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

暗号

Group Name

Cryptography

プロジェクト番号/Project No.

18-A

プロジェクトリーダ/Project Leader

中村碧　Nakamura Aoi

グループリーダ/Group Leader

東未来翔　Mikuto Azuma

グループメンバ/Group Member

東未来翔　Mikuto Azuma
中村碧　Aoi Nakamura
野澤真生　Masaki Nozawa
北山奏　Kanata Kitayama
青山慎太郎　Aoyama Shintaro
森谷史奏　Shion Moritani
岡本英太　Eita Okamoto

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

January 18, 2023

概要

本プロジェクトは, 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ものである. 近年は,IT 化が進み多くの個人や組織の情報をインターネット上で扱うようになり, セキュリティのリスクと重要度も増加している. そこで, 本グループは暗号技術の利活用を通して上記の問題の解決を目指した. 最終的には ID ベース暗号を応用した電子署名を用いて, メールによる標的型攻撃の被害漸減を目標として活動した. 具体的な成果物としては, 今年から学内メールシステムが Gmail に移行したため,Chrome 拡張機能と Google Apps Script を用いて学内メールシステムに電子署名機能を実装した.

キーワード　セキュリティ, ID ベース暗号, 電子署名, メール

（※文責: 岡本英太）

Abstract

The purpose of this project is to deepen understanding of security and to actually use and experience it. In recent years, with the advancement of IT, information of many individuals and organizations is handled over the Internet, and the risks and importance of security are increasing. Therefore, this group aimed to solve the above problems through the use of cryptography. The final goal of the project was to reduce the damage of targeted attacks by e-mail using digital signatures based on ID-based cryptography. As a specific deliverable, we implemented a digital signature function in the campus email system using a Chrome extension and Google Apps Script, since the email system has been migrated to Gmail this year.

Keyword Security, identity-based cryptography, digital signatures, email

（※文責: 岡本英太）

目次

第１章　背景

1.1　背景

主に一昨年からの COVIT-19 の流行により, 日本で仕事や生活の IT 化が進んでいる. 学校ではオンライン授業, 仕事はオンラインでできる環境や IT を利用する人がが増えた一方で, サイバー犯罪の検挙数やウイルスによる被害総額なども増加傾向にある. したがって今後,IT の発展とともにセキュリティインシデントは増加していくだろう. 中でも一般に多く利用されている電子メールは様々なセキュリティ上の問題を抱えている. 例えば, 標的型攻撃メールによる被害がある. 標的型攻撃メールとは対象の組織から重要な情報を盗むことを目的として, 組織の担当者が業務に関係するメールだと信じてしまうように巧妙に作り込まれたウイルス付きのメールのことである. 特定の組織を狙った標的型攻撃は昨今, 様々な企業が被害を受けている. 今年では（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 [1]. また, 今年度の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 [2]. 情報処理推進機構（IPA）の資料である「情報セキュリティ１０大脅威　２０２２」[3] では, 組織の１０大脅威として２位に標的型攻撃が位置付けられている.

さて, 標的型攻撃は一般に攻撃対象の組織に侵入する必要がある. その侵入方法としては以下の方法が報告されている.

（１）メールを経由する方法

これは事前調査で入手した社員・職員の名前・メールアドレス, 担当業務内容, メール通信相手などの情報を利用し, 日常的にやり取りを行っている相手に成りすますことで, マルウェアを仕込んだメールを受信させ感染させる方法である. 送信者名やメールアドレスが業務上の通信相手に成りすまされたメールや, 担当業務内容に即したメール内容など, 受信した社員・職員がなりすまされたメールであることを検知するのが難しいように工夫されている. しかも, 利用されるマルウェアは未公開のものである場合があり, 一般のウイルスチェックソフトでは検出できないものが多い.

（２）Web 参照を利用する方法

これは水飲み場攻撃と呼ばれることもある. これは比較的新しい標的型攻撃で, ターゲットが日常的に閲覧する Web サイトに不正プログラムを仕込み, ウイルスやマルウェアに感染させる方法である. 普段職員や従業員が利用しているページに脅威を仕込み, 対象者が参照する場合にのみ, マルウェアを送り込むなど, マルウェアの存在の発覚を遅らせるよう工夫されていることが多い.

（３）ソフトウェアの更新を利用する方法

攻撃対象の組織の社員・職員の業務内容から, 利用している可能性の高いソフトウェアの更新情報を装い, マルウェアを送り込む方法である.（１）（２）と同様にこちらの方法もマルウェアの発見が困難になるように作成されている場合が多い.

上記のような侵入方法がマルウェアの感染に使われているが, 特にメールを利用した標的型攻撃メールによる感染が非常に多いことが各種調査期間より報告されている. 例えば, トレンドマイクロ (株) の「国内標的型サイバー攻撃分析レポート 2016 年版」[4] によると,2015 年に行った標的型サイバー攻撃の調査において, 侵入のきっかけが標的型メールであると特定された事例が全体の

93 %と報告されている.

したがって, 標的型攻撃メールは早急に対策が必要であり, 現在では主に人的対策と技術的対策の 2 種類の対策が考えられている. 人的対策については,「WEB」グループが対策として様々な試行を行っているため, 私たち暗号グループは技術的対策を検討することとした.

技術的に標的型攻撃メールの被害を抑えるためには, メールの内容が送信者の意図したものであるかの確証が必要である. しかし, 私たちが日頃利用している Gmail にその機能はなく, 送信されたメールの内容が第三者に改ざんされた内容の可能性があることを受信者はわからないところが現状の課題である.

（※文責: 中村碧）

1.2 目的

本プロジェクトの目的は, メールを用いた標的型攻撃メールの被害を技術的に防ぐ機能を実装することである. 送られてきたメールに対して送信者を明確にし内容が改ざんされていないことを確かめることができれば, なりすまし防止の効果があるため標的型攻撃メールの被害を抑えることができると考える. 既存の技術として, 電子署名をメールに追加する技術に S/MIME（Secure / Multipurpose Internet Mail Extensions）があるが, いくつか問題点があるため ID ベース暗号を用いた電子署名（ID ベース署名）を実装することとした.ID ベース署名は学内メールシステムのような小規模なメールシステムにおいて, メールアドレスを公開鍵（ID）として設定する特性がある. したがって, 一般の暗号方式より公開鍵の取得が容易なことから, 有効に安全性を保ちやすいという特徴があり ID ベース署名を実装することで, 学内の誰から送られてきたのか明確にわかる機能を作ることができる. そして, 今回実装する ID ベース署名は学内で日頃利用しているメールシステムに実装することで効果があると考えた. そのため Gmail に実装することになるのだが,Gmail に機能として実装するためには Google 拡張機能として開発を行う必要がある. よって, 成果物は Google 拡張機能の仕様にしたがって開発を行うことになった.

