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 Security

グループ名

CTF

Group Name

CTF

プロジェクト番号/Project No.

18-C

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

源平連太郎　Rentarou Genpei

グループメンバ/Group Member

源平連太郎　Rentarou Genpei
原健宏　Takehiro Hara

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

Jan. 18, 2023

概要

公立はこだて未来大学の学生は、IT 系の企業に就職する学生が多いにもかかわらずセキュリティ分野での実践経験が少なく、講義でも基礎的な知識を受講するだけで実践的な演習は行われない。そのため、実際にセキュリティ分野の問題に直面した際に、Wireshack やバイナリ解析のソフトウェアを駆使して問題解決できる学生は少ない。そこで、本グループで設定した課題は、未来大生により深く実践的なセキュリティの技術と知識を身に着けてもらうことである。実施した解決策は初心者向け CTF（Capture The Flag）サイトを作成して、サイト内で問題を解いてもらうことである。CTF とは、情報セキュリティの専門知識や技術を駆使し、隠された Flag（正解）を見つけるハッキングコンテストの一種であり、実践的にセキュリティの技術を身に着けるための最適なコンテンツである。

キーワード　セキュリティ, Capture the flag, 暗号, ネットワーク, Web

（※文責: 源平連太郎）

Abstract

Students in Future University have little practical experience in the security field despite the fact that many of them are employed in IT companies. This is because that the students can only take basic knowledge in the lectures in Future University and can not take practical knowledge. Therefore, when faced with actual problems in the security field, few students are able to solve them using Wireshack or binary analysis software. Therefore, the challenge set by this group is to provide the students with more in-depth, practical security skills and knowledge. The solution is to create a CTF (Capture The Flag) site for beginners and have them solve problems on the site. CTF is a kind of contest to find hidden flags (correct answers) by using information security expertise and techniques, and is the best content to acquire practical security skills.

Keyword Security, Capture the flag, cryptography, Network, Web

（※文責: 原健宏）

目次

第 1 章　背景

1.1　背景

近年、新型コロナウイルスの流行により、仕事のテレワーク化、学校のオンライン化が進んだ。それに伴い情報セキュリティ人材の需要が高まっている。情報セキュリティとは、「情報の機密性、完全性、可用性を確保すること」である [1]。情報セキュリティ上の具体的な脅威としては、不正アクセス、機密情報の漏洩、フィッシング、盗聴などがあり、独立行政法人情報処理推進機構（IPA）の調査によると、2022 年はランサムウェアが最も脅威であるとされている。一方、経済産業省の調査によると日本の情報セキュリティ人材は 2016 年の時点で約 13 万人不足していることから、現在では深刻な人材不足に陥っていると推測できる [2]。また、公立はこだて未来大学（以下、未来大）の学生の多くは IT 企業に就職するため、この問題は未来大生にとっても重要な問題であることが分かる。前年度までのところ、本プロジェクトは、一般的なセキュリティの知識をクイズ形式で学ぶことが出来るウェブサイトを作成するチーム、学内メールのセキュリティを向上させる Google 拡張機能を作成するチームに分かれて活動を行ってきた。

（※文責: 原健宏）

1.2　目的

本グループの目的は、未来大生に、現時点では不足している実践的なセキュリティ分野の技術や知識を身に付けさせることで、日本の IT 企業のセキュリティ意識、延いては日本全体のセキュリティのレベルを上げることである。未来大において現在、セキュリティがキーワードに設定されている講義は 5 つしかなく、そのほとんどが理論のみを扱い、かつ座学を中心としたものである。実際に、セキュリティに関しては、一方的な講義や議論できることを学習目標としているものがほとんどで、脆弱性を理解し、具体的な対策の実装が出来ない学生が多い。また、今年度のプロジェクト学習全体では、セキュリティを取り扱っているプロジェクトは本プロジェクトのみであり、その中でも実践的なセキュリティ技術を体験しながら学べるグループは本グループのみである。そのため、未来大学に不足している実践的なセキュリティ分野の技術や知識を提供することが本プロジェクトの目的である。

