することにより、より説得力の高いデータを示すことができた。

（文責: 松村涼）

3.2.8 課題解決の方法 (クイズ班　レイアウト)

レイアウトの決定は、次のようなプロセスで行った。

1. 調査し校正した文章をページに書き込む
2. Web ページとして違和感がある部分や読みにくい部分を洗い出す
3. メンバーがその問題に対して改善案を提案
4. 改善案を吟味し、Web ページに反映
5. 2 に戻る

レイアウトは、全体的な自然さや文章の読みやすさ, 機能性を考慮した。全体的な自然さは、Web ページの色合いや各見出しと本文との文字の大きさのバランスを整えることで表現した。文章の読みやすさは、文字の大きさや赤字などでの重要な箇所を強調することで表現した。また、文章自体

を回りくどくしない工夫もした。機能性面は、ポイントに飛べる目次の追加をした。また、PC だけでなくスマホの利用も想定し、文章の置き方を変えるなどの工夫も行った。

（文責: 小原賢太）

3.2.9　課題解決の方法 (クイズ班　ウイルスについて載せた Web サイト)

クイズ班 Web ページの「コンピュータウイルスについての知識をつける」ことを目的としたページの説明である。以下のような構成となっている。

1. コンピュータウイルスの定義
2. コンピュータウイルスの種類について
3. コンピュータウイルスの種類についてより詳しく
4. コンピュータウイルスの感染経路について
5. コンピュータウイルス感染対策
6. セキュリティソフトの重要性について
7. 個人でできるセキュリティの向上方法について

構成としては、コンピュータウイルスについての知識をつけた後にセキュリティソフトについての情報や、簡単にできるセキュリティの向上方法について学ぶことができるようになっている。よってセキュリティに関する知識が無い未来大生でも、このサイトを利用すればすぐにセキュリティ対策が可能だ。また、この後に自分に適したセキュリティソフトがわかるクイズのページのリンクがあるが、これを自分のセキュリティに関して考える第一歩とすることができるだろう。つまり、利用することでコンピュータウイルスに関する知識やセキュリティの向上が見込める Web ページとなっている。

（文責: 小原賢太）

3.2.10　課題解決の方法 (クイズ班　自分に適したセキュリティソフトがわかるクイズ)

「はい、いいえ」の二者択一の質問 6 つに回答することで、回答者の PC やその用途に適したセキュリティソフトを提示するクイズを Web サイト上に作成した。提示するセキュリティソフトについては、昨年度のプロジェクト「暗号とセキュリティ」のセキュリティ意識調査班が作成した Web サイトにて紹介されていたものを採用した。具体的には、Windows Defender、ESET インターネット セキュリティ、マカフィー リブリーフ、カスペルスキー セキュリティ、ウイルスバスタークラウド、ノートン 360 の 6 種類である。回答する質問は、「使用している OS は Windows である」「ウイルスソフトにお金をかけたくない」、「PC だけでなく、スマホやタブレットにもセキュリティソフトを導入したい」「PC の重さに悩んでいる」「ウイルスの誤検知をしないことより、新種ウイルスへの安心感のほうが重要である」「よく Twitter1 や Facebook などの SNS を使用する」の 6 つである。質問に回答した後は、その回答に適したセキュリティソフトとその概要を提示するとともに、そのセキュリティソフトの昨年度プロジェクトメンバーによるレビューが見られるよう、昨年度に作成された Web サイトの該当ページへのリンクも提示するようにした。
クイズ作成の際には、各質問に「はい」か「いいえ」で回答した際にそれぞれ該当するセキュリ

ティソフトにポイントを 1 つ加点し、合計したポイントが最大となるセキュリティソフトが回答者に最適なものであるとした。具体的な例を挙げると、質問 1 の「使用している OS は Windows である」に「はい」で回答した場合には全てのセキュリティソフトに 1 つポイントを加点し、「いいえ」で回答した場合にはマカフィーリブリーフ、ウイルスバスタークラウド、ノートン 360 のそれぞれに 1 つポイントを加点する、となる。

（文責: 岩舘玲於奈）

3.2.11　課題解決の方法 (クイズ班　使用した言語、環境について)

Web サイト作成では、主に HTML や CSS、また JavaScript などの言語を使用する必要がある。しかしながら、本グループのメンバーはこういった言語についての知識が少なく、また実際に Web サイトの作成をした経験が少なかったため、初めにこれらの知識・経験の習得を行う必要があった。そこで、インターネット上でプログラミング言語を学べる Progate というサイトを主に利用し、HTML、CSS についての知識を習得した。また、Progate では実際に簡単な Web サイトを作成しながら HTML、CSS の学習を行ったため、成果物である Web サイト作成の流れを大まかに把握することが出来た。ソースコード記述の際には、オープンソースのテキストエディタである Atom を利用した。また、「自分に適したセキュリティソフトが分かるクイズ」の作成では、HTML、CSS の他に JavaScript のライブラリである jQuery を使用した。jQuery では、JavaScript で記述するソースコードよりも短いソースコードで同じ処理を行えるため、ソースコードの短縮が可能である。そのため、ソースコードの可読性が向上し、デバッグや内容変更を行う際に効率よく作業をすることが出来た。