また, 暗号化に必要な送信者の本文とメールアドレスを送信する前に取得する必要があるので,GAS（Google App Script）を用いて取得している. 本プロジェクトでは, こうしたメールシステムにおける標的型攻撃メール対策を, 暗号化技術を通して考え実装することを目指す.

（※文責: 中村碧）

1.3 従来の問題点

1.2 節で触れた S/MIME とは,1995 年に IETF により発表された MIME でカプセル化した電子メールの公開鍵方式による暗号化とデジタル署名に関する標準規格である.

S/MIME によりメールの暗号化とメールへの電子署名が可能になり, 機密情報の安全な通信やなりすまし対策を実現することができる. このように, 電子メールを使う上でのリスクを低減することができる S/MIME は標的型攻撃メールなど様々なリスクに大変有効である.

しかし, 現実では S/MIME の利用は広く普及し活用されている状況ではない. 現在では,COVID-19 の影響により, いままで顧客に紙の資料として渡していた機密性の高い資料を, 安全かつなりすましのリスクがないメールを顧客に送信するために利用されたり, そもそも顧客へのメールに電

子署名と安全性を付与したい企業が利用しているが, あくまで BtoC の場面だけに限定されており,BtoB の活用事例は少ない.

なぜ,S/MIME が BtoB の場面で広く利用されていないのか. それは S/MIME には３つの課題があるためである. まず, メールアドレス証明書発行費用の問題があげられる. メールアドレス証明書発行サービスを提供している業者の数は多く, 一般に利用されているが, 証明書の費用として 1 メールあたり数千円が必要となり, 設定の代行を行うとすると５万円以上の金額になる. そのため, 証明書発行の費用が一つのハードルになっていることは間違いないだろう. 次に,S/MIME 利用者である送受信者双方の設定の煩わしさである.S/MIME メールの送受信には, 通信相手のメールアドレス証明書の入手・管理が必要であるが, メールアドレス証明書の有効期間は１年〜３年と短い期間でしか利用できないため, 適宜最新版を入手し保管中のメールアドレス証明書の更新が必要である点も S/MIME を導入する際のハードルになっている. 最後に, 単独で S/MIME の導入・利用のための投資をしても, それだけでは投資に見合う効果が期待できないという点にある. 例えば「GMO インターネットグループ株式会社」が提供する S/MIME のライセンス料金は１年で 57,200 円となっており, 個人同士で利用するには費用対効果で見合ったメリットを享受できない. そのため,S/MIME は業務通信が多い大規模な組織で共通的に利用することによりはじめて大きな効果を期待できる技術である. したがって,S/MIME による電子署名の付与および, 暗号機能の追加は我々学生や個人で利用するにはデメリットが大きい.

また,S/MIME の暗号化機能についても課題がある. まず, 組織の機密情報漏洩防止が難しい点である. メール送信者が S/MIME の暗号化機能を利用した場合, メール受信者以外は復号できないため, 送信組織としては, 機密情報がメールに含まれていないかどうかのダブルチェックが難しくなる. 次に, 受信したメールのウイルスチェックが難しい点である. 受信したメールが S/MIME の暗号化機能により暗号化されている場合, 受信組織のメールサーバでの受信メールのウイルスチェックは難しくなってしまう. したがって,S/MIME という技術の利用する際のハードルと暗号化技術の問題点がいくつか確認されているため,S/MIME は広く普及されていない.

（※文責: 中村碧）

1.4 方針

1.2 節で述べた目的を達成するために,ID ベース暗号を用いた ID ベース署名を Google 拡張機能で実装することを実装方針とした. なぜなら, 既存の技術である S/MIME は 1.3 節で示した通り,「メールアドレス証明書発行費用の問題」と,「S/MIME 利用者である送受信者双方の設定のわずらわしさ」,「単独で S/MIME の導入・利用のための投資をしても見合う効果が期待できない問題」, 以上の３つの問題点と, 暗号機能の問題点である「組織の機密情報漏洩防止が難しい点」,「メールのウイルスチェックが難しくなる点」から私たちは S/MIME ではなく,ID ベース暗号を用いた電子署名を実装することとした. そもそも ID ベース暗号とは, メールアドレスや学籍番号といった自分を示すことができる識別子を公開鍵として暗号化する公開鍵暗号方式である. そして, この暗号化技術を用いた署名方式が ID ベース署名である.ID ベース暗号は S/MIME とは違い, 受信者側が公開鍵をもっているため, 鍵生成局から公開鍵を取得する必要がないのが利点である. そして, 実装する学内 Gmail は利用者の大半が学生であり, 利用しているメールアドレスには学籍番号等が使われているため, メールアドレスから個人との紐づけが容易である. 加えて, 小規模な学内 Gmail システムに対して Google Chrome 拡張機能を用いて実装することで, 簡単に Gmail から ID ベース暗

号を用いた電子署名を利用することができ, 電子メールに対する標的型攻撃メール対策という目的の達成が可能であると考えた.S/MIME のメールの内容の暗号化機能については Gmail にデフォルトで搭載されているため今回のプロジェクト学習では実装しないこととする. また,Gmail から本文の内容, 送信者のメールアドレス取得のため Google Apps Script（GAS）を使い,Google 拡張機能に実装することとする. これらの実装用件を満たしながら,Google Chrome 拡張機能に電子署名を実装することを方針とする.

（※文責: 中村碧）

第 2 章　プロジェクト方針に関する基礎知識

2.1　暗号

暗号とは, 通信文を一定の規則に則りほかの表現に変換し, 第三者が特別な知識なしに読み解けなくするものである. 暗号は, 一般に機密性, 完全性, 正当性のいずれか, またはその複数の性質を確保することを目的として用いられる.

機密性　正当な受信者以外が通信内容を知ることはできないという性質のことである. 機密性が確保された現代暗号の暗号方式では, 共通鍵暗号方式であれば共通鍵, 公開鍵暗号方式であれば秘密鍵を持つ者だけが暗号を復号し内容を知ることができる.

完全性　通信内容が, 送信者以外の認可されない者の手によって改竄されないという性質のことである. 完全性の確保には一般的に電子署名やメッセージ認証による改竄の検知が用いられる.

正当性　その送信元がなりすましではなく正当な送信元本人であるということを担保する性質である. 正当性の確保には電子署名をはじめとする認証が用いられる.

