暗号とセキュリティ
プロジェクト報告書

Cyrptography and Security

今井 徹雄 Tetsuo Imai

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。今年度は、セキュリティ技術に攻撃手法や暗号の仕組み等について学習し、より効果的な暗号方式の利活用について検証する「メール班」と、ユーザのセキュリティ意識の把握と改善を目標とする「Web 班」に分かれて活動した。

1.2. メール班

今日では IT 技術の進歩や新型コロナウイルスの蔓延に伴って電子メールを用いて会話や書類のやり取りをする場面が増加した。しかし、電子メールには多くの危険が存在している。例えば、送信者と受信者の間に悪意のある第三者が割り込み、なりすましや電子メールの改ざんを行うことで悪意のあるテキストや危険性のあるファイルを送りつけると行ったことが挙げられる。この危険性の対策手段として電子署名がある。これを使用することでデータの改竄となりすましを検知することが出来る。しかし、あまり普及されていないのが現状である。メール班ではこれを背景として、安全かつ簡単にメールのやり取りを行うための技術や仕組みなどの対策手法の検証を主として活動を開始した。

1.3. Web 班

Web サイトを見て貰うことで、未来大生のセキュリティ意識を向上させることを目的とした。IPA の調査を参考にした結果、「サイバー攻撃に関する知識が少ない」と「セキュリティに関して考える機会が少ない」ことが問題であるとし、セキュリティに関しての知識と考える機会を提供する「サイバー攻撃疑似体験」と「自分に適したセキュリティソフトを推奨するクイズ」の機能を Web ページで実装することとした。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。到達目標は、この Web ページの完成である。

2. 課題の設定と到達目標

初めに昨年度の暗号とセキュリティプロジェクトの発表用スライドや製作物、報告書の内容を認識し、「今年度におけるセキュリティ問題の変化」や「昨年のプロジェクトでは何が問題であったか」を考えることを課題として設定し、1.1 でも述べたような背景からどのような問題解決の方法があるかを到達目標として活動した。この活動から 2 つの班に各人の希望でメンバーを分け、それぞれの班でより詳しく課題と到達目標を設定して活動を開始した。

2.1. メール班

メール班では、安全かつ簡単にメールのやり取りをするため、高機能暗号の実装を通してこれによる結果と課題を検証することを目的とした。高機能暗号とは通常の暗号技術に加えて高度な機能を付加したもののことを言う。これは不特定多数が受信することを前提に構成されており、クラウド環境などの複雑な通信環境やユーザのプライバシー保護などの高度な安全性に対応して暗号化を行うことが出来る。高機能暗号には様々な種類があり、今回は ID ベース暗号とタイムリリース暗号に注目した。

ID ベース暗号とは 2001 年に提案された [1] 公開鍵暗号方式の一種であり、これは通常の暗号技術に対して ID という個人を特定できるような要素を公開鍵として用いるものである。これは学内メールシステムのような狭い組織であるほど安全性を保ちやすい。加えて公開鍵証明が不要なことから、これを用いた電子署名によりコストやや機能対応に対する問題点が解消されると考えられる。三浦 (2020)[2] はこの ID ベース暗号に関する鍵生成・電子署名の安全性

及び正当性についての検証を行った。

タイムリリース暗号とは 1993 年に初めて議論されて以降多くの研究が行われている [3][4] 公開鍵暗号方式の一種であり、これは通常の暗号技術に対して時間の要素を付加したものである。これによって指定された時刻以前は復号できないことを保証することができ、受信者は復号時刻になると初めて情報を見ることが出来る。また ID ベース暗号と多くの共通点があり、応用が可能となっている。菅原 (2021)[5] はこのタイムリリース暗号に関する鍵生成の正当性についての検証を行った。

これら 2 つの暗号技術に関する研究は存在するものの実装例が少なく、実際にこれらを実装するのにどのようなシステム・技術が必要なのか、どのような問題が発生するのか、どのような方法・仕様で実現できるのかといった点が明らかになっていないと考え課題とし、実際に実装してこれらを検証することを到達目標とした。

2.2. Web 班

課題を解決するために、前期では主に、どのような知識や情報、対策が必要なのかを考え方向性を決定。後期では、Web サイトのメイン機能を作成することで問題解決を行った。具体的に以下のような手順で活動した。

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. プログラミングの学習と Web ページ作成 Web ページ作成のために必要な、html と css の学習を学習サイト Progate を用いておこなった。また、これから作る Web ページの基礎となる部分や、機能の一部を実装した。

3. 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。

4. 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。

5.IPA 調査の考察
アンケートだけでは情報が不十分と考え、IPA（情報処理推進機構）の「2020 年度情報セキュリティの脅威に対する意識調査」報告書 [6] を参考に、掲載する情報などを吟味した。