（※文責: 源平連太郎）

1.3　方針

上記の目的を達成すべく、CTF サイトを作成しようと考えた。CTF とは、隠された Flag と呼ばれるファイルまたはキーワードを見つけるために、情報セキュリティの専門知識や技術を駆使するハッキングコンテストの一種である。また、実践的なセキュリティ分野の技術と知識を身に着けるためには最適なコンテンツである。実際に本グループが作成した CTF サイトを未来大生に体験・学習してもらうことで、実践的なセキュリティ問題に直面した際にも自己解決できる能力を、

身に付けることができると考えた。本グループが作成した CTF サイトは従来の CTF サイトとは異なり、解法も同時に提供するようにした。従来の常時開放型の CTF サイトでは問題しか提供されず、解答方法を有志が作成するのを待っている場合が多い。そのため、本グループが作成する CTF サイトは非常に敷居が低いものになる。よって本グループは、わかりやすい解答方法を用意することで、初心者が一人で学習が出来るような、未来大生だけではなく CTF を始める初心者に対しても優しく、学習しやすい CTF サイトを作成した。

（※文責: 源平連太郎）

第 2 章　CTF

2.1　CTF

2.1.1　概要

CTF とは、Capture The Flag の略語であり、チームで旗 (flag) を奪い合う旗取りゲームを意味する。本稿での CTF とは、実物の旗を取り合う旗取りゲームではなく、セキュリティ分野の専門知識や技術を使い競い合う、コンピューター上での旗取りゲームを指す。代表的な CTF のスタイルには下記の 3 パターンが存在する。

Jeopardy（ジョパディ）形式

参加者は、一問一答形式で出題される複数分野の問題を解く。高難易度な問題ほどより多くの得点が加算されるルールであり、参加者は期間内により早く、より多くの問題を解くことで順位を競い合う。Jeopardy の由来はアメリカの長寿クイズ番組「Jeopardy!」からきている。大きな CTF 大会の予選や、いつでも参加できる CTF でもあり、本グループが採用する形式でもある。スコアを気にしなければ Github などで問題が公開されているため、過去の CTF の問題を解くことも可能である。

攻防戦（Attack and Defense）形式

参加者がチームに分かれ、他チームへ攻撃してフラッグを奪取する形式である。フラッグがサーバーやアプリケーション内に含まれており、各チームは対象の脆弱性を解析し、攻撃方法や防御方法を編み出すことで攻撃や防御が行われる。多くのフラッグを集めると得点が加算されていき、より多くの得点を取得したチームが勝者となる。

King of the Hill 形式

攻撃と防御の両方が重視される方式で、他チームが防御しているフラッグを書き換えて獲得するか、獲得したフラッグを他チームから防御すればするほど得点が加算されていく。各チームがフラッグを維持している時間に応じて得点が配分され、より多くの得点を取得したチームが勝者となる。

（※文責: 源平連太郎）

2.1.2　歴史

1996 年、コンピューターセキュリティ分野で世界最大の国際会議（DEF CON）の 4 回目の開催である Defcon4 の中で行われた、現在も続いている Defcon CTF が、最初の正式な CTF の大会だと言われている [3]。最初の大会では、審査員が誰に得点を与えるか決めていたが、その結果、多くの混乱を引き起こした。よって、現在ではルールの成熟とともに得点付与の部分は自動化されることが一般的となっている。今日では、2022 年の Defcon CTF の参加チーム数は 470 チーム

に至る。そのため、参加人数の増加に対応するため、予選をオンライン上で行い、上位の参加者のみが DEF CON に招待される方式で行われている。最近では、DEF CON 以外でも CTF の大会が開催されるようになり、日本では、2012 年から始まった日本ネットワークセキュリティ協会 (JNSA) が主催する SECCON CTF を筆頭に様々な CTF の大会が開催されている。

（※文責: 原健宏）

2.1.3 出題例

本グループが採用する Jeopardy 形式では Cryptography（Crypto)、Web、Network、Pwnable (pwn)、Programming、Misc などがある。

Cryptography（Crypto）

Cryptography とは暗号法という意味で、略して「Crypto」と呼ばれる。主にネットワーク通信における暗号技術に関連する問題が出題される。Base64 や RSA 暗号など、一般に普及している暗号化方式が頻繁に問題のネタにされ、エンコードやデコードを行うとフラッグを得ることができる。また、自分で暗号を解読するアルゴリズムを実装することもあり、思考力と共にコーディング力が必要とされる。