暗号はまず古典暗号と現代暗号に大別されている. 古典暗号とは暗号化や復号に鍵の概念が存在しない暗号である. 例えば, 少数しか知らない特殊な言語を用いたり, 本来の文字と別の文字を割り当てたりするものである. 現代暗号は暗号化や復号に鍵を用いる暗号である. 本書において暗号と記述した際は現代暗号を指す. 現代暗号には様々な方式が存在しており, 用途によってそれぞれの方式が採用されている. これらの現代暗号の暗号方式のほとんどは, 暗号化と復号に同じ鍵を使用する共通鍵暗号方式 (2.2.1) と, 暗号化と復号に異なる鍵を使用する公開鍵暗号方式 (2.2.2) に大別される.

（※文責: 東未来翔）

2.2　暗号方式

2.2.1　共通鍵暗号方式

共通鍵暗号方式とは, 暗号化と復号を同一の鍵を用いて行う方式である. 対称鍵暗号方式とも呼ばれる. 暗号化と復号時に使用する鍵が共通していることから, この方式で使用する鍵は共通鍵と呼ばれる. この方式は後述する公開鍵暗号方式 (2.2.2) に比べ暗号化及び復号に必要な処理が高速である. 共通鍵暗号方式においては, 共通鍵を保持するものは誰でも, その共通鍵での暗号化およびその共通鍵で暗号化された暗号の復号を行うことができる. この性質から受信者への鍵の受け渡しには注意が必要である. なぜなら, 共通鍵を第三者が手に入れた場合, 暗号の機密性が失われ内容が漏洩するるのはもちろんのこと, なりすましも可能となり正当性まで失われることになるからである. また, 共通暗号方式では受け渡し相手ごとに鍵を生成する必要が生じる. なぜなら, 相手ごとに鍵を生成せず使い回すと, 同じ鍵を使い回した全ての相手が同じ共通鍵を使うものに対して傍受となりすましが可能となるからである. この必要性から, 管理する鍵の数が相手の数だけ増加することとなり, 鍵管理の負担は大きなものとなる. 共通鍵暗号方式に分類される代表的な暗号として AES がある.AES はブロック暗号の一つであり,128bit のブロックごとに処理を行う. 鍵は 128bit, 192bit,

256bit の 3 つの長さを用いることができる. ブロック暗号と異なり,1bit 単位で処理を行う暗号をストリーム暗号と呼ぶ. これの代表例としては RC4 や ChaCha20 が挙げられる.

（※文責: 東未来翔）

2.2.2 公開鍵暗号方式

公開鍵暗号方式とは, 暗号化と復号で異なる鍵を使用する方式である. 暗号化に使用する鍵は, 一般に公開し使用されることから公開鍵と呼ばれる. 対して復号に用いられる鍵は受信者が隠匿することから秘密鍵と呼ばれる. この公開鍵と秘密鍵はペアで使用される. 公開鍵暗号は一般に下記の手順で用いられる.

1. 受信者は公開鍵と秘密鍵のペアを入手 (または生成) し公開鍵を公開する.
2. 送信者は公開された公開鍵を用いて本文を暗号化し受信者に送信する.
3. 受信者は秘密鍵を用いて暗号文を復号する.

公開鍵暗号方式においては, 複数の送信者が受信者が公開した同一の公開鍵を用いて暗号化を行うことができる. そのため共通鍵暗号方式とは異なり, 受信者は送信者ごとに鍵を用意する必要がなく, 鍵管理の負担が小さい. また, 鍵の受け渡しに伴う鍵の流出の問題も解決されている. なぜなら, 公開鍵は暗号化のみに用いるものであり, 公開しても問題ないからである. また, 漏洩が問題となる秘密鍵を持つのは受信者のみである. よって, 漏洩してはならない共通鍵を受信者と送信者の双方が持つ共通鍵暗号方式に比べて, 公開鍵暗号方式は漏洩の可能性が小さい. ただし, 公開鍵暗号方式は共通鍵暗号方式に比べて処理が遅いという特徴を持つ. また, 公開鍵が公開されていることから送信者がなりすましを行うことが可能である. この防止策として, 一般的に受信者は公開鍵の有効性を証明するための電子証明書を信頼できる第三者機関から発行するという仕組みが用いられる. 公開鍵暗号方式に分類される代表的な暗号として RSA がある.RSA とは, 桁数が大きい合成数の素因数分解が現実的な時間内で困難であることを安全性の根拠とした暗号である. 公開鍵暗号を応用し, 文書等に電子的な署名を付与する技術として電子署名がある.

（※文責: 東未来翔）

2.3 電子署名

電子署名とは電子文書に付与される署名の役割を持つデータのことである. インターネット上の文書や通信は, 第三者によるなりすましや改竄のリスクにさらされている. 電子署名はこのようなリスクの防止のために本人確認や改竄検知の機能を持つ. 本プロジェクトでは公開鍵暗号を用いた電子署名を用いる. 公開鍵暗号方式の電子署名を用いた伝送は以下の手順で行われる.

1. 送信者は本文に対し秘密鍵を用いて公開鍵暗号方式の暗号に類似した手順を行い署名を生成する.
2. 送信者は本文と電子署名を受信者に送る.
3. 受信者は電子署名に対して公開鍵を用いて復号に類似した手順を行い, 署名の検証を行う.
4. 受信者は検証結果と, 本文の一致を確認する. この一致から, 手順１での電子署名生成時の本文と受信者が受け取った本文が一致していることと, 送信者が本人であることが保証される.

上記手順１からわかるように, 送信者は署名を生成する際にデータとともに自分の秘密鍵を使用する. 送信者の秘密鍵を持つのは送信者のみである. そのため, この秘密鍵とペアである公開鍵で検証し, 正しい結果が出る署名を生成できるのは送信者だけである. このことが電子署名が送信者の正当性を保証する根拠となる. ただし, この論理は送信者の正規の公開鍵を受信者が取得しているという前提のもとのものである. 実際には, 署名検証時に公開鍵が送信者本人のものであるか確かめる必要がある. そのために, 一般的に受信者は公開鍵の有効性を証明するための電子証明書を信頼できる第三者機関から発行する. 公開鍵暗号方式の電子署名では上記のように送信者の正当性と伝送文の完全性が担保している.