（文責: 岩舘玲於奈）

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

小原賢太の担当課題は以下のとおりである。

4 月　プロジェクト学習のガイダンスを確認
5 月　昨年度の Web ページの改善案の話し合いをし、セキュリティソフトやサイバー攻撃についての調査と HTML、CSS の学習
6 月　HTML の環境構築 (Atom) と Web ページを触りながら学習、jQuery の学習、中間発表のポスター作成
7 月　中間発表の準備と中間発表のフィードバック
8 月　中間発表から今後の方針を決める、クイズ班 Web ページ作成を進める
9 月　クイズ班 Web ページ作成を進める
10 月　クイズ班 Web ページ作成を進める
11 月　クイズ班 Web ページ作成を進める、成果発表会のポスターを作成する
12 月　成果発表会
1 月　報告書作成

（文責: 小原賢太）

松村涼の担当課題は以下のとおりである。

4 月　プロジェクト学習のガイダンスを確認する。
5 月　昨年度の Web ページの改善案の話し合いをし、セキュリティソフトやサイバー攻撃についての調査と HTML、CSS の学習をした。
6 月　Web サイトに掲載するクイズの内容を考える。
7 月　Web サイトに掲載する文章を考え、中間発表の動画を作成。
8 月　クイズ班 Web ページ作成を進める
9 月　クイズ班 Web ページ作成を進める
10 月　クイズ班 Web ページ作成を進める
11 月　クイズ班 Web ページ作成を進める、発表会の動画を作成する
12 月　成果発表会
1 月　報告書作成

（文責: 松村涼）

岩舘玲於奈の担当課題は以下のとおりである。

4 月　プロジェクト学習のガイダンスを読んだ
5 月　昨年度の Web ページの改善案を考案し、セキュリティソフトについての調査と HTML、CSS の学習をした
6 月　追加する Web ページのレイアウトを考案し、コーディングに入った

7 月　Web ページのコーディングの続きと、中間発表
8 月　クイズ班メインページのコーディングと、中間提出物の作成
9 月　Web ページのコーディングと、今後の活動内容の確認
10 月　Web ページのデザインを見直し、コーディング
11 月　Web ページに追加掲載する内容の調査とコーディング、Web ページの修正
12 月　Web ページの修正、成果発表、期末提出物の作成
1 月　報告書の訂正

（文責: 岩舘玲於奈）

多田龍生の担当課題は以下のとおりである。

4 月　プロジェクト学習のガイダンスを読んだ
5 月　Web ページ班のテーマ決めとサイバー攻撃についての調査, HTML CSS の学習
6 月　疑似体験班のテーマ決めとコーディング
7 月　コーディングと中間発表
8 月　サイバー攻撃疑似体験班の Web ページを作成する
9 月　サイバー攻撃疑似体験班の Web ページを作成する
10 月　サイバー攻撃疑似体験班の Web ページを作成する
11 月　サイバー攻撃疑似体験班の Web ページを作成する
12 月　成果発表会
1 月　報告書作成

（文責: 多田龍生）

佐藤壱磨の担当課題は以下のとおりである。

4 月　プロジェクト学習のガイダンスの確認
5 月　昨年度成果物を評価し改善案を出すこと、そして新しくアンケートの作成案を出す。HTML と CSS の学習
6 月　サイバー攻撃疑似体験班となり Web ページのレイアウト案を出す。インターネットでセキュリティに関する調査と学習を行う。中間発表のスライドと原稿作成を担
7 月　中間発表のスライドと原稿作成を担当
8 月　サイバー攻撃疑似体験班の Web ページを作成する
9 月　サイバー攻撃疑似体験班の Web ページを作成する
10 月　サイバー攻撃疑似体験班の Web ページを作成する
11 月　サイバー攻撃疑似体験班の Web ページを作成する
12 月　成果発表会
1 月　報告書作成

（文責: 佐藤壱磨）

山崎将也の担当課題は以下のとおりである。

4 月　プロジェクト学習のガイダンス確認
5 月　サイバー攻撃についての調査および、web ページ作成に必要なスキル習得。主に HTML や

CSS。

6 月 サイバー攻撃についての調査、それと同時にペー氏の流れや頁の趣旨などを確認。

7 月 web ページのコーディング開始。中間発表資料作成。中間発表での回答や意見の共有。

8 月 夏季休暇は各次ページのコーディングを実施。

9 月 Web ページのコーディングと、今後の活動内容の確認

10 月 Web ページのデザインを見直し、コーディング

11 月 Web ページに追加掲載する内容の調査とコーディング、Web ページの修正

12 月 Web ページの修正、成果発表、期末提出物の作成

1 月 報告書の訂正

（文責: 山崎将也）

4.2 担当課題解決過程の詳細

4.2.1 小原賢太

4 月 プロジェクト学習のガイダンスを確認し、プロジェクト配属希望書を提出。

5 月 Web ページ作成班に配属、その後クイズ作成グループに配属。Web ページの改善案と実装機能について話し合い。HTML と CSS の学習を行う。書籍 [5] などでセキュリティソフトやサイバー攻撃について調査。

6 月 引き続きセキュリティソフトやサイバー攻撃について調査。Atom の環境構築と Atom を使ってコーディングしながら学習。jQuery の学習。また、中間発表のポスター作成を行う。