Web

出題者が用意した Web サイトの脆弱性を見つけ出し、その脆弱性を利用しフラッグを獲得するジャンルである。クロスサイトスクリプティング（XSS）や SQL インジェクションなどの Web の脆弱性を突くような問題や、PHP や Apache などの言語やサーバーの脆弱性を突く問題が出題される。Dockerfile などを利用し自機で動作させることで他の参加者のアプローチから分離して解答させることも多い。

Network

WireShark などのパケット解析ソフトを駆使して、http 通信や TCP 通信などのネットワーク上に流れるパケットを解析する問題が出題される。具体的には、WEP や WPA などの現在はあまり使われていない脆弱性が発見された通信を利用しているときのパケットを解析することが多い。

Pwnable(pwn)

pwn とは、あるプレイヤーがビデオゲームで相手に勝った際に、俗に「相手を打ち負かした」を意味する「own」を、「pwn」とミスタイプしたことを由来とする、サーバーの脆弱性を攻撃するジャンルである。具体的には、ssh 接続などでサーバーに接続し、クラックするような問題が出題される。

Programming

Programming では、名前の通り、プログラミング、特にアルゴリズムに関する問題が出題される。具体的には、競技プログラミングの問題のように、愚直にコーディングすると現実的な時間では計算が終了しないが、適切なアルゴリズムを使い計算量を抑えると解けるような問題が多い。

Misc

Misc とは Miscellaneous の略であり、「雑多な」という意味である。CTF においても、他のジャンルには分類されない、雑多な種類の問題が出題される。一方、傾向として、インターネット上の様々なサービスや検索エンジンなどを利用して情報を集める「Recon」と呼ばれる種類の問題や、ログファイルやステガノグラフィーなどで情報の埋め込まれた画像を解析する「Forensic and Stego」という種類の問題が出題されることが多い。

（※文責: 源平連太郎）

2.1.4 活用例

CTF は様々な目的で活用されている。具体例として、セキュリティ意識の高い企業では、社内 CTF を開催し、作問と解答を経験することで、攻撃側の視点も含めた実践的なセキュリティ知識の習得 [4] に使われる。また、学生の能力を測るため、社内で作成した問題を利用し、就職を希望する学生が参加する CTF を開催することで、採用試験での選抜 [5] などの目的で活用されることもある。

（※文責: 源平連太郎）

第 3 章　到達目標

3.1　問題設定

現在、セキュリティがキーワードに設定されている講義は情報機器概論、オペレーティングシステム、システム管理方法論、情報マネジメント論、ネットワークセキュリティの 5 つであり、これらの講義では、Wireshark やバイナリ解析ツールなどのソフトウェアを用いた実践的な授業は行われない。しかし、未来大生の多くは IT 企業に就職するため、実践的なセキュリティの知識を求められる。そのため、本グループでは、未来大に不足している実践的なセキュリティ分野の技術や知識を提供することを問題として設定した。

（※文責: 原健宏）

3.2　課題設定

この問題の解決には、実践的なセキュリティ分野の知識と技術を未来大生に身に付けてもらうことが必要不可欠である。しかし、前年度までの本プロジェクトの活動では、一般的なセキュリティの知識を提供するまでに止まっていた。そのため、今年度では、新たに CTF を通して未来大生に実践的な知識を身に付けてもらうことを目的とした CTF を設立した。しかし、初めて CTF に参加する場合、既存の CTF のサイトの多くには共通する 3 つの問題点がある。1 つ目の問題点は、セキュリティ分野に関する専門知識を要求されることである。実際、Network ジャンルの問題のほとんどでは、WireShark などのソフトウェアの操作ができるだけでは解答は難しく、RSA 暗号の基本的な仕組みや脆弱性、IP や TCP などのプロトコルの仕様についての知識などが要求される。2 つ目の問題点は、身近に感じにくい問題を扱っていて、興味を持ちにくいことである。3 つ目の問題点は、丁寧な解説が提供されないため、参加者のスキルアップにつながらない場合がある。多くの場合、未来大生は初めて CTF に取り組むことが想定されるため、既存のサイトでは興味を失ってしまうと考えられる。よって、今年度の CTF グループは、CTF を楽しんでもらえるようなデザインとシステム、身近に感じやすい問題、分かりやすい解説を備えた CTF サイトを作成することを課題として設定した。