（※文責: 東未来翔）

2.4 S/MIME

S/MIME(Secure / Multipurpose Internet Mail Cryptography and Security Extensions) とは, 背景でも触れた通りメールの暗号化とメールへ電子署名を行うための標準規格である.S/MIME の仕様は業界標準として利用されていた PKCS を元に RSA Data Security 社が開発し,IETF によって 1998 年に最初の規格が標準化された.S/MIME は公開鍵暗号を用いた電子署名によって実現している.S/MIME を使用するためには, 事前に認証局から鍵ペアと証明書をインストールしなければならない.S/MIME では送信時にまずメールに電子署名が添付される. その次に, 署名されたメールごと暗号化が行われ送信される. この方式は Sign-Then-Envelop 方式と呼ばれる.PEM と呼ばれる S/MIME に似た古い仕様では, 電子署名したデータと暗号化をしたデータを結合し送信する Sign-And-Envelop 方式が採用されており,S/MIME では PEM との互換のためにのみこの方式が用いられる.S/MIME における公開鍵の信頼は PKI(公開鍵認証基盤) によって行われている.

（※文責: 東未来翔）

2.5 PKI(公開鍵認証基盤)

PKI(公開鍵認証基盤) とは公開鍵とその持ち主の対応関係を認証局（CA）という第三者機関を用いて保証するものである. あらかじめクライアント側のソフトウェアに, 信頼するに足ると判断した認証局の証明書を組み込んでおく. そして, ほかの認証局はより上位の認証局が署名した証明書をによって自身の信頼性を証明する. この認証の連鎖を遡ればいずれかの時点でソフトウェアに組み込まれた証明書の認証局にたどり着く. この時点で遡上元の認証局の正当性が確保される. このような認証局間の信頼の連鎖によって公開鍵とその持ち主の対応関係を保証する社会的基盤が PKI である.

（※文責: 東未来翔）

2.6 ハッシュ関数

公開鍵暗号方式では, 相手に送るメッセージなどをハッシュ関数によってハッシュ化する. ハッシュ（hash）とは, 細かく刻んでぐちゃぐちゃにするようなことを意味する. つまりハッシュ関数とは, 入力された文字列を一見して理解できない不規則な数列などの値に変換して出力する関数のこ

とである. 出力された値をハッシュ値という. とはいえハッシュ関数は名前の通り関数であるため, 同じ文字列からは必ず同じハッシュ値が出力される. また, 入力された値がどれほど大きなサイズであっても, ハッシュ値は常に同じサイズである. 例えば 32 バイトで出力されるハッシュ関数であれば, 入力された値の大小にかかわらず出力は常に 32 バイトである. さらに, 暗号プロトコルで使用するハッシュ関数は上記に加え, 以下のような性質が重要である. ハッシュ関数を H, 入力された値（メッセージ）を m, ハッシュ値を h とする.

- 原像計算困難性　h から $H(m) = h$ となる m を求めることが困難である.
- 第二原像計算困難性　m_1 から $H(m_1) = H(m_2)$ となる $m_2(\neq m_1)$ を求めることが困難である.
- 衝突困難性　$H(m_1) = H(m_2)$ かつ $m_1 \neq m_2$ である m_1 と m_2 の組み合わせを求めることが困難である.

原像計算困難性は, ハッシュ値からメッセージを再現できないようにする性質である. また, 第二原像計算困難性と衝突困難性は同じ性質に見えるが, 条件を満たす数字を見つける確率が異なることから別の性質である. これは誕生日のパラドックスと呼ばれる現象と同様である. あらかじめ指定された数字と同じものを探し出す確率と, 様々な組み合わせの中から数字が同じ組み合わせを見つける確率が異なることである.

（※文責: 岡本英太）

2.7　ID ベース暗号とペアリング

ID ベース暗号は 2000 年以降に登場した, 比較的新しい楕円曲線を利用する暗号である. この暗号方式において用いられる数式が, 線形代数学におけるペアリングである. ペアリングは, 本プロジェクトにおいて受信者が電子署名を検証する数式にも用いられている非常に重要な数式である. 次項から,ID ベース暗号とペアリングについて詳しく説明する.

（※文責: 岡本英太）

2.7.1　ID ベース暗号

ID ベース暗号とは, 公開鍵に文字列 ID を用いる暗号方式である. 従来の公開鍵暗号方式では, 公開鍵に法則性は存在せずその公開鍵が誰のものであるか一目で理解することは難しかった. メールアドレスや学籍番号などの明らかに受信者本人だと分かるような文字列 ID を公開鍵として用いることが, 従来との大きな差異である. 送信者は受信者の ID からメッセージを暗号化し送信する. 受信者は鍵生成局から受け取った秘密鍵で暗号文を復号する. この暗号方式の特徴として, メールアドレスを ID として運用する暗号システムの場合, 受信者がシステムに未加入であっても送信者は暗号文を生成して一方的に送信することができる. この時, 受信者が受け取ったメッセージを復号するためには同一システムに加入し秘密鍵を受け取る必要がある. 鍵生成局はシステム加入者全ての秘密鍵を生成することができるマスター鍵を持つため, 必然的に大きな権限を持つことになる. 仮に鍵生成局が不正を働いた場合多くの被害が出るため, 鍵生成局を分散させる方式が提案されている.

また, 鍵の失効に関する課題もある. 何らかの不手際で個人の秘密鍵が流出したとき, 通常の公開鍵暗号の場合, 秘密鍵を新たに生成し, 流出した秘密鍵を失効するだけで事足りる. しかし ID ベー

ス暗号の場合は, 他の公開鍵暗号方式のように秘密鍵を作り直すことは容易ではない. 例えばメールアドレスを ID としていたとき, 一つの対処方法としてマスター鍵を変更し, それに伴い各個人に秘密鍵を配布しなおすという方法がある. しかし, 鍵生成局の不手際でマスター鍵が流出したならまだしも, 一個人の不手際のために, マスター鍵を変更するのは費用やシステムの観点から現実的ではない. この場合, 自らの秘密鍵を流出した本人が秘密鍵を変える必要があるが, 秘密鍵を新たに生成するためにはメールアドレスを変更する必要がある. しかし, メールアドレスを別のシステムで利用している場合など変更するのは難しい. これは社員 ID や保険番号などの場合も同様である.