7 月 中間発表の準備と本番、中間発表のフィードバックから今後の課題を考えた。

8 月 後期の方向性を決める。

9 月 追加機能を考える。クイズ班ページのレイアウトを考える。

10 月 追加ページ「自分でできるセキュリティ向上方法」を作成。また、クイズ班ページの調整を行う。

11 月 ポスターの作成などの、製菓発表会の準備を行った。追加ページ「自分でできるセキュリティ向上方法」はクイズ班ページに統合した。

12 月 成果発表会の準備と本番。成果報告書などの作成をした。

1 月 成果報告書などの作成をした。

（文責: 小原賢太）

4.2.2 松村涼

4 月 プロジェクト学習のガイダンスを読み、プロジェクト配属希望調査を提出し、本プロジェクトに配属、その後 Web ページ班に配属した。

5 月 昨年度の本プロジェクトの製作物である Web サイトを閲覧し、メンバーと改善点やアップグレードできる点を話し合った。そして、インターネットなどでコンピュータウイルスの感染経路や、その対策、セキュリティソフトの有用性などを調べた。そして、その内容を Web サイトに載せるために必要な HTML、CSS の学習をした。

6 月 引き続き HTML や CSS の学習をしつつ、Web ページに掲載するクイズの内容を考えた。

7 月 中間発表で必要な動画の作成をした。また、中間発表のフィードバックを共有した。

8 月 Web サイトに掲載する情報をインターネットで調べてまとめ、文章にしました。

9 月 引き続き Web サイトに掲載する情報をインターネットで調べてまとめ、文章にしました。

10 月 引き続き Web サイトに掲載する情報をインターネットで調べてまとめ、文章にしました。

11 月 暗号とセキュリティのトップページの作成に取り掛かりました。

12 月 暗号とセキュリティのトップページを見直し修正を加えました。そして、成果発表用の動画作成に取り掛かりました。

1 月 期末提出物の作成と訂正をしました。

（文責: 松村涼）

4.2.3 岩舘玲於奈

4 月 プロジェクト学習のガイダンスを読み、本プロジェクトに配属、その後 Web ページ班に配属した。

5 月 昨年度の本プロジェクトで制作された Web サイトを閲覧し、メンバーと共に改善点や追加機能を出し合った。そして、文献やインターネットでセキュリティソフトの重要性を調査し、6 つの主要なセキュリティソフトについて、それぞれの特徴やメリット・デメリットをまとめた表を作成した。さらに、Web ページ作成のために HTML、CSS の学習をした。

6 月 インターネット上の他の Web ページなどを参考に Web ページのレイアウトを考案し、Web ページのコーディングに取り掛かった。

7 月 引き続き、Web ページのコーディングを行った。また、中間発表を行い、その意見を共有した。

8 月 クイズ班のメイン Web ページのレイアウトやデザインを考案し、コーディングに取り掛かった。また、グループ報告書の担当部分を作成し、その構成や内容をメンバー間と共有しながら適宜修正した。他の中間提出物である学習フィードバックシートや学習ポートフォリオも同時に作成し、各提出物の誤字や内容の矛盾などをチェックし修正した。

9 月 引き続き、クイズ班のメイン Web ページのコーディングを行った。また、前期に行った活動の振り返りと後期の活動内容の確認を行った。

10 月 作成した Web ページのデザインをメンバーと見直し、修正した。特に、文章の読みやすさを考慮して文字サイズの大きさを変更したり、見出しやボタンの配置を変更した。

11 月 クイズ班のメイン Web ページに追加掲載する内容を調査し、主にコンピュータウイルスに関する文章を作成、Web ページに掲載した。具体的には、コンピュータウイルスの種類やその概要、また実際の例などを紹介した。文章を作成する際には、なるべく読みやすく分かりやすいものにするよう注意し、見直しと修正を繰り返した。

12 月 作成した Web ページを全体的に見直し、誤字やデザインの細かな修正を行った。また、成果発表を行い、質疑応答を担当した。その後は、学生や教員からのフィードバックを確認し、期末提出物の作成を行った。

1 月 引き続き期末提出物の作成を行い、誤字や内容の修正を行った。

（文責: 岩舘玲於奈）

4.2.4　多田龍生

4 月　何を制作するのかの検討, プロジェクト学習のガイダンスを読んだ
5 月　サイバー攻撃についての調査、HTML　CSS の学習を行った。
6 月　疑似体験班のテーマ決めとコーディング（主に機能）をした。
7 月　コーディングと中間発表の反省をした。
8 月　各次ページのコーディング（主に機能）をした。
9 月　Web ページのコーディング（主に機能）をした。
10 月　Web ページのコーディング（主にデザイン）をした。
11 月　Web ページのコーディング（主にデザイン）と web ページの見直しをした。
12 月　Web ページの修正、成果発表、期末提出物の作成をした。
1 月　報告書の訂正をした。

（文責: 多田龍生）

4.2.5　佐藤壱磨

4 月　プロジェクト内で何を目的とするかを決め、班ごとに分かれることになり、Web ページ作成班を担当することになった。
5 月　去年の先輩方が行ったアンケートを参考に、新しいアンケートを作成した。また、HTML と CSS の学習を行った。
6 月　Web ページ班をさらにグループ分けをし、サイバー攻撃疑似体験班となり Web ページのレイアウトを考えた。そして、インターネットを用いてセキュリティに関する調査・学習を行った。中間発表のスライド作成を担当した。
7 月　Web ページ作成を行いつつ、スライドを完成させた。
8 月　web ページのコーディングを進め、中間提出物の作成をした。
9 月　web ページのコーディングの進捗を共有し、web ページのコーディングを進めた。
10 月　web ページのデザイン案を出し、web ページのコーディングを進めた。
11 月　web ページの最終調整をし、追加掲載する内容をネットで調査し web コーディングを進めた。
12 月　成果発表のスライドと原稿の作成をし、成果発表後には期末制作物の作成をした。
1 月　期末提出物の作成と訂正をした。