（※文責: 原健宏）

3.3　到達レベル

本グループでは、初心者に優しく、解説がわかりやすい、未来大生に向けた CTF サイトを作成することを目標とする。具体的には、デザインは直感的に操作が可能であり、一目見て興味をもってもらえるようなものを目標とする。問題は Web、Crypto、Network、Misc ジャンルと幅広いジャンルを取り扱うことを目標とする。Web ジャンルの問題では XSS を実際に体験できるような環境を作成する。また、Crypto ジャンルの問題では、実際に使われている暗号を取り扱うことで、暗号を身近に感じてもらえるようにする。Network ジャンルの問題では、ネットワークには常に

情報漏洩の危険性があることを感じてもらえるようにする。Misc ジャンルの問題では、テキストエディタのみで解答できるような、特別なソフトウェアを必要としない内容にする。これらの身近に感じる問題とわかりやすい解説を通して、実践的な知識と技術を参加者に身につけてもらう。

（※文責: 源平連太郎）

第 4 章　プロジェクト内のインターワーキング

4.1　源平連太郎

グループリーダーとして、全体の取りまとめやスケジュール管理などプロジェクトをマネージメントした。また、技術分野では、React,　Typescript,　github について学習してきた。具体的には、以下のスケジュールで行った。

- 5 月には担当教員から暗号・セキュリティに関しての基礎知識の講義。
- 6 月には「TCP/IP の絵本」を輪読し、ネットワークの基礎知識の獲得。React, Typescript の習得。CTF コンテストに出場した。
- 7 月に中間発表の準備、中間提出物の作成をした。
- 8 月に Docker を使った環境構築を学んだ。
- 9 月に Javascript を使った、XSS を学んだ。
- 10 月に Web ジャンルの問題作成とそれに関する学習を行なった。
- 11 月に最終発表の準備、最終提出物の作成をした。
- 12 月に最終発表の準備、最終提出物の作成をした。
- 1 月にグループ報告書の作成。

（※文責: 源平連太郎）

4.2　原健宏

私はこれまでに、グループのミーティングにおいては議事録の作成やグループリーダーのサポート、ネットワークの学習教材の選定と共有、CTF サイトのデザイン、問題の作成を行ってきた。また、それに伴い、HTML5, CSS3, Javascript, React, Typescript, Github について学習してきた。具体的には、以下のスケジュールで行った。

- 5 月には担当教員からの講義によって、暗号・セキュリティに関しての基礎知識の獲得。
- 6 月には「TCP/IP の絵本」を輪読し、ネットワークの基礎知識の獲得、グループの活動テーマの決定、React, Typescript, Javascript, CSS3 の学習、中間発表の原稿、ポスターの制作。CTF コンテストに出場した。
- 7 月には Web サイトのデザインの決定、実装、中間提出物の作成。
- 8 月にネットワークやインターネット技術の勉強。
- 9 月に Network ジャンルの問題作成。
- 10 月に Crypto ジャンルの問題作成、CTF サイトのコードのリファクタリング。
- 11 月に Misc ジャンルの問題作成、CTF サイトのデザインのブラッシュアップ。
- 12 月に成果発表会の準備・発表、最終提出物の作成。
- 1 月に最終提出物の作成。

（※文責: 原健宏）

第 5 章　まとめ

5.1　プロジェクトの成果

初めにプロジェクト全体で、担当教員からの講義により、暗号・セキュリティについての基礎知識を身に付け、各グループの活動を体験した。その後、暗号班、Web 班、CTF 班に分かれ活動を開始した。CTF 班では、中間発表までに Web サイトのシステムの設計まで完了した。成果発表会までに、CTF サイトを作成し、Github 上で公開した。

（※文責: 原健宏）

5.2　プロジェクト内の自分の役割

5.2.1　源平連太郎

グループリーダーとして、グループの進捗の管理、他グループとの連絡や連携、メンバーの意思や意見の把握と反映、各種協議における進行などの役割を負った。後期の活動では、円滑な開発実装を目指し、リーダーとしてスケジュール管理やメンバー間のコミュニケーションの円滑化に努め、メンバーが成果物作成に集中できる環境の構築を行った。