（※文責: 岡本英太）

2.7.2 ペアリング

厳密な定義は非常に難解であるため, 電子署名のシステムにおいて重要な部分の概略を説明する. ペアリングとは楕円曲線 E 上の 2 個の点の組からある有限体 F_q への写像のことである.

$$e : E \times E \ \rightarrow \ F_q$$

楕円曲線上の 2 点を P, Q とし,$\overrightarrow{R} = \overrightarrow{P} + \overrightarrow{Q}$ となる R からなる平行四辺形 $OPRQ$ の面積は P, Q の 2 点から決まるため,$S(P, Q)$ とする. 面積 $S(P, Q)$ を, ある有限体 $g \in F_q$ の指数に乗せたものがペアリングの値である.

$$e(P, Q) \ \rightarrow \ g^{S(P,Q)}$$

ペアリングの性質として, 点 P の値が 2 倍になると, 面積 $S(P, Q)$ は 2 倍になり, ペアリングの値は 2 乗になる.

$$e(2P, Q) \ \rightarrow \ g^{S(2P,Q)} \ \rightarrow \ g^{2S(P,Q)} \ \rightarrow \ (g^{S(P,Q)})^2 \ \rightarrow \ e(P, Q)^2$$

ペアリングのこの性質は,ID ベース暗号などの楕円曲線暗号の復号や, 電子署名の正当性を検証する際に使われる非常に重要な性質である.

（※文責: 岡本英太）

第 3 章　到達目標

3.1　問題設定

近年,IT 化が進み多くの個人や組織の情報を情報機器上で扱うようになり, 一方で, サイバー犯罪の検挙数やインターネット上のトラブルの被害件数は増加傾向にあり, 犯罪の手口も高度化・多様化している. これにともない, セキュリティのリスクと重要度も増加してきている. 最も警戒するべき組織向け脅威として「標的型攻撃」が存在する. その標的型攻撃の対抗策として電子署名が有効である.

電子署名とは, その文書ファイルが第三者の手によって改ざんされていないことを証明する物である. 現実の紙書類の印鑑やサインのような証明をする役割がある. 印鑑やサインのような役割を果たすためには, その署名が正しいものであると証明する必要がある. そのためには認証局がその署名が正しいことを証明できるようにするために, 電子証明書と確認を行うことを必要とする. 電子署名は「電子署名及び認証業務に関する法律」で基準が定められている. 通常の電子メールは送信者と受信者の間に第三者が割り込み, なりすましや電子メールの改ざんを行うことが可能になっており, そのなりすましや改ざんによって悪意あるテキストやウィルス等のファイルを送ることが可能になってしまう. 具体的には, 受信者から信頼できる送信者本人を名乗ったテキストメールを送り, 金銭を扱うサイトへ誘導することができてしまう. その対策として, ハッシュ値を用いた電子署名を使うことができる. 送信者の認証を行うことで本人の証拠が残るため, メールを偽装して送信者を偽るなりすましも検知することができる. 電子署名のシステムを作成する上で, 鍵の受け渡しのためのユーザーごとの認証機能が必要になる. ユーザー認証システムは新規に作成する上では難易度が高い. 既存の電子署名の規格としては「S/MIME」というものがある.

「S/MIME」とは電子メールの公開鍵方式による暗号化とデジタル署名に関する標準規格である. 安全性が高いのに加えて, 企業で使用されるメールソフトの 90 %が対応済みでありインフラが整備されているといえる. しかし S/MIME の仕組みとして, 自分で作成した公開鍵/秘密鍵のペアのうち, 公開鍵を認証局に送付し, 本人確認を経て証明書を発行してもらう必要があるので, 実装/導入のハードルが高い. また, 認証局による公開鍵認証サービスを契約する必要があるため年間コストが高いと言った側面がある.

そこで本グループでは, 電子署名導入の障害となっている上記 2 つの理由「実装/導入のハードルが高い」「年間コストが高いこと」に着目した. 電子署名は, 送信者は送信する本文を秘密鍵とハッシュ化を用いて署名を生成し, 本文と一緒に送信する. 受信者側は公開鍵と一緒にその署名を検証して得たハッシュ値と本文をハッシュ化したものを比較する. 電子署名に関連した暗号技術として ID ベース暗号がある.

ID ベース暗号は公開鍵にメールアドレスのような本人であることを示すことが出来る ID を使用し, 秘密鍵は同様の ID を元に生成を行う. 公開鍵の生成の際に宛先のユーザー ID を用いて鍵の生成を行うため, 認証局に公開鍵を送付して証明書の発行を行う必要がなく, 導入負担が少ないといえる.

このように導入負担の少ない暗号技術があるにも関わらず, 既存の電子署名は導入負担が大きいことにより, 電子署名が普及していないことから標的型攻撃の対策が十分にできていないことを問題として設定した.

（※文責: 北山奏）

3.2 課題設定

標的型攻撃は情報セキュリティ上の最も深刻になりうる攻撃の 1 つであり, 対策すべきものである. 具体的には, なりすましや改ざんを行い, 受信者本人を油断させ, 攻撃に使うファイルを開かせる方法である. この方法は, 受信者にとって警戒する手段が少なく, 事前に確認を行わない限り防ぐ手段が少ない. 攻撃に使うファイルの中にはランサムウェアが仕込まれる可能性がある. ランサムウェアとはファイルを勝手に暗号化し, ファイルの復号と引き換えに金銭を要求する悪意のあるプログラムである.

コンピュータはもはや人類にとって欠かすことのできないツールであり, パソコンや日常的に所持するスマートフォンの中には大量の個人情報が詰め込まれている. 一個人のデータだけでなく企業の顧客管理や機密情報を扱うパソコンだった場合, 情報を漏洩されてしまうと企業の信用問題などにも繋がります. これらの心理を用いて身代金を要求するものである. ランサムウェアは身代金を払うことより解除されるものが多い. ランサムウェアの目的はデータの取得ではなく, あくまでも金銭であり, 金銭を払えばデータが元に戻ると主張し, 実際にデータが戻ってくれば金銭を払ってもらえる可能性が高い.

しかしランサムウェアに対して身代金を払うことは推奨されていない. このようなランサムウェアにかからないために事前にセキュリティの強化を行う必要がある. そこで有効な対策として電子署名が挙げられる. 電子署名はメールに添付し, なりすましの防止やデータ改ざん検知を行うことができる暗号技術である. 電子署名は公開鍵暗号の処理と類似しており, それらの知識を使うことが出来る. メールでの電子署名が普及すれば, 標的型攻撃によるランサムウェアなどの攻撃を事前に防ぐことが出来る.

しかし 3.1 節で述べた通り, 標的型攻撃の対抗技術として S/MIME(電子署名) が存在するが, 年間コストが高いこと, 相手のメールアドレスが電子署名に対応しているかわからないことなどから普及しておらず, 標的型攻撃の対抗技術として十分な機能を満たせていない事を問題として設定した. 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グループメンバーと議論を行った. その結果, 電子署名が普及していない原因である年間コストを減らすことが出来れば, 標的型攻撃の主な攻撃先である大学や企業, 資金面で問題がある個人でも電子署名を導入・運用することができるのではないかと考えた. また, 電子署名を利用する大学・企業等が増えれば, 様々なメールシステムでも対応していくことにも繋がると考えた. その他, どのような手段で電子署名の年間コストを減らすのかについても議論を行った. その結果, 暗号技術を学ぶために並行して行っている 2020 年度の卒研生の成果報告書から着想を得て,ID ベース署名を利用することで年間コストを減らすことができるのではないかと考えた.