（文責: 佐藤壱磨）

4.2.6　山崎将也

4 月　Web ページ班に配属。その後 Web ページでどのようなコンテンツを提供するか検討。HTML 学習を行う。
5 月　Web ページ班のサイバー攻撃疑似体験グループに配属。サイバー攻撃について調査。
6 月　サイバー攻撃について調査。Web ページの流れやコンテンツの配置などの検討、コーディングを行う。

7 月　中間発表の意見を共有。Web ページのコーディングを行う。

8 月　夏季休暇に伴い、各自での web ページコーディング作業を行った。また、変更点やミス等あった場合は slack で情報の共有を行った。

9 月　9 月前半は 8 月同様であった。後半からは、各自夏季休暇中に行った作業内容の確認などをした。

10 月　web ページ全体における内容の確認や、グループ内でのフィードバックをもとに変更点を洗い出した。その後各自で web ページのコーディングを進める。

11 月　11 月前半までは 10 月同様 web ページのコーディングを進めた。後半からは、8 割程度完成していたので、web ページの挙動確認や、複数のデバイスで実際に操作するなどの確認を行った。

12 月　自分たちの成果物が完成していたので、成果発表に向けて、質疑応答の際の内容の確認や、ほかのグループのサポートなどに回った。

1 月　報告書を作成

（文責: 山崎将也）

第 5 章　結果

5.1　中間発表

今年の中間発表は 7 月 9 日の 4 時限目と 5 時限目に行われた。中間発表では、他プロジェクトの人に自分たちの活動背景や活動目的の発表や前期の間に行った活動の報告を行った。また、他プロジェクトの活動の発表を一人 3 プロジェクト見に行き、評価をした。これらをプロジェクト内で二つのグループに分かれ、4 時限目と 5 時限目で交代して行った。また、一回当たり 15 分の発表で 1 時限あたり 3 度の発表を行い、発表後には質疑応答を行った。発表後には評価アンケートを集計し、見つかった課題や指摘された問題を解決するためにグループで議論した。

（文責: 佐藤壱磨）

5.1.1　紹介用動画

本プロジェクトの説明を行うために中間発表では動画での紹介を行うことにした。理由としては、紹介用動画用のスライドを作成予定であったことからこのスライドの内容を最も簡潔に分かりやすく説明するためである。このスライドは各班制作し、制作したスライドを 1 つのスライドにまとめて動画のスライドとした。動画の作成方法としては、音声を録音しそれをスライドの動画と合わせることによって作成した。

（文責: 松村涼）

5.1.2　紹介用スライドと原稿

中間発表のスライドと原稿は紹介用動画でも使用し、5 分程度の動画にして提出予定であったため、時間内に発表が終わるように調整して作成した。また、紹介用動画を閲覧してもらえれば誰が見ても自分たちの活動がどのようなものなのかわかるように、聴講者の方々にできるだけ自分たちのやっていることがわかりやすく伝わるように意識して作成した。文字が多くなってしまわないようにイラストを使用し、前提知識が必要になりそうな言葉の使用を控えた。作成後には紹介用動画担当の方と話し合い、時間内に発表が終わるのか、発表時にわかりやすい、またはわかりにくい語彙の取捨選択を行い修正した。また、web ページ作成班とメールシステム班のスライドを合わせたときに、発表の時間が長くなりすぎてしまわないように調整した。メールシステム班の方がこちらのスライドと比べて内容が専門的であったため、こちらのスライドをできるだけ簡潔にし、できるだけ時間に余裕ができるように調整した。結果として、スライドが見やすかった、わかりやすかったという意見を多く頂けたためスライドの作成は成功したと考えている。しかし、反省点として、話の内容が薄いためもう少し詳しく説明が欲しかったという意見もあった。文字を減らしてイラストを多く入れてしまったため、時間内に話の内容を深く掘り下げることができなかったことが原因であると考えている。

（文責: 佐藤壱磨）

5.1.3　中間発表の集計結果

回収したシートの枚数：39 枚

発表技術について

・平均点:7.3

・今後の課題

とても高評価であったが、課題点も多く見つかった。いただいた意見より、 次のような課題点が挙げられた。

- 質疑応答の際には、質問を想定したスライドを作成しておく
- 今後の計画をより具体的に立てる
- メンバー全員が活動内容を十分に把握する
- 課題達成の度合いを測る方法を考えておく

「質疑応答の際には、質問を想定したスライドを作成しておく」に関しては、最終成果物発表の際に実現するように努める。「今後の計画をより具体的に立てる」に関しては、中間発表の反 省会後に実際に計画を立てた。「メンバー全員が活動内容を十分に把握する」は、他グループ間で のやり取りが少なかったことが原因として、今後は報告を徹底するように努める。「課題達成の度合いを測る方法を考えておく」は、方法がまだ決定していないため、今後の課題とした。

・評価点:4(5 段階評価のうち)

理由　スライド、原稿に関してはわかりやすいものを作成でき、紹介用動画作成も見やすく聞きやすいものを作成できた。実際に、見やすかった、わかりやすかったという意見もいただけたため、良かったと考えている。しかし、中間発表時に聴講者の質問に対して瞬時に答えられないような場面があったため。