（※文責: 源平連太郎）

5.2.2　原健宏

前期の活動では主に、議事録の作成、CTF サイトのデザインを担当した。中間発表においては、発表スライドの作成、質疑応答を担当した。後期の活動では、CTF サイトのデザインの改善、CSSAnimation のプログラミング、Crypto、Network、Misc ジャンルの問題の作成を担当した。成果発表会においては、プロジェクター、パーティションの運搬、発表原稿の推敲、発表、質疑応答を担当した。

（※文責: 原健宏）

5.3　今後の課題

当初の想定通り、初心者に優しく、できる限り身近な問題を扱う日本語の CTF サイトを作成することができたが、未来大に CTF 文化を根付かせるには至っていない。問題点は主に 2 つ考えられる。1 つ目の問題点は、未来大生のほとんどの人は CTF に興味がないため、実際の CTF サイトにアクセスしないからだ。2 つ目の問題点は、CTF サイトの問題をすべて解いた後に何をしたら良いかわからず、CTF をやめてしまうためだ。多くの CTF の大会は複数人のチームで参加することが前提となっているため、他の CTF の大会に参加しにくいことがやめる原因として考えられる。これらの問題の解決方法として、CTF に関するコミュニティを作成することが挙げられる。

1 つ目の問題点は、作成したコミュニティでイベントなどを開催して、CTF に興味がない人にも実際に CTF を体験してもらうことで解決できる。2 つ目の問題点は、コミュニティ内で技術的に優れている人やモティベーションの高い人と交流を行うことで、継続して CTF の大会に参加してもらうことで解決できる。以上より、未来大に CTF のコミュニティを作成することを今後の課題としたい。

（※文責: 源平連太郎）

5.4 成果の評価

5.4.1 中間発表の評価

Google Form によって集計した評価アンケートでは、「発表技術についての評価」の平均が約 7.0/10 点となった。評価の理由としては、「グラフが見づらいから」、「メモを見て発表しているから」、「話す人が 1 人だと単調で飽きてしまうから」という意見が多かった。「発表内容についての評価」の平均は約 7.7/10 点ととなった。評価の理由としては、「根拠に基づき、テーマを設定しているから」、「計画がよく考えられているから」という意見が多かった。また、教員から CTF の説明がわかりづらいという指摘があった。本グループでは、活動のテーマの決定に時間をかけている一方で、発表を他のグループと交代で、一回の発表ごと１人づつに任せていたため、このような評価になったと考えられる。

5.4.2 最終成果発表の評価

同じく Google Form によって集計した評価アンケートでは、「発表技術についての評価」の平均が約 6.6/10 点と芳しくない結果となった。評価の理由としては、「声が小さいから」、「原稿を見て発表しているから」、「スライドが白飛びしていて見づらいから」という意見が多かった。「発表内容についての評価」の平均は約 7.6/10 点と比較的良い結果となった。評価の理由としては、「実際に動いているものを見ることができるから」、「完成度が高いと感じたから」という意見が多かった。全体的に成果物に対する評価は高いが、発表技術に対しての評価は低かった。この原因として、発表場所の体育館では、他のグループが動画などを再生していたことから声が聞き取りづらかったことや、プロジェクト全体で通しての発表練習を一回もしていなかったことが考えられる。また、未来大の教員の方から「グループ間の連携がないことが気になる」という指摘があった。

（※文責: 原健宏）

5.5 担当分担課題の評価

5.5.1 源平連太郎

初心者向け CTF サイトの問題作成（Web 分野）

Web ジャンルの問題において脆弱性を持った Web サイトを構築しようとした。なぜならば Web ジャンルは最も手軽に参加できる CTF の問題であり、CTF 始めたての人は Web の問題を初めて解くことが多いためである。しかし、Web の問題は相互通信が必要なため、初心者向け CTF サイトを公開している Github 上の無料のサーバでは理想的な Web の問題を実装できなかった。

