提出日 (Data) 2022/01/18

暗号とセキュリティ

Cryptography and Security
Project Final Report

中村 碧 Nakamura Aoi

1. 背景

1.1 プロジェクト全体

本プロジェクトは、暗号化技術用いて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。主に一昨年に感染拡大した COVID-19 の影響により、オンライン授業やリモートワークが増加した。世の中が PC などの IT 機器に触れる機会が社会の中で増加した反面、IT 機器を通した詐欺や悪質なソフトウェアに感染してしまう機会も増加した。そこで、個人情報を守る暗号技術や悪質なソフトウェアに感染しないための教育・セキュリティ対策が重要である。今年度、暗号とセキュリティはセキュリティ技術や悪質なソフトウェアの攻撃方法、暗号の仕組みを学び実装を試行する「暗号班」と、悪質なソフトウェアから自分自身を教育的な視点で対策と改善を目標にする「WEB 班」、そして、公立はこだて未来大学（以下、未来大）にセキュリティの実践的な講義が少ないことを背景に、セキュリティに関する実践的な問題を解いたり、作問を行う CTF にも挑戦する。

1.2 暗号班

SNS が発展した今日でも、メールを連絡手段するコミュニケーションは盛んにおこなわれている。友達や家族とは SNS で連絡をとり、企業との連絡や仕事はメールを使うという使い分けをしている人は一般的になってきた。私たち学生も教授と連絡を取る際は SNS ではなく学内で利用している Gmail を通して連絡する場合が多い。電子メールを利用していると SNS とは違ったセキュリティリスクが存在する。その中でも近年、様々な組織に被害を出している標的型攻撃メールという攻撃がある。これは、第三者が被害者の普段やり取りしている従業員や上司になりすまし、あたかも本人であるかのようなメールを送信し、被害者を悪質な WEB サイトに誘導したり、PC をウイルスに感染させる攻撃手法である。例として今年は（株）リケンが標的型攻撃の被害を受けており、従業員の住所や氏名、電話番号、顔写真など６０００件の個人情報が流出し、顧客の取引データ６０件が流出している。また、今年の３月にはトヨタ自動車系の部品メーカーである（株）デンソーも今年の３月に標的型攻撃によって身代金の要求をされている。今年も猛威を振るっている標的型攻撃メールであるが、対策として電子メールに電子署名を付けることで送信者の身元を証明することができ、標的型攻撃メールの被害を回避することができる。また、電子署名はメール本文の改ざん防止にもつながるので標的型攻撃メールの対策をしつつ、通信中に悪意のあるリンクをメール本文に埋め込まれることも防止することが可能だ。この技術は標的型攻撃メールに対して大変有効であるが、広く普及しているわけではない。メールに電子署名を添付する既存の技術として S/MIME がある。しかし、S/MIME はその導入の障壁の高さから十分に普及しておらず、被害防止の効果を十分に発揮できていない。よって、暗号班では、メールを技術的に安全な連絡手段とするため、実現するための技術や仕組みを学び、実装することを方針として活動した。

1.3 WEB 班

COVID-19 が流行する以前から IT 技術を利用する人の数は増えていたが、流行後はオンライン授業やオンラインで自宅にいながら仕事をする人が劇的に増えた。IT 機器を利用することは、業務の効率化や状況に合わせた働き方が増えていくため便利になるが、一方で、正しい知識を身に着けていないと予期していないところで詐欺にあったり、個人情報を悪意のある人に取得されてしまう恐れがある。未来大生にも、入学したばかりで始めて PC を触る人や高校の時の授業で少しだけ触ったことがある人が存在する。悪意のある第三者から攻撃被害にあわないためには、正しい知識を身に着ける機会が必要であるが、未来大学の講義だけでは、すべてのリスクを理解して対策するのは難しい。そこで、スマホからアクセスできて手軽に読める WEB サイトを作成する。WEB サイトには、「自分が使用している PC がランサムウェアに感染してしまう疑似体験」と「クイズに答えていくだけで、ネット上の危機から身を守ることができる」2 つの機能を作成し、この WEB サイトを閲覧するだけでネット上の危機を体験と学習をすることができるとし、WEB サイト作成に着手した。WEB サイト作成にあたって「情報セキュリティ１０大脅威　２０２２」[1] を参考にクイズページを作ることで、正しい知識を身に着けることができると考える。

1.4 CTF 班

未来大学は情報工学の基本的なことを学びながら、各学科、コースに合わせたカリキュラムが組まれており、学生はカリキュラムに沿った必修科目と興味に合わせて選択できる科目があり、自分の好きに合わせて学ぶことができる。しかしながら、学んだ知識や技術を実験という名目で活かすことができる機会は少なく、特にセキュリティに関しては、実験を通してセキュリティの重要性を理解したり、暗号化技術を実装する機会はさらに少ない。そういった状況の中、未来大生の IT 企業の就職率は高いため、大学でセキュリティについての実戦経験をあまりできずに卒業してしまう場合がある。そこで、私たちは CTF（Catch The Flag）を通して、未来大生にセキュリティ意識の改善と実践経験の両方を獲得できる機会になるのではないかと考えた。そも

そも、CTF とは情報セキュリティスキルを競い合うコンテストのことで、情報セキュリティのスキルを用いて問題の中から Flag を見つけ出し、得点を稼ぐ競技だ。本プロジェクトでは、CTF の競技性を低くし、初学者でも遊びやすいよう改善した CTF を未来大生に体験してもらうことで、未来大生のセキュリティ意識改善と、情報セキュリティインシデントの対応能力向上に挑戦する。

