暗号とセキュリティ

Cryptography and security

酒井　竜馬　Ryoma Sakai

1. 背景

本プロジェクトは、主に暗号化技術を用いて、セキュリティに関する分野について理解を深め、実際に体験することを目的としたプロジェクトである。今年度は新型コロナウイルスの影響によるオンライン授業やリモートワークの増加に伴い、情報の管理がより一層重要なものとなった。ここで大切になってくるのが、情報を管理するセキュリティ技術やそれを扱う我々ユーザの危機管理である。そこで今年度の活動は、セキュリティの脆弱性をついた攻撃手法や現在の対策等について学習し、メンバを 2 つの班に分け、それぞれを「メールアドオン班」、「セキュリティ意識調査班」理解を深めるとともに、より効果的な対策手法の提案や意識喚起を最終目標として活動した。

昨今では IT 技術の進歩に伴って、他者との会話や重要な書類の送付を電子メールのやりとりによって行う場面が多くなった。電子メールを利用すると当然移動の負担や遠距離の人との意思の疎通・情報の共有が図りやすい。しかしその反面、第三者がなりすましを行い、これらの情報の盗聴や改ざんに遭う被害が増加している。このような攻撃は標的型攻撃(APT)と呼ばれ、「組織」向けの脅威が毎年第 1 位であることがわかっている。対策として、一般の利用者に対しては電子メールに安易にファイルの添付をしないような呼びかけや、企業に対しては社員や職員に向けた標的型攻撃に対する訓練を行う人的対策、電子メールの認証機構や電子署名を利用することで攻撃を防止している。しかし、対策により生じる利便性の低下、ヒューマンエラー、導入・運用コストの高さなどから、標的型攻撃による被害は増える一方であり完全には対応できていないのが現状である。メールアドオン班ではこれらを背景として効果的な対策手法の提案を主として活動を開始した。

新型コロナウイルスによる授業や会議のオンライン化により Zoom などのオンラインアプリケーションが注目され始めたが、それと同時に当初はセキュリティに関する問題が発生していた。 今は改善されてきてはいるが、こういった社会情勢の変化から今後もリモートワークやオンラインを使ったコンテンツのニーズが高まってくる。その一方で、セキュリティに関しての知識や意識を持たない多くのユーザが、悪意のあるユーザによって、個人情報などが知らず知らずのにうちに流失してしまったという事例も多くある。これらのことから、今後、各人のセキュリティの知識の習得や対策に意識を向ける必要がある。セキュリティ意識調査班では、これらを背景に知識の習得、啓発を主として活動を開始した。

2. 課題の設定と到達目標

初めは、安全なメールシステムをテーマとした昨年度の卒業研究[2]の発表用スライドを、誰でもわかりやすいように改善していく、という活動を行なった。講義で学んだ程度の知識しか持っていなかったため、「自分たちが卒業生の研究内容をしっかりと理解すること」「スライドなのでより見やすいレイアウト・配色・図・表現を用いてわかりやすいものを作る」という 2 点を当初の課題として設定した。到達目標としては、中間発表や最終発表の際に、閲覧してくれた方に内容を正しく伝えられることを目標とした。それらの活動の中で、本年度の活動として活動内容を 2 つ選出してそれぞれグループを分け、それぞれ課題・到達目標を設定し、活動を開始した。

2.1 メールアドオン班

メールアドオン班は、標的型攻撃を防ぐことができる安全な学内メールシステムを構築しようと考え、

2001 年の文献［1］によって提案された公開鍵暗号方式の一種である ID ベース暗号(IBE)を用いた過去の文献[2]をさらに進めることを目的とした。理由として、背景の電子署名が普及していない理由「コストが高い」「相手のメールアドレスが電子署名に対応しているか不明」に着目し、電子署名が導入されていないことで標的型攻撃の対策が十分になされていないことを問題として設定した。同卒業生の研究では、メールシステムの実装までは至っていなかったため、何らかの方法で実装することを目標とした。ID ベース暗号は学内メールシステム等の狭い組織間であれば安全性を保つのに適しているといった特徴を持ち、ID ベース暗号を用いた電子署名により、従来の電子署名の煩雑さを解消することができると考えられる。文献[1]やその参考文献では、ID ベース暗号による鍵生成及び電子署名の正当性や安全性についての検証が行われていた。ここで課題となるのが、ID ベース暗号の実装方法である。どのような方法・仕様で ID ベース暗号の機能を搭載したメールシステムを実現するのかが一番の課題であった。