そのため、学校側が提供しているポイントを消費して AWS（Amazon Web Service）を使える制度を利用した。その際、問題になることは生徒一個人が持っているポイントでは 1 週間も AWS を動かすことができないことである。その問題を解決するためには、Docker-compose を用いて Dockerfile を管理し、複数の生徒の AWS サーバーで円滑に Web の問題を実行する環境と参加者のデータをデプロイさせる必要があった。実際の問題を提供する環境には、LAMP 環境を用いた。LAMP 環境とは、4 つのオープンソースソフトウェアを使った Web アプリの環境のことで、「Linux」、「Apache」、「MySQL」、「PHP」を使った環境のそれぞれの頭文字をとって「LAMP」と呼ばれている。なぜ LAMP 環境を用いたかというと Web ジャンルの CTF では PHP の採用率が高いこと、LAMP 環境がレガシーな Web サイトでよく使われているためである。そのため、LAMP 環境を用いることでユーザに身近に感じられると考えたため LAMP 環境を選択した。そして、Gmail-API を用いたメール認証のログイン機能を実装し、クラッキング防止のためログインした参加者のみが問題に取り組めるようにした。実際の問題として SQL インジェクションを用いた問題の作成にあたった。SQL インジェクションを実行できる Web サイトは完成したものの、SQL インジェクションを検知するプログラムの実装が未完成であったため公開することはできなかった。特定の SQL インジェクションを検知し実行するが、それ以外の SQL インジェクションをブロックするプログラムの作成が困難であった。以上のことをまとめると間に合わなかった原因として以下のことが考えられる。

- AWS、Docker、Docker-compose の学習が新たに必要だったこと。
- Linux、Apache、MySQL、PHP の学習が新たに必要だったこと。
- 脆弱性を持った Web サイトの作成が初めてで、脆弱性を持ったサイトの作成方法についての記事がインターネット上に考えている以上に無かったこと。

以上のことにより学習する範囲が広すぎたため Web ジャンルの問題を提供をすることができなかった。だが、すべての技術を使わないと理想の問題が完成しなかったため見積もりが足りなかったと考えられる。また、少しでも労力を減らすための CTF のテクニックとして Dockerfile をユーザーに提供し、ユーザー自身のパソコン上で Web アプリを動かしてもらう方法はあるが、初心者向け CTF を謳っているため Docker の技術をユーザーに求めるのは断念した。

（※文責: 源平連太郎）

5.5.2 原健宏

CTF サイトのデザイン作成

初心者は、CTF をフィクション映画の演出されたハッキングのような派手なものだとイメージしていることが多く、実際に参加すると想像より地味であることから辞めてしまうことが多い。そのため、CTF サイトのデザインでは、CTF 参加者が楽しめるように、SF 映画である「マトリックス」のオープニングで用いられている文字が上から下に流れてくる演出をオマージュした。また、直感的でわかりやすくするため、様々なアニメーションを組み込んだ。具体的には、問題のタイトルをクリックすると問題文が徐々に表示されるアニメーション、解答欄に入力中のときは入力した文字が振動するアニメーションを実装した。その他には、コンテンツの区切りを視覚的にすぐ理解できるようにするため、余白を意識した。また、Bootstrap などの CSS のフレームワークを使わずにデザインをコーディングしたため、他のサイトでは見たことのないようなオリジナリティの

あるデザインになった。興味を持ってもらえるような CTF らしいデザインと使いやすさ・見やすさの両方を参加者に提供できたと考えられる。一方、主にラップトップ型、デスクトップ型のパソコンでのアクセスを想定して作ったため、モバイル端末でのアクセスの場合、必ずしも美しいレイアウトにならない場合がある。そのため、モバイル端末への対応を今後の課題としたい。