ID ベース署名とは,ID を公開鍵とした公開鍵暗号方式であり, メールアドレスを公開鍵として利用することができる. 既存の技術である S/MIME では, 別途に公開鍵を作成し, メールアドレスと公開鍵を紐づけ, 公開鍵の所有者が本人であることを第 3 者機関 (認証局) から認めてもらう必要があった. そのため, 公開鍵証明書を貰うためのコストが大きく, 電子署名が普及するための大きな妨げとなった.ID ベース署名を利用することができるのであれば, 公開鍵証明書が必要ないため電子署名の導入・運用コストを大幅に削減することができると考えられる. しかし,2020 年度の卒研生は学内メールシステムに電子署名の機能を実装していたが, 今年度から学内メールシステムが Gmail に移行したため, 以前の機能が使用できなくなった.

そこで, 本グループでは,ID ベース署名機能を Gmail システムで使用できるように, 電子署名のシステムを新しく作成し直すことを目的として活動していくことになった.

（※文責: 森谷史奏）

3.3 到達レベル・具体的な手順

ID ベース暗号機能を用いて電子署名の生成, 検証ができる機能を Chrome 拡張機能として学内メールシステムに実装することを目標とした. 機能の実装をするにあたり, 本文の内容を読み取り, ハッシュ化を行う班, 電子署名の作成, 検証を行う班, 電子署名をメール末尾に署名添付, 読み取りを行う 3 つの班に分けた. 前期活動には, プロジェクト全体で暗号についての知識を深めるための講義を行い, グループ内では,Chrome 拡張機能への実装にあたって,JavaScript と HTML の学習を行いグループメンバー全員が JavaScript と HTML を用いた簡易的な拡張機能を作成することにより Chrome 拡張機能についての知識を身に着けた. 後期活動に入り, 成果物作成に本格的に着手し, グループ内で 3 つの班に分かれ制作し, それぞれの機能の統合を行った. 詳細を下記に示す.

（※文責: 北山奏）

3.4 スケジュール

前期の活動は 5 月から 8 月にかけて行われた.5 月では担当教員から講義として, プロジェクト全体で暗号の基礎知識の習得を行った後, プロジェクトメンバーを暗号班,WEB 班,CTF 班の 3 つのグループに分けて, それぞれのテーマを決め, 活動を行った. 講義は RSA 暗号やシーザー暗号を始めとした基礎的なものから学んだ.6 月はその講義で得た知識を元に, 前回のプロジェクトや卒業研究生の論文, 外部の先行研究などを参考にして暗号システムの理解を深め技術習得に取り組んだ.7 月は中間発表の準備のため, スライドの作成や発表のためのポスターの作成を行った. 中間発表を行い, 参加者から受けた指摘をまとめ, 今後の参考にした.8 月では Chrome 拡張機能の技術習得を行うために,JavaScript や HTML の学習を行った.

後期の活動は 9 月から 1 月にかけて行われた.9 月と 10 月では夏季休暇中に課題として出した,JavaScript と HTML を用いた簡易的な Chrome 拡張機能をグループ内で発表を行い前期に習得した知識の復習を行った後, 成果物の作成に着手した. 詳細的な機能の制定を行い, ウェブサイトの Gmail 本文の内容の読み取り, 電子署名の作成, 電子署名をメール末尾に添付, 本文の取得, 署名の読み取り, 署名の検証の 6 つのプロセスに分割し, このプロセスをグループ内で 3 つの班に分かれ成果物作成と同時進行で前期に引き続き,Chrome 拡張機能についての知識習得を行うことにした.11 月,12 月では各機能の制作を行い, 各班の制作が終わり次第, 統合をおこない Chrome 拡張機能への実装をはじめた. 成果発表会に向けた, 成果物の作成, 発表のためのスライドの作成, ポスターの作成, 発表用の動画の作成を行った. 成果発表会で受けた指摘をリストアップし, それをもとに改善を行った.1 月は後期末提出物の作成を行った.

- 前期

5 月 メンバーの班決め, 暗号の基礎知識の習得, 担当教員による暗号の講義

6 月 前回プロジェクトや卒業研究生の論文, 先行研究を参考に暗号システムの理解を深める, 作成する機能の制定

7 月 中間発表準備, 中間発表

8 月 必要知識の習得, プログラムの理解

- 後期

10 月 実装する機能の詳細の制定, メンバーごとの役割の割り当て

11 月 プログラムの作成

12 月 成果発表に向けた成果物の作成, 成果発表の準備

1 月 後期末提出物の作成

（※文責: 森谷史奏）

3.5 前期活動

暗号のシステムを構築するに当たり, 前期では担当教員による暗号に関する講義を受けた. 内容は主に, 暗号に関する知識の会得であった. 実在する暗号方式を例に取り, シンプルな暗号システムからはじめ, プロジェクトに使う暗号の学習をした. シーザー暗号は簡単な暗号の一つである. シーザー暗号は原文である文字のアルファベットをある一定数ずらし, 読めなくする暗号であり, これは暗号化が簡単であり便利といったメリットがあるが, それと同時に復号のための動作が読みやすく, 暗号を解読されやすいといったデメリットが存在する. プログラム上では, まず乱数を作成し, その乱数によって文字をずらす量を決める. 計算には mod を用いた計算を行い, 復号を行えるようにしている. 復号のための key を複数個作成することも出来る. 鍵の受け渡しを行うため鍵配送問題がある. メールを暗号化し, 復号する上で送信者が受信者に対して鍵を送らなければいけない. しかし, 鍵をメールで送ってしまうと, その鍵を見られてしまったら本末転倒となってしまう.

その問題を解決したのが公開鍵暗号である. 復号と暗号化の鍵が違い, 公開鍵と秘密鍵を作成する. 送信者は受信者から予め公開鍵を受け取り, 送信するメールにその鍵を使って暗号化しメールを送る. 受信者は秘密鍵を使用して復号することが出来る. このような鍵システムを用いる.