発表内容について

・平均点:8

・今後の課題

とても高評価であったが、課題点も多く見つかった。いただいた意見より、 次のような課題点が挙げられた。

- 背景の説明が長いので、背景はもっとまとめて活動内容や作品の説明にもっと発表時間を割く
- 発表内容が薄かったため、もう少し詳しい説明を加える

「背景の説明が長いので、背景はもっとまとめて活動内容や作品の説明にもっと発表時間を割く」に関しては、最終成果物発表の際に実現するように努める。「発表内容が薄かったため、もう少し詳しい説明を加える」に関しては、見やすくわかりやすいスライドを作成しようと心掛けた結果、内容が深堀されなかったと考えているため、最終成果物発表ではわかりやすいスライドを作成することは心掛けながら、内容が薄くなりすぎてしまわないように意識して作成するように努める。

・自分のグループの評価
評価点:3(5 段階評価のうち)
理由　聴講者の方全員に自分たちの活動の概要はある程度伝えられたのではないかと考えている。しかし、意見でも頂いたが、発表時に活動背景の時間が長かったり発表内容が薄かったりしたため、説明するべき内容の割合をもっと考えるべきだった。最終成果発表ではこの課題点を意識して取り組んでいくべきだと考えている。

（文責: 佐藤壱磨）

5.2　成果発表

成果発表は 12 月 10 日 (4 限 5 限) に行った。プロジェクト内で前半後半に別れ行った。一回あたり 15 分の発表で、前期の活動報告および、質疑応答を行った。発表後に発表についての評価アンケートを集計し、今後の課題についてグループごとに議論した。

（文責: 多田龍生）

5.2.1　紹介用動画

本プロジェクトの説明を行うために成果発表では動画での紹介を行うことにした。理由としては、紹介用動画用のスライドを作成予定であったことからこのスライドの内容を最も簡潔に分かりやすく説明するためである。このスライドは各班制作し、制作したスライドを 1 つのスライドにまとめて動画のスライドとした。動画の作成方法としては、音声を録音しそれをスライドの動画と合わせることによって作成した。

（文責: 松村涼）

5.2.2　紹介用スライドと原稿

中間発表で作成したスライドを改良する形で進めた。最終発表で主に伝えたかったのは成果物であるため、成果物とその説明を多く追加した。また、中間発表では話が薄いと指摘を受けたため、説明のスライドを増やした。そのため、文字が多く、スライドが見づらくなってしまった。スライドを増やして 1 ページ当たりの情報量を減らすなど、まだ改善の余地があった。

（文責: 佐藤壱磨）

5.2.3　成果発表の集計結果

回収したシートの枚数：　38 枚

・発表技術について

・平均点：7.4

プラスの評価では、発表がスムーズでよかった、動画だけでなく要点を発表していて内容がわかりやすかった、質疑応答の開始前に質問の仕方や注意事項についての説明があり、良かった、質問がない時間にプロジェクトの説明を行っており空白時間が生まれないようにしていた、とても詳しく説明されていた、プレゼン資料もイラストが豊富に用いられていることもあり理解しやすかった、という意見が多かった。専門用語が多い分野のため、初耳の人にも理解できるよう準備していたのが効果的であった。

マイナス評価では、早口に感じた、所見の言葉が多いため後半に行くにつれて前半に紹介された言葉を忘れてしまって、後半の内容を理解するのが大変だった、画像と文章が被ってしまっている部分があったので残念だった、成果物に辿り着くまでの説明がかなり長く感じた、という意見が多数であった。内容が濃く、専門用語も多数あるため、多く説明を取り入れなければ理解するのが難しいと考え、早口になってしまった部分は反省すべき点である。やはり専門用語が多いため内容を理解するのが難しいと感じる人が多数いたため、専門用語を別の言葉に置き換えて説明する、より要点を絞って理解しやすい説明にするなどして改善していきたい。

・自分のグループの評価
評価点：4　(5 段階評価のうち) 理由　研究結果が良くわかる発表であった、疑似体験のスクリーンショットを用いることでどのような流れで行くのか理解しやすいなど、発表スライドへの評価は良かった。しかし、無言の時間があったとの指摘から 4 点とした。

・発表内容について

平均点：7.9

プラス評価では、動画、スライドで網羅的に触れられていた、セキュリティソフトの比較がわかりやすい、疑似体験では実際にメールからパスワード入力まで体験でき、情報流失までの流れを体験できた、クイズでは自身に合うセキュリティソフトの提案などを行えてセキュリティに対する意識などが生まれる、細かい部分までシミュレーションを想定していてよかった、テーマと制作物がちゃんとあっていた、目標設定もしっかりとしていると感じた、という意見が多かった。きちんと作業に入る前に目標設定と制作物のずれがないか話し合ったのが効果的であった。そして、疑似体験はフィッシング詐欺とはどういうものなのか知らない人でもわかるように制作したのが良かった。マイナス評価では、内容を噛み砕いても良いのでは、目標が未来大生のセキュリティ意識を向上させることなのに、アンケートをとれなかったのが残念、動画のスライドにおいてイラストが使われてわかりやすくなっている部分と、情報量が多くてわかりづらい部分の差が大きい、セキュリティ意識を上げるという目的のためにセキュリティソフトを提案する Web サイトを作るのはあまり直接的ではない、という意見があった。特にアンケートをとれなかったのが残念という意見が多数あった。実際アンケートを取ったが、母数が少ないと判断し、使用できなかった。アンケートを取る方法を他に考えるという課題を見つけることができた。そして情報量が多くわかりづらい部分については、より要点をまとめてわかりやすい文章を考える能力を習得するという改善策が浮き彫りとなった。