2.2 セキュリティ意識調査班

セキュリティ意識調査班は、本大学の学生がセキュリティ対策の意識が低いのではないかという課題を仮説として立てたのち、アンケート調査を行い、結果から課題点を考察し、本大学の学生及び一般の方のセキュリティ意識の向上や知識の習得を目的とした web ページの作成を目標とした。

インターネットを利用するにあたり、セキュリティ意識を持って利用するのはとても重要なことである。しかし、一口にセキュリティ意識と言ってもその範囲はとても広い。IT に関わる人とそうでない人の違いだけでも相当な幅になるだろう。ここで、一つの指標として IPA の「2019 年度情報セキュリティに対する意識調査」に基づいたアンケートを実施した。IPA とは Information-technology Promotion Agency の略で日本語では独立行政法人情報処理推進機構というものである。 その結果から、目標達成のため身近な話題で理解しやすく、正しい知識を身につけることで役立つ場面が多いと予想される「セキュリティソフト」「インターネット詐欺」の２つに着目し、それらに関する知識の習得及び意識の向上を目標として環境を整えることとした。

3. 課題解決のプロセスとその結果

3.1 メールアドオン班

上記の通り、標的型攻撃の対策の主なものに電子署名が存在するが、高いコストなどからあまり普及していないのかが現状である。そこで、どのように改善すれば電子署名を普及させることができるのか、議論した結果、原因であるコストを減らすことができれば導入・運用がしやすいのではないかと考えた。また、利用する組織が増えることで、対応するメールシステムの増加にもつながるのではないかと考えた。その後、どのような手段で電子署名のコストを減らすことができるかを議論した結果、暗号化技術を学ぶために並行して行なっていた文献[2]発表資料の修正の活動から着想を得て、ID ベース暗号を用いることでコストを減らすことができると考えた。

前期の活動では、課題であった実装方法について、オープンソースソフトウェアを用いて、既存のメールクライアントソフトに ID ベース暗号の機能を追加して実装することとなった。夏季休暇中に暗号化、復号、電子署名の各プログラムを記述し、後期初めに実装を試みたが、予想していた結果・挙動を得ることができなかった。ここで起きていた問題がソフトの対応している環境によるものであった。この問題については、今回の活動期間で修正するのは不可能と判断し、この実装方法を放棄、代替案による解決を行うこととした。いくつか案を出し合い、最終的には本学内で使用している Web メールについて、利用しているブラウザの拡張機能として ID ベース暗号を実装することとした。これにより OS による実装方法の違いや、挙動の不備を軽減できるとした。その後、後期の活動によって実装できたのは Google Chrome の拡張機能のみとなってしまったが、Chrome 上では ID ベース暗号を利用した署名の検証、添付ファイルの暗号化と復号を実現することができた。また、学内メール利用時の認証が

利用できないため別の認証基盤を利用した。これによって、従来の電子署名同様に送信者と受信者がどちらも正しく本人であることの証明が可能となった。

3.2 セキュリティ意識調査班

セキュリティについての意識向上を目的として調査を行い、結果から「セキュリティソフト」と「インターネット詐欺」の二つを主な課題として設定した。セキュリティソフトに関しては、知識を広め、意識の向上を図るためには、本グループのメンバがそれぞれしっかりとした理解が必要になる。しかし、使用したことのないセキュリティソフトの詳細を、他人に教示できるレベルで知ることは難しく、インターネット上にある情報のみでは他のまとめサイトとの差別化が図れないため、実際に入手して使用感、使用した際の不具合などを確かめてみることにした。グループメンバが 6 人それぞれ 1 種類ずつ使用できるよう、グループ内で協議して代表的な 6 つを選出した。

インターネット詐欺については、事実として過去 5 年間で検挙数が 1.2 倍以上に増加している。身近にインターネットが普及してきたこともあり、その手口もさまざまである。また、詐欺というのはその手口、手法をあらかじめ認識しておくことで、個人の裁量で回避することが可能である。自分が引っかかるわけがない、といった意識をなるべく減らすことがとても重要になる。

以上のことから、「セキュリティソフト」「インターネット詐欺」についての知識を発信し、身につけてもらうための手段として、Web サイトを作成するという方法を採用した。理由としては、先述のアンケート結果などが掲載しやすく、比較しやすい点や、セキュリティソフトとインターネット詐欺の項目の切り替えがクリックひとつで行えるという使いやすさが適していると考えたからである。また、操作の説明をせずとも閲覧するユーザが直感的に操作できる点、作成する際に学習方法や解説書が豊富であるため学習環境を整えやすい点も選択した理由の一つである。具体的なコードの記述に際しては、メンバは HTML 等の Web 制作に関する知識が乏しかったため、プログラミング学習サイトや web 上の知識、過去の講義などを参考にして、前半の活動は知識の習得に時間を費やした。エディタはオープンソースで共同編集が行える Atom を採用し、メンバ同士わからない点を教えあったり、コミュニケーションを取りながら作業を分担する際の効率化を図った。