2. 課題の設定と到達目標

まず、プロジェクト全体として昨年度の暗号とセキュリティのプロジェクト学習の活動の様子やプロジェクト報告書、グループ報告書を参考にし、メンバーの希望に合わせて班分けを行った。その結果、前年通りメールについての課題を解決する「暗号班」、教育的な観点からセキュリティ意識改善に努める「WEB 班」、そして今年は CTF を通して未来大生のセキュリティ技術向上と意識改善を行う「ＣＴＦ班」の 3 つに分かれて活動を行った。これらの活動は各グループリーダーが課題と到達目標をより詳しく決め、それぞれの班で課題解決に向けて活動を始めた。

2.1 暗号班

背景で述べたように、標的型攻撃の被害は大きなものである。よって、我々はメールによる標的型攻撃の被害の大きさを課題とし、この被害の軽減を目指すこととした。背景でも述べた実例のように、標的型攻撃ではなりすましが行われることが多い。よって、この被害を軽減するためには、メールによるなりすましを防止する必要があると考えた。このためにはメールへの電子署名の付与が現実的な手法である。しかし、背景でも述べたように既存の、電子署名を付与する技術の S/MIME は十分な効果を発揮できていない。よって我々はより導入障壁が低い形での電子署名の付与システムを開発することを目標とした。これによってメールによるなりすましを防止し、標的型攻撃の被害軽減を実現できると考えた。

2.2 WEB 班

課題として未来大学の講義だけでは、すべてのセキュリティインシデントを理解し、対策できない。よって、未来大生の現状のセキュリティ意識を課題とし、私たちは WEB サイトを通して教育的な観点から未来大生のセキュリティ意識改善に取り組んでいくことを目標とした。目標を達成するために、前期では主にどのような知識や情報が必要か、どのような言語を学習するのか方向性を決めた。次に後期では、WEB サイトのメイン機能である「クイズページ」と「ランサムウェア感染の疑似体験ページ」を作成することで問題解決のための作業に着手した。まずクイズページの作成手順は具体的には以下の手順で活動を行った。

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

つづいて、サイバー攻撃疑似体験ページについての具体的な作成手順は以下の通りである。

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。

課題: 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。

課題: 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。

課題: 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。

課題: 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成
ランサムウェアの対策について調べる。
8. GitHub に移行、実装
GitHub 用に調整をする。

2.3 CTF 班

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。

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着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。

到達目標として、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ことを意識し、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。さらに、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ととした。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ことを到達目標としている。

3. 課題解決のプロセスとその結果

3.1 暗号班

先ほど述べた「より導入障壁が低い形での電子署名の付与システムを開発する」という目標を達成するため、我々は ID ベース暗号を用いた電子署名をメールに付与するシステムの開発を行うということを、課題解決の手法として定めた。ID ベース暗号においては、公開鍵を ID 等の既知の情報とする。このことから、ID ベース暗号を用いた電子署名では、既存の暗号方式による電子署名の検証で必要であった、認証局からの公開鍵の入手が不必要となる。このことから、システムの導入障壁を低下させることが可能となると考え、この手法を採用した。実装として、我々は当初 Chrome 拡張機能としてこのシステムを完成させることを目指した。なぜなら Chrome 拡張機能であれば導入が容易なのであると考えたからだ。しかし、Chrome 拡張機能からではメールの本文の内容の認識や、メールへの電子署名の付与に支障があった。よって GAS(Google Apps Script) を併用する形での作成に変更した。上記のような経緯で、Chrome 拡張機能と GAS を併用したメールへの電子署名の付与と検証の機能を持ったシステムを作成した。この成果物は ID ベース暗号を用いた電子署名の有用性を示すことができたと考えている。

3.2 WEB 班

背景で述べた未来大生のセキュリティ意識を向上させるために 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 [1] から具体的なサイバー犯罪の事例を参考に作成した。サイトのないようとしては、クイズが１０問用意されており、1 問ず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こと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できる 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・対応を知ることができるようになっている。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あわせることによりセキュリティ知識が深まるよう制作した。

3.3 CTF 班

問題提起で述べた「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、具体的な解決策として、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し、活動を行った。Web サイト作成にあたって当初はサーバを契約することで、CTF サイトにログイン機能や特典表示機能を実装し、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問題点があるため、サーバーレスの構成を実現した。また、CTF サイトの問題作成に当たって、AWS を利用して SQL インジェクションを用いた問題を作成した。これは、当初予定していた Web ジャンルの問題を作成途中に、理想的なサーバー環境を構築することが叶わなかったため、断念したからである。そして、Web サイトのデザインは 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いため、実際に参加したときのギャップを埋めるべく、CTF サイトのデザインでは、CTF 参加者が楽しめるように映画「マトリックス」をオマージュした文字が上から下へながれていくデザインを採用した。

4. 今後の課題

4.1 暗号班

今回の成果物は、GAS と Chrome 拡張機能を使用した代償として、Gmail 上でのみ動作するものとなった。この制約は実際の普及において大きな問題となると思われる。今後の課題としてはユーザーのメールサーバーや利用サービスにとらわれない形への改良が必要であると考えている。また、機能の開発に当初の予定以上の期間を使ってしまい、ユーザーインターフェースの配慮が疎かとなった。ユーザーがより使いやすいソフトウェアとすることも今後の課題である。

4.2 WEB 班

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と考える。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ように制作した。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。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。

4.3 CTF 班

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。

参考文献

[1] IPA。 情報セキュリティ１０大脅威、 2022。