6.Web ページの作成とレイアウトの調整をおこなった。

IPA 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 、課題設定・到達目標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 ページの作成を行った。

3. 課題解決のプロセスとその結果

3.1. メール班

前述した通り、ID ベース暗号やタイムリリース暗号、加えて電子署名は実用例が少なく、あまり普及していない。これにより、実装した際に必要な技術や問題が何であるか明らかになっていないとし、実際に実装して検証することでこれらの技術の導入・運用がしやすいのではないかと考えた。議論の結果、ID ベース署名、ID ベース暗号によるファイル暗号化、タイムリリース暗号によるファイル暗号化の 3 つの機能を実装し検証を行うこととした。

前期の活動では、知識の習得・定着を中心に行った。プロジェクト教員による講義を行っていただき、班のメンバー全体に対して基礎知識の習得から、鍵生成局や今回関わる高機能暗号などの応用的な知識の習得を中心に行い、また講義後に内容の確認を行い知識の定着に対しても活動を行った。講義による知識の習得後、議論の結果、今回実装するシステムに向けてクライアント班とサーバ班へさらにメンバーを分け活動を行った。クライアント班は実際に暗号化部分の処理を実装する必要があることから、知識の定着の一貫として各メンバーでそれぞれ任意の言語を用いて暗号技術を実装することを後期開始までの課題として活動した。サーバ班は Firebase などの認証機能やサーバに関しての知識の習得が必要と考え、必要技術の調査を継続的に行った。

後期の活動では本格的にメールシステムの実装を開始した。ID ベース暗号とタイムリリース暗号に関する文献が学内メールシステムについてである

点、比較的小規模である点から、公立はこだて未来大学で実際に用いられている学内メールシステムに対して機能実装をすることとした。また議論の結果、Google Chrome の拡張機能を用いて実装することで容易に実装でき、かつ有効に課題の検証が可能であり、これを実装方針とした。その後、活動によってすべて有効に実装することができた。ID ベース署名はメール送信の本文の末尾に付加する形で送信し、受信者は付加された署名を元に検証することができる。ID ベース暗号によるファイル暗号化は拡張機能によって付加された場所にファイルを添付することで暗号化されたファイルをダウンロードすることが出来る。タイムリリース暗号によるファイル暗号化は復号時刻を指定した上で同様に拡張機能によって付加された場所にファイルを添付することで暗号化されたファイルをダウンロードすることが出来、受信者は指定した時刻以降のみ復号することが可能となる。なお、ID ベース暗号に関する機能はすべて事前にユーザを登録・認証をする必要がある。また、これらの機能を実装するためには鍵生成局や認証局が必要であり、そのシステムを図 1 と図 2 に示す。

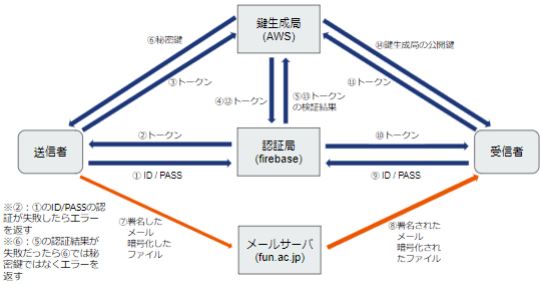

図 1　ID ベース暗号に関するシステム構成

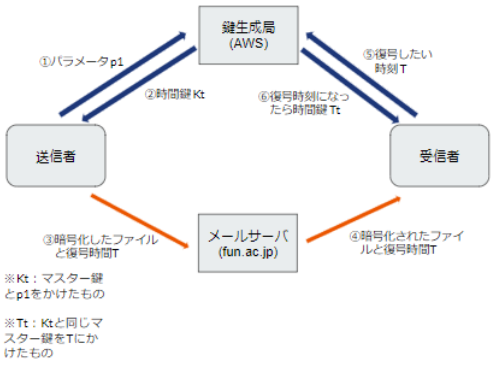

図 2　タイムリリース暗号に関するシステム構成

3.2. Web 班

目標としていた Web サイトが完成した。具体的には以下のページである。

1.Top ページ
2. サイバー攻撃疑似体験ページ
3. 疑似体験の振り返りページ
4. ウイルス感染とその対策ページ
5. 自分にあったセキュリティソフトページ

上記の 2 番と 3 番が疑似体験班の Web ページ、4 番と 5 番がクイズ班の Web ページとなっている。また、それぞれの班のページには Top ページからアクセスできる。