具体的な機能の構成としては,ID ベースには送受信者やメールサーバ以外にも鍵生成局というものがあり, 送信者は暗号化のための特定の ID を公開鍵として使用するが, 受信者は復号のための秘密鍵を鍵生成局から貰う必要がある. 以上の知識や仕組みを学んだ. また,Chrome 拡張機能への実装にあたって,JavaScript と HTML の学習を行いグループメンバー全員が JavaScript と HTML を用いた簡易的な拡張機能を作成した.

（※文責: 北山奏）

3.6　課題の割り当て

各人の興味のある分野及び関連性, 時間軸のスケジュールを基準に以下のように割り当てた.

送信者側

・ウェブサイトの Gmail 本文の内容の読み取り (中村・野澤)
・電子署名の作成（東・岡本・森谷）
・電子署名をメール末尾に添付（北山・青山）

受信者側

・本文の取得（中村・野澤）
・署名の読み取り（北山・青山）
・署名の検証（東・岡本・森谷）

（※文責: 北山奏）

3.7　前期活動のフィードバック

プロジェクト全体の活動として暗号についての知識を習得した. 本グループでの前期の活動として, 暗号についての知識をより深め,Git を用いた開発を行うことを想定し,Git についての知識習得や, 共同開発を行うテストをおこなった. また,Chrome 拡張機能への実装にあたって,JavaScript と HTML の学習を行い, 知識の習得に取り組んだ. そのため, 実際の開発は後期活動期間中に行うこととなった. 前期活動中には成果物の具体的プロセスは固まらず, 後期活動への向けての反省点とした.

また, 中間発表についてはスライドや発表内容に関しては好評であったが, 質問のなかった時に無言の時間があり空白の時間が生まれていたことや, 質問に対して知識不足による回答ができなかった部分が反省点であった. そのため, 後期はこの反省を生かすことをプロジェクト全体で共有した.

（※文責: 北山奏）

3.8 後期活動

後期の活動にあたり, 前期の活動で習得した知識が抜けている部分が多々あったため知識の再習得を行なった. 前期活動と夏季休暇の期間のなかで JavaScript と HTML を用いた簡易的な拡張機能を作成してもらい, 後期活動の初めにその成果物の発表をグループ内で行った.

ID ベース署名を用いた電子署名の作成のための必要な機能を, ウェブサイトでの Gmail 本文の内容の読み取り, 電子署名の作成, 電子署名をメール末尾に添付, 本文の取得, 署名の読み取り, 署名の検証の 6 つのプロセスに分割し, それをもとにグループ内で課題の割り当てを各人の興味のある分野及び関連性をもとに割り当てた. 機能としては送信者側の機能と受信者側の機能に分けられるが, どちらの機能でも同じ技術を使うことが多くあったため技術ごとに 3 つのグループに振り分けて活動を行った.

1 つ目のグループはメール本文とメールアドレスを読み取る機能, またそれらをハッシュ化する機能を担当した. 2 つ目は ID ベース暗号を用いて電子署名を作成し, ハッシュ値を用いてメールの検証を行う機能を担当した. 3 つ目は電子署名をテキストファイルとしてメールに添付し, 受け取ったメールから電子署名の読み取りを行う機能を担当した. マージを行う際には特別なツールを使用することなく, メンバー同士とコミュニケーションを取りながらコードの統一などを行なった. 統合が終わった後, 発生したエラーやバグなどを取り除き, プログラムの完成を目指した.

後期の活動によって実装・実現できたのは,Google Chrome のみでの拡張機能によって,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である.

（※文責: 森谷史奏）

3.8.1 送信者側の機能の使用手順

送信者側の機能の使用手順を以下に記載する

1. 本文を書く
2. 本文をハッシュ化する
3. 受信者のメールアドレスを ID として公開鍵を生成する
4. ハッシュ値に対し, 公開鍵暗号における暗号化と類似の手順を行い, 電子署名を生成する
5. 本文の末尾に電子署名を.txt として添付する
6. 送信する

（※文責: 森谷史奏）

3.8.2 受信者側の機能の使用手順

受信者側の機能の使用手順を以下に記載する

1. メールを受信する
2. メールから電子署名のファイルを読み取る
3. 平文からハッシュ値を計算する
4. 署名を相手の ID ベース暗号の公開鍵で復号してハッシュ値を取得する
5. ハッシュ値を比較する (署名検証)
6. 署名検証に問題がなければ, 復号された平文が正しいと判断することができる

（※文責: 森谷史奏）

3.9 後期活動のフィードバック

後期の活動では, 前期活動と夏季休暇の期間のなかで各々簡易的な拡張機能を作成してもらい, 後期活動の初めにその成果物の発表をグループ内で行うことから始まった. その後, 前期活動で習得した知識が抜け落ちている部分が多々あったため知識の再習得を行なった. 知識の再習得の部分は夏季休暇で復習を続けていれば発生することがなかったため反省点とした.ID ベース署名を用いた電子署名の作成のために必要な機能を明確にし, それをもとにグループ内で課題の割り当てを各人の興味のある分野及び関連性をもとに割り当てた. マージを行う際には特別なツールを使用することなく, メンバー同士とコミュニケーションを取りながらコードの統一などを行なった. 前期活動で Git を用いた共同開発を想定していたにもかかわらず一切使用する機会がなく完全に無駄な時間となってしまったため反省点とした. 成果報告会の準備では, 成果物の完成が遅れていたため, 準備の時間が想定よりもあまり取れず, スケジュール管理について問題があったと考えられ反省点とした. 成果報告会では, 想定以上に良い反応を得られたことから準備の時間があまり取れなかったにもかかわらず, よりよい発表資料を作成することができたと考えられる.

（※文責: 森谷史奏）

第 4 章　プロジェクト内のインターワーキング

4.1　東未来翔

前期

本グループのグループリーダーの任を引き受け, グループの取りまとめやスケジュール管理, 他グループとの連絡等を行った. グループの活動方針決定にあたっては, 各案の取りまとめや先行例の紹介, 技術的な指摘を行った. 発表資料作成においては電子署名技術の解説部分の作成を行った. 技術的な仕様が前提知識なしでも理解できるように図を用いた解説を作成した. また, グループリーダーとして発表資料全体の編纂も行った. 具体的には, 発表資料の大まかな流れの決定や分担の割り振り, 各章における重複部分の修正, 発表環境の構築等を行った.