・自分のグループの評価

評価点：4　(5 段階評価のうち) 疑似体験班は専門用語も少なく、スクリーンショット付きでの説明であったためわかりやすく、目標と成果物のずれもなかったため、良い評価であった。ただ、アンケートをとれなかった部分がマイナス評価となり 4 点とした。

（文責: 多田龍生）

5.3　プロジェクトの結果

今期の私たちの活動方針は、前年度の先輩方が作成した web サイトを改良・改善することが目的であった。そのため、前期の活動ではまず前年度の成果物を見て良い点改善点などを議論し、伝わりずらい文章などを改善し、前提知識のない人が見ても理解できるような web サイトにできるように変更した。また、HTML の知識がなかったため HTML の学習を進めながら、インターネットや情報ライブラリを用いて情報を集め、現在の社会情勢も考えながら web サイトに記載する情報を追加していった。そして、後期に入ってから web サイトのコーディングを始めるために web サイトのレイアウトや大まかなデザインについての話し合いやページごとの役割分担などを決めた。前年度の web サイトはどこに何が記載されているのかわかりづらかったり、もっと見やすいデザインにできるのではと考え、後期に入ってからは前年度のものとはデザインを一新することにし、初めから web サイトのコーディングを進めていった。

web サイトには未来大生に実際にアンケートを取って、その情報を参考にして web サイトを作成する予定だったが、大人数にアンケートを取ることが困難であったため、IPA が提示している「日常における情報セキュリティ対策」を参考にして web サイトを作成していった。IPA では予定よりもはるかに多い人数にアンケートを行っていたため、前年度では未来大生へのアンケート結果のみを用いて web サイトを作成していたが、より信頼性のある web サイトへ改良・改善したセキュリティに関する web サイトを作成できた。

また、クイズに答えることでその人に合ったセキュリティソフトを提案するサイトも作成した。こちらでは「はい」か「いいえ」に答える質問が全 6 問あり、それらに答えることでセキュリティソフトを提案してくれる。セキュリティソフトに関してどのような効果を持ったものなのかの説明やソフトのレビューの書いてあるサイトを記載し、自分に合ったセキュリティソフトがどのようなものなのか疑問を持って調べてもらえれば、よりセキュリティ意識が向上すると考えた。

最後にフィッシング詐欺を疑似的に体験できるサイトを作成した。こちらでは普段の生活の中に潜むサイバー攻撃を疑似的に体験し、より意識してもらえるようにと考えた。体験後にはどのように対策すればよいのか、他にどのようなサイバー攻撃があるのかなどを詳しく書いた web サイトを作成した。

（文責: 佐藤壱磨）

5.4　プロジェクトの評価

5.4.1　前期評価

前期においては、プロジェクトを進めるにあたって、背景や目的を確認した上で、今後それぞれのグループが目的を達成するために何をすればいいのかを決めることができた。背景に関しては、

昨今の新型コロナウイルスによって在宅勤務などのオンライン化が加速していることに触れ、警察によるサイバー犯罪の検挙件数や、公立はこだて未来大学の学生を対象としたアンケート結果などを参考にし、セキュリティ意識の低さを指摘した点に関しては、数値的な証拠などを挙げ、説得力のある web ページを作ることができた。同様に目的設定においても背景に沿っていて、なおかつ公立はこだて未来大学というフィールドでのプロジェクト遂行に積極的であったといえる。また、中間発表に関しては、準備作業を各メンバーで分担し、期日通りにポスターや動画編集を完成されることができた。しかし、質疑応答の際に、一部の質問で明確に答えることができなかった点もあった。そこに関してメンバー間での内容の再確認が必要となった。

（文責: 山崎将也）

5.4.2 後期評価

後期に関してはそれぞれのグループが成果物完成に向けて作業を行った。各々、必要なスキルを身につけたうえで、web ページの UI 改善や、新規ページ作成にも取り組んでいた。特に『疑似体験班』の成果物に関しては、実際に疑似体験をしてもらい、フィッシング詐欺の特徴を知ってもらうという、新たな成果物を作成した。また、後期の成果発表時においても、『疑似体験のクオリティが高かった。』、『疑似体験のストーリーなどがあり面白く思いました。』などといった評価もいただいた。今後は、疑似体験班やクイズ班のページの UI 一新や、新たにセキュリティ意識の向上に向けた web サイト作成やアプリの開発などを行ってもよいと考える。しかし、後期の最大の反省点として挙げられるのが 2 点存在してしまった。1 つ目はフィードバックを行わなかったことである。そもそも web ページの作成の背景として、セキュリティ意識の向上を目的にしていたのにもかかわらず、未来大生に対しての情報公開やフィードバックの実施をおろそかにした結果、ただ web ページを作成しただけになってしまった。来年のプロジェクト学習に関してはフィードバックの徹底をしてほしいと考える。2 つ目は疑似体験班とクイズ班の共同親ページの UI デザインの一新ができなかったことである。今回親ページを作成したが、親ページのもととなるもののデザインが、前年度のものであり、そのページの UI を解決するという目標があったが、それぞれのグループが web ページの作成に集中しすぎたことや、グループ間での連携がうまく取れなかったので、結果として全面的な UI 改善に至ることができなかった。今回の件をもとに、今後このようなプロジェクトを行う際は、まずグル―プ間での情報を円滑やり取りできるように、情報の共有の時間を設けたうえで議論などするべきであると考える。