CTF サイトのシステム作成

当初はサーバーを契約することで、CTF サイトにログイン機能や得点表示機能を実装し、実際の CTF の大会のように参加者が点数を競い合うようなシステムにする予定だった。しかし、参加者の人数が競争できるほど十分に集まらない可能性や、サーバーの運用にかかる費用を継続して払い続けることができないことに気づいた。最終的には、Javascript によるクライアントサイドの処理でシステムを実装することで、サーバーサイドでの処理を無くし、サーバーレスの構成を実現し、Github Pages でのデプロイが可能となった。具体的なシステムとしては、問題のタイトル、問題文の HTML、flag を入力とするコンポーネントを作成することで、問題追加のたびにシステムの変更が必要ないようにした。また、コンポーネントの作成には React、Typescript 言語を利用した。さらに、React の特徴である「宣言的な View」を用いることで、現代の Web アプリケーションにおいて一般的である、ページ遷移のないシングルページアプリケーションでの実現に成功した。具体的には、最初には問題のタイトルのみの一覧が表示され、問題のタイトルをクリックすると、その問題文が表示・非表示される。このシステムによって、コストを払わずに長く利用できる、現代的な設計の CTF サイトが提供できたと考えられる。一方、問題点として得点機能やログイン機能がないことによる、CTF 自体のゲーム性の低下が挙げられる。この問題の解決には、未来大に CTF サークルの作成が考えられる。サークルがあれば、参加人数を競技が成り立つ程度に集められ、かつサークルの運営費用として大学にサーバー代を申請することもできる。しかし、この方法の実現には、サークルの作成に必要な人数を集める必要があるため、その方法の考察を今後の課題としたい。

Network ジャンルの問題作成

興味を持ってもらうため、未来大の講義の中で個人情報が流出したという問題設定にした。また、実際に未来大で使用されている Free-wifi を扱った。具体的には、http のサイトへログインする際のパケットからパスワードを抜き出すという問題である。初心者向けであるため Free-wifi の SSID、パスワードは予め公開した。初心者に優しく興味を持ってもらえる問題になったと考えられる。

Crypto ジャンルの問題作成

身近に感じられる暗号とは何かを考えた結果、SSH や HTTPS 通信などで使われている RSA 暗号を扱うことにした。また、興味を持ってもらうため、可能な限り現実的な問題設定にした。具体的には、実際によく使われる OpenSSH 形式の公開鍵ファイルから、復号に必要な秘密鍵を割り出す問題を作成した。初心者に優しく興味を持ってもらえる問題になったと考えられる。

Misc ジャンルの問題作成

他の問題の難易度が初心者には難しいと考えたため、テキストファイルから文字列を検索するだけで解けるような問題を作成しようと考えた。また、未来大に入ってから Web プログラミングを始める人も多いと思ったため、私自身が Web プログラミングを始めた際に驚いた Refferrer の仕

様を扱った。具体的には、HTTP 通信のアクセスログの Refferrer からパスワードを抜き出す問題を作成した。初心者に優しく興味を持ってもらえる問題になったと考えられる。

成果発表会での発表

中間発表の評価アンケートにて、「話す人が 1 人だと単調で飽きてしまう」、「聴講者の方を向かずに、原稿を見ながら発表していることが気になる」、「CTF の説明が分かりにくい」というフィードバックを受けた。そのため、成果発表会では、発表の途中で発表者を交代していくことで、各グループの発表は実際にそのグループに所属している人が発表するようにした。加えて、CTF の説明の際は概要の説明だけでなく、実際に CTF の問題を解いてみることで、理解しやすくした。また、原稿を暗記して、聴講者の方へ目を向け大きな声で発表することを意識したため、成果をよく伝えることができたと考えられる。一方、スライドを実際に映してみると、普段の活動場所との照明の明るさの差異によって、視認性の悪いと感じられる部分があったため、次の発表では気を付けたい。

（※文責: 原健宏）

参考文献

[1] 総務省 (2022). サイバーセキュリティって何？. https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/intro/intro_security.html. (2022/07/15 アクセス).

[2] 経済産業省 (2016). IT 人材の最新動向と将来推計に関する調査結果. https://www.meti.go.jp/shingikai/economy/daiyoji_sangyo_skill/pdf/001_s02_00.pdf. (2022/07/15 アクセス).

[3] vulc@n of DDTek. A history of Capture the Flag at DEF CON. https://defcon.org/html/links/dc-ctf-history.html. (2022/07/20 アクセス).

[4] tofu_cider 富士通クラウドテクノロジーズ (2021). 社内 CTF を開催しました. https://tech.fjct.fujitsu.com/entry/2021/12/06/094339. (2022/12/23 アクセス).

[5] 株式会社ラック 採用担当 (2017). 【2017 年】『即！西本面接』CTF による新卒採用キャンペーン！才能ある「あなた」をお待たせしません。. https://www.lac.co.jp/lacwatch/announce/20170418_001271.html. (2022/12/23 アクセス).