次に、重要になってくるのが Web サイトのレイアウトである。本グループは、セキュリティソフトやインターネット詐欺という事例に対して、web サイトの閲覧に不慣れな高齢者の方や、小さい子供でも利用しやすいように、シンプルで直感的な操作を後押しするようなデザインを目指した。本グループにはデザインコースの学生がいないため、テーマに沿ったサイトを共有しながら、どのようにすればシンプルでわかりやすいレイアウト・デザインになるか意見を出し合った。その際、シンプルでわかりやすい自分たちが目指すものに近しいサイトには、いくつかの共通点があることを発見した。画面上部にヘッダー、画面下部にフッターがあり、各項目を見やすいように配置しているなどが挙げられた。それらの点を元にしてレイアウトを作成した。加えて、強調したい文章や言葉を太文字にしたり、色を変えるなどできるだけ見やすくなるような工夫をした。

Web サイト上の具体的な文章、内容について、セキュリティソフトに関しては各ソフト間の比較がしやすいように、無料試用期間や一つのライセンスでインストール可能な台数など、掲載する情報、項目は可能な限り類似したものを記載するようにした。専門用語を多用した比較サイトが多く見受けられたため、それらを細かく、知識のない人でも理解できるように噛み砕いた説明になるように意識した。また、実際に使用したメンバの評価を、「性能的にこの値段が妥当だと思うか」など具体的なポイントを 4 つ指定しそれらの評価、使用環境、導入したデバイスなどを記載し再現性を持たせるような工夫をした。インターネット詐欺に関しては、詐欺の種類、特徴、手口、被害に遭う人の傾向などをそれぞれまとめた。

そしてゲーム感覚で自分のセキュリティ意識を図ることができるとし、サイト内に Web アプリケーシ

ョンを作成した。これは、前述の調査の際に行なったアンケートを、Web サイトを閲覧した人にも答えてもらい、結果をすぐに表示することで、自分のセキュリティ意識について知ってもらおうというものである。

4. 今後の課題

4.1 メールアドオン班

現状では、動作環境が Chrome のみとなっているため実用的と呼べるレベルには至っていない。そのため、対応するブラウザを拡張することやスマートフォンでの利用を想定した改善が必要であると考えられる。そして UI に関しても、ユーザの利用を促進するために、検証が失敗した際の警告や処理、拡張機能利用時の画面などにあまり力を入れることができなかった。そのため、危機感を感じさせるような通知や、安全性を感じさせるデザインなどを工夫して、仕組み以上に安全性を向上させる必要があると考えられる。また、鍵生成サーバーにそれぞれのユーザが秘密鍵を要求しなければ、このサービスを利用することができない。たとえ、通信経路を暗号化して、秘密鍵をそれぞれのユーザに転送できたとしても、不安点は残る。そこで、学生証に秘密鍵を埋め込み、入学時にその学生証手渡しで渡すことによって、安全に本人へ秘密鍵を配布することが可能である。学生証が難しいとしても、FeliCa カード等に鍵情報を埋め込み、実際に配布することができると考えられる。

そして、今回は活動計画や期間との兼ね合いもありブラウザの拡張機能としての実装となったが、本来目標としていた Web メール以外のメールクライアントソフトに ID ベース暗号を用いた暗号化、復号、電子署名の機能を実装できたらと思う。この解決策としては、アーキテクチャに対応したライブラリの選定、あるいは作成が必要であると思われる。

4.2 セキュリティ意識調査班

前期の活動では、IPA の「2019 年度情報セキュリティに対する意識調査」を参考に、未来大生を対象としたセキュリティ意識に対するアンケートを行い、未来大生のセキュリティ意識の現状を調査した。その結果から、未来大生のセキュリティ意識やセキュリティに関する知識が低い傾向にあることがわかった。そこで、未来大生のセキュリティ意識の向上やセキュリティに関する知識を深めるため、セキュリティに関する詐欺手口をまとめた Web サイトを作成した。後期からは、前期に作成した Web サイトのレイアウトの改善やあまり知識の無い利用者にも理解しやすいよう、インターネット詐欺に関するクイズを作成し、そのクイズに使用する問題や図表などの作成も行った。またアンケート機能を実装した Web アプリケーションの開発を行った。今後は、学外の人へアンケートを実施し未来大生以外の人のセキュリティ意識の向上が見込める Web サイトを目指す。また、多様なデバイスへの対応や、利用しやすいインターフェースを追求することが必要である。

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.