（文責: 山崎将也）

5.5 担当分担課題の評価

5.5.1 小原賢太

Web サイトとクイズの作成　セキュリティ意識の向上を目的とした Web サイトの作成にあたって、「適したセキュリティソフトを推奨するクイズ」機能の実装に向けて活動した。また、クイズ班の Web サイトのレイアウトやバランスなどを何度も考え、よりよい物にする努力ができた。よって Web サイト並びにクイズ作成は、特に問題なく順調に進めることができた。

調査活動　掲載内容を決めるため、文献や IPA などの Web サイトを利用して調査を行った。その

結果、クイズ班の Web ページにて個人でできるセキュリティ向上方法の内容を掲載することができた。

HTML CSS の学習と利用　はじめは、学習サイト progate を利用して基礎的な能力を習得した。ここで身に着けたもの以外の知識は実際にコードを書く際に必要に応じて様々な Web ページから情報を仕入れた。これにより、ボタン機能や折り畳み機能、スキップ機能などについて理解することができた。

ポスターの作成　中間発表　ポスター作成は、メール班のメンバーと共同で行った。中間発表フィードバックで、今後のより具体的な計画を立てるべきという指摘を頂いたので、最終成果物までの活動では改善する。

ポスターの作成　成果発表　中間同様、メール班のメンバーと共同で作業を行った。色や文章のバランス、背景のデザインやどのような図を乗せるのかなど、入念に話し合い試行錯誤をすることで、完成度の高いポスターを作成することができた。

（文責: 小原賢太）

5.5.2　松村涼

コンピュータウイルスへの対処法の調査　セキュリティ意識の向上を目的とする Web サイトの作成にあたって、コンピュータウイルスの予防やかかってしまった時の対処法などをインターネットなどで調査をした。さらに、調査を進め理解を深めていくことが課題である。

中間発表での動画の作成　中間発表で使う動画の作成をした。動画に関して話すペース、声の大きさが聞き取りやすかったという指摘があったので、このクオリティ以上のものを作り上げることが今後の課題だ。

成果発表での動画の作成　中間発表に続き、成果発表で使用する動画作成をした。動画の時間制限がある中、必要な情報を正確に伝えるために尺などを考慮しつつ、話し方や内容を工夫することができた。

（文責: 松村涼）

5.5.3　岩舘玲於奈

セキュリティソフトについての調査　「適したセキュリティソフトを推奨するクイズ」の作成に当たって、文献やインターネットを用いてセキュリティソフトの果たす役割やその重要性を調査し、これに基づいて 6 つの主要なセキュリティソフトをまとめた。ここでは、誰が見ても分かるような分や表を作る努力をし、見やすいまとめを作成できた。

HTML、CSS、jQuery の学習　Web ページ作成のため、まずは HTML と CSS の学習をして技術の習得を目指した。これらの学習では主に progate を利用し、分からない事やさらに詳しく学習したい事などについては、適宜ほかの Web ページなどを参考にして理解を深めた。また、「適したセキュリティソフトを推奨するクイズ」の Web ページを作成する際には、HTML と CSS の他に jQuery を利用する必要があったため、複数の Web ページを参考にその基本知識や利用方法などを学習した。

Web ページのレイアウト、デザイン　Web ページのコーディングに入る前に、まずはその大まかなレイアウトを考案した。その際には、昨年度に本プロジェクトで作成された Web ページ

などを参考にしながら、目次や文章の位置を変更するなどの試行錯誤を繰り返し、より見やすいものとなるようにした。また、ひと通り Web ページが完成した後には、グループメンバーにその見やすさなどのフィードバックをもらい、それに従って背景の色や文章の大きさ、文字サイズなどの微調整を行った。

Web ページのコーディング　HTML と CSS および j Query の開発言語を用いて、「適したセキュリティソフトを推奨するクイズ」とその Web ページ、またクイズ班のメインページをコーディングした。その後はグループメンバーからフィードバックをもらい、バグなどの修正を行った。

コンピュータウイルスに関する調査　クイズ班のメインページにコンピュータウイルスに関する文章を追加掲載するため、その調査を行った。主に IPA やその他の Web サイトを参考にして、コンピュータウイルスの種類とその特徴、実際の事例などをまとめ、文章化した。

（文責: 岩舘玲於奈）

5.5.4　多田龍生

サイバー攻撃に関する調査　疑似体験 Web サイトを通して体験する人に有意義な情報を提供するために、サイバー攻撃についての詳しい情報が必要であった。そのため、インターネットなどを用いてサイバー攻撃についての知識を蓄えた。IPA の年間サイバー攻撃件数などのデータを用いて、情報の整理と目標設定の基準を決定した。そして班員ごとに収集する情報を分けて、役割分担をし、しっかりと時間を取って各々で振られた仕事の情報を PDF などでまとめ、班員に共有した。そして、PDF でまとめた情報を見た後のフィードバックを班員各々からもらった。

Web サイトのコーディング　事前学習で、コーディングには HTML CSS , PHP, JavaScript などの知識が不可欠だと判明した。そのことから、Atom でそれらの環境構築を行い、インターネットの情報を参考にしてコーディングを実施した。まず、WEB サイトに記述する文章を班員同士話し合い、思考した。そして、私は、WEB サイトの大まかな流れと、1 ページの構成（文章とデザイン）を考え決定し、大まかに HTML を記述した。その後、仮案として CSS でデザインを行った。最後に装飾したページに動きを付けるために、Javascript でページ移動、文章省略機能などを作成した。