「Top ページ」には、参考にしたアンケート調査、Web ページの概要、成果物の情報、Web ページ作成班の活動内容について掲載される。

「サイバー攻撃疑似体験ページ」では、メールによるフィッシング詐欺を再現しており、そこで行った行動によって、どのような情報が盗まれたのかを提示する。その後、「疑似体験の振り返りページ」にて、フィッシング詐欺の対策やその他のサイバー攻撃について学ぶことができる。

「ウイルス感染とその対策ページ」では、コンピュータウイルスについての情報や、個人でできるセキュリティの向上方法について掲載している。

「自分にあったセキュリティソフトページ」では、自分の環境や考え方に合ったセキュリティソフトを、計 6 種の中から提示される。

4. 課題と展望

4.1. メール班

前述した通り実際に学内メールシステムに対して該当の暗号技術を実装後、メンバーで問題点やそれに対する対処、または展望に対する議論を行った。次から述べるのはその内容である。

実装の容易さという観点から Google Chrome の拡張機能を用いて実装したが、拡張機能ならではの問題があった。当初はメール送信画面にファイルを直接添付した際に直接拡張機能によってファイルを暗号化して、その暗号化したファイルを添付することを想定していたが、拡張機能の特性上難しいことが判明した。今回の実装では実装方針を 3.1 で示したとおりに変更することで対処した。この点に関して、実際に新しくメールシステムを構築する際はメールの添付処理自体にこの暗号化処理を施すことで実装することが可能であるため、この問題は対処可能であると考える。

今回サーバ側において SSL 証明書やドメインを無

料のものを使用しており、この点において実用的ではないという問題点はある。しかし、有料のものと無料のものではセキュリティ的な暗号強度は違いがないものの、有効期限やサポートといった観点において優位性があるため、実際は有料のものを使用することでより安全なサービス運用ができるのではないかと考える。

加えて、今回内部動作の実装を目的としていたため、ユーザ視点でどのような利点があるのか分かりづらいという意見が出た。これに関して、暗号技術もといセキュリティ技術はユーザが安心してメールやファイル送信が出来るようになることが目標であるため、今後ユーザ視点での暗号技術を考えることも重要なのではないかと考えられる。

4.2. Web 班

目標としていた「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」を Web ページに実装することができた。成果発表の制作物に関するコメントには、「面白い」というコメントが複数あったため、特に「セキュリティに関して興味を持って貰う」という目標は達成できただろう。しかし、作成した Web ページがどのように未来大生に検証を与えるのかという検証を行えていない。そのため、実際に被験者に Web ページを利用してもらい、データを取るなどして効果を検証する必要があるだろう。

また、我々がおこなったセキュリティ意識調査アンケートは、サンプル数が少ないため考察する根拠としては不十分であった。理由として、コロナ渦の影響で、学内でのアンケート収集ができなかったことが挙げられる。

そのため、IPA の男女 10 代と 20 代のアンケートで代用し、セキュリティ意識について考察したが、未来大生を対象とした Web ページを作る上で、IPA の調査を用いるのはややデータとして広すぎるため、目標設定の際、事実より考察の部分が多くなってしまった。やはり未来大生に直接アンケートを取り、データを参考にするのが良いだろう。ついては、学内にて直接アンケート活動をすることで、今回よりも効果的にアンケートのサンプルを集めることができるだろう。この方法を用いて再度アンケートをとり、未来大生のセキュリティ意識向上にはなにが必要なのか、また、未来大生には何が足りていないのかを考察し直す必要があると考えられる。

参考文献

[1]D. Bonoh and M. Franklin, Identity-based encryption from the Weil pairing. In: Annual international cryptology conference. LNCS 2139, Springer, Berlin, Heidelberg, pp. 213- 229, 2001.

[2] 三浦幸泰, ID ベース暗号の学内向けメールシステムの鍵生成, 公立はこだて未来大学 卒業論文, 2020.

[3]K. Chalkias and G. Stephanides, Timed release cryptography from bilinear pairings using hash chains, CMS 2006, LNCS 4237, pp. 130-140, 2006.

[4] 笠松宏平, 松田隆宏, 江村恵太 花岡悟一郎, 今井秀樹, フォワード安全暗号を用いたタイムリリース暗号の一般的構成の安全性証明, コンピュータセキュリティシンポジウム 2011, 2011.

[5] 菅原健斗, タイムリリース暗号を用いた学内向けメールシステムの鍵生成, 公立はこだて未来大学 卒業論文, 2021.

[6]IPA, 「2020 年度情報セキュリティに対する意識調査【倫理編】【脅威編】」報告書, IPA 情報処理推進機構, 2021, https://www.ipa.go.jp/security/economics/ishikichousa2020.html, (参照 2022-01-05).