Web ページのメインコンテンツ作成　フィッシング詐欺の疑似体験を作成することになり、まず初めにどのような展開でフィッシング詐欺の体験をしてもらうのか検討した。そして大まかに疑似体験を進める展開が決まった後に、展開ごとに一つ一つ web コーディングを行っていった。その際、メンバー間での想定のすれ違いを防ぐために、ひとつの展開のコーディングが出来次第、時間を取って全員で確認した。

Web ページのレイアウト、デザイン　まず初めに大まかなレイアウト、デザインを決定した。詐欺の体験のため、少し重い雰囲気にすることにし、そこから、background-color, フォントサイズ、アニメーションなどを暗めの設定にした。機能面では、次どのような操作をするべきなのかわかりやすいようにレイアウト、デザインを決めた。そして Javascript,CSS を用いて、WEB サイト全体のデザインをした。最後に班員以外からもフィードバックをもらい、最終調整を行った。

（文責: 多田龍生）

5.5.5 佐藤壱磨

中間発表のスライド作成 Web ページ作成班はさらに 2 つのグループに分かれているので別の班の方からも話を聞き、Web ページ作成班が何をしているのかわかるようにスライドをまとめた。反省点として、プロジェクトの背景を長く書きすぎてしまい、もう少し目的を具体的に説明すべきとの指摘を受けた。

成果発表のスライド作成 中間発表で作成したスライドではもう少し具体的に説明すべきとの指摘を受けたので、見づらくなってしまわない程度に成果物の説明などを具体的に書いた。

web ページの作成 前期でプログラミングを学習したので、後期では web ページのコーディングを進めた。また、どのようなレイアウトとデザインだとページが見やすくなるかなどの案出しも行った。

サイバー攻撃に関する調査 自分自身が知識がなければいけないので、Web ページを作成するにあたって必要な情報をインターネットで調査した。知識のない人でもわかりやすいと思ってもらえるような Web ページを作成するためにはまだ知識が足りないため、今後も学習を続けていきたい。

HTML と CSS の学習 Web ページを作るためのプログラミングの知識がなかったため、基礎的な HTML と CSS の学習をした。基礎知識だけでは Web ページを作ることができないので、今後はもう少し踏み込んだレベルのプログラミングの学習をしていきたい。

（文責: 佐藤壱磨）

5.5.6 山崎将也

web ページの作成 web ページの作成は最終ページを担当した。web ページを作成するにあたって、どのようなレイアウト構成にするかや、どのようなコンテンツを取り入れれば、フィッシング詐欺の疑似体験をした後の振り返りをすることができるかなどを考え、グループメンバーからの意見をもらいながら作業を進めた。また UI 面においても、デバイスによって表示を変えたりなどの変更作業も行った。

HTML と CSS の学習 HTML と CSS の学習においては前期の活動で progate を用いて基本的な考え方を学んだ。実践においては、基本的な考えをもとに、自分が作りたいサイトで、どのようなスキルを使えばよりいいサイトになるかを考えたうえで、インターネットでどのようなタグなどがあるかを調べたうえでプログラムを行った。

成果発表のフィードバック 成果発表におけるフィードバックはおろそかにしてしまったと感じる。私たちのグループは、web ページの作成ということで取り組んでいたが、完成後のアンケートをおろそかにしてしまった結果、目的である『セキュリティ意識の向上』を確認することができなかった。今後はこのようなことがないようにフィードバックを徹底するように心掛けたい。

（文責: 山崎将也）

第 6 章　今後の課題と展望

私たちの課題として挙げられるのは、成果物に対してのフィードバックをとることである。実際、プロジェクト学習の最終目標は成果物を作るという考え方になってしまい、その成果物は、ターゲット層に対して、どのような影響をもたらしたのか、また改善点などはあるかなどの意見をもらわずに終わってしまった。フィードバックをもらわない限り、来年に向けた反省点や改善点などを来年に引き継ぐことができないので、来年からはフィードバックをとることを徹底してほしい。また、フィードバックに関連して、未来大生を対象としたアンケートに関しては、アンケート数が少なかったため、実際に公表して、アンケート結果を使用しても、証拠不十分であると判断されてしまった。来年度以降は、アンケートについても積極的に協力してもらい、より正確なものに強いてほしいと思う。今後の展望として、ウイルスバスターに関する web ページの UI 改善や、最新トレンドに対応したセキュリティ情報を記載したいと考える。また、『疑似体験班』のようなフィッシング詐欺の疑似体験なども、よりリアルでクオリティの高いものにし、セキュリティ意識の向上に貢献する web サイトを作りたい。

（文責: 山崎将也）

付録 A　新規習得技術

HTML
CSS
jQuery
JavaScript
Web サイト作成

付録 B　活用した講義

講義名　情報機器概論
活用内容　Web サイト作成にあたって、HTML を活用

参考文献

[1] 警察庁,”令和２年におけるサイバー空間をめぐる脅威の情勢等について”,2021
[2] IPA,”2020 年度情報セキュリティの脅威に対する意識調査 概要報告書”,2021
[3] IPA, ”2020 年度情報セキュリティの脅威に対する意識調査 性年代軸報告書”,2021
[4] IPA,”日常における情報セキュリティ対策”, https://www.ipa.go.jp/security/measures/everyday.html,2019
[5] 増井敏克, 図解丸わかり セキュリティの仕組み, 翔泳社, 2018