後期

前期に引き続きグループリーダーとしてグループの取りまとめやスケジュール管理, 他グループとの連絡等を行った. スケジュール設定に当たっては, 現状の再認識を行い多少厳しいスケジュール設定とした. また, 前期まではあいまいであった各メンバーの担当分野を明確にし, 成果物作成における分担の割り振りを行った. この割り振りにおいて私は電子署名の生成と検証を担当した. 具体的には,JavaScript を使用して Chrome 拡張機能上で動作する電子署名の生成と検証の関数を, 同じ担当となった岡本と協力して作成した. また, 成果物作成においてはリーダーとして進捗管理と各担当間の調整を行った. 調整においては, 各担当部分間でのデータのやり取りの仕様を指定するなどした. また, 進捗管理においては, 各担当の障害となっている点を把握し知見を持つほか担当者を紹介したり, 文献を紹介したり, スケジュールの調整を行うなどした. 発表準備に関しては, 他メンバーが改良を行った資料の添削, 発表環境の整備, 各グループ間の調整などを行った.

（※文責: 東未来翔）

4.2　中村碧

前期

前期はプロジェクトリーダーとして主に各グループリーダーとコミュニケーションをとりながら, 提出する書類の確認や進捗の確認を行い, 問題があれば原因を探し解決までサポートすることを行った. さらに, プロジェクト全体の進捗状況を把握するためには, プロジェクト学習が終わる数分前に各グループリーダーから進捗の報告を行う習慣を作ることで, 自分だけが各グループの進捗を把握しているという状態を防ぎ, 全員でプロジェクト学習を行っているという意識を増やす工夫をした.

また, 暗号班の１メンバーとして, 中間発表に向けてポスター作成を主に活動した. 暗号班のポスター文章を作成したり, ポスターのデザインの作成も担当した. そして, 各グループリーダーにポスターの文章作成をお願いし, その文章の査読, 違和感がないかをチェックして中間発表に使用した. 次に, 中間報告書ではグループの背景を担当し, なぜ Google 拡張機能に電子署名を実装しようとしたのか, 改めて考え報告書に反映することができた.

後期

後期も前期と同様にプロジェクトリーダーと主に各グループリーダーとコミュニケーションをとりながら, 提出する書類の確認や進捗の確認を行い, 問題があれば原因を探し解決までサポートすることを行った. 前期と違ったところは, 問題が一切発生しなかったところだ. これは各グループリーダーがプロジェクト学習に慣れてきたことでスムーズに活動を進めることができたからだと考える. さらに, 前期同様に活動終了前に各グループリーダーから進捗報告を受け, 進捗の確認とプロジェクトのエンゲージメントを失わないように意識して活動した.

また, 暗号班のメンバーとして, もう一人の相方と分担作業を行いながら,GAS を使って Drive を操作したり GmailAPI からメール本文取得と, メールアドレス取得して引き渡す部分の機能追加を行った. そして, 前期同様にポスターの査読, 各グループリーダーに文章の作成を依頼し, 成果発表会で使用するポスターを完成させることができた. 成果発表会当日は, プレゼンテーションを行い補助資料を読まないことを意識しながら大きい声で聴いてくれる方に聞こえるように発表することを心ががけた. 成果報告書は, 前期同様に背景を担当し, グループリーダーからの聴取や参考文献を探しより詳しく背景を理解し, 読み手のことを考え読みやすい文章を書くことを心がけた.

（※文責: 中村碧）

4.3 青山慎太郎

前期

プロジェクト配属当初は暗号に対する知識が乏しくプロジェクトの目標が定まっていなかったためプロジェクト全体で暗号に関する資料や以前のプロジェクト学習の内容について調べ, 担当教員からの講義や実際に Capture The Flag を行うことで暗号について理解を深めた. その後, プロジェクトメンバー全員で話し合いプロジェクトの活動を定め活動ごとにグループに分かれた. グループに分かれた後は Google 拡張機能による Gmail での ID ベース署名の開発に JavaScript の知識が必要なため JavaScript について学習し, 簡単な Google 拡張機能を作成することで拡張機能を実装するためのスキルを身に着けた. また, 共同での開発を円滑に進めるために GitHub というソフトウェア開発プロジェクトのバージョン管理を共有できる Web サービスについて学習した. 前期末には中間発表に必要なスライドやスライドに使用するイラストや図表, 発表に必要となる台本の作成を行い実際に発表するために発表練習を行った. また, 夏季休暇中にグループメンバー各々が拡張機能を作成することとした.

後期

後期は最初にメンバー各々が作成した拡張機能をお互いに紹介した. その後,ID ベース署名のファイル生成, 添付と署名の読み取りの部分を担当することになった. まず生成された ID ベース署名を添付するためにファイル化する必要があるため署名を Google Apps Script 用いてテキストファイル化した. 次に署名の添付を JavaScript で実現しようと試みた. しかし送信者側では下書きに署名を添付することはできたが受信者側では送信者が添付した署名を確認することができず, 受信者側で署名を確認するには署名をアップロードできるサーバーが必要であるということが判明した. よって JavaScript による添付機能の実現は困難であるという結論に至った. そこで Google が提供しているプログラム言語である Google Apps Script を使用して添付機能の開発を行うことに

した.Google Apps Script は JavaScript を基にしているため JavaScript を学習した経験を生かすことが可能である. また Google が提供しているため Gmail 専用のメソッドが存在し Gmail に対する拡張機能の開発に適している. よって JavaScript よりも Gmail への署名の添付が容易にできるだろうと考えた. 実際に開発を進めると送信者側では署名の添付に成功し受信者側では添付した署名を確認することができた. 成果発表会では私たちのグループの成果物を発表した.

（※文責: 青山慎太郎）

4.4 岡本英太

前期

RSA 暗号などの暗号の種別や暗号生成方法, 暗号の利用方法・利用目的の知識を身につけた. 現在の学内でのセキュリティにおける問題点などをグループで話し合い, 暗号の活用方法を検討した結果,ID ベース暗号を応用した電子署名を学内メールシステムに Google 拡張機能を用いて実装することを最終成果として設定した. 共同開発のための Git や Google 拡張機能について学んだ. 個人としては工房でポスターを印刷する方法を学び中間発表におけるポスターの印刷を担当した. 中間発表や提出物については期限に余裕を持って作成を進めることができた.

後期

後期では, 最終成果物の作成を進めた. 主にメール本文や ID となるメールアドレスから署名を生成・検証する部分を担当した. ペアリング暗号ライブラリの mcl を活用し JavaScript 上で署名の生成・検証の機能を完成させることができた. ただ mcl を理解することに時間がかかり, また署名の根幹のある値を生成するハッシュ関数のコードを書くことに非常に時間を取られ, 個人的に計画通りに進まなかった印象だった. またそれに伴い, 成果発表会の準備や最終報告書の作成に十分に協力することができなかった. 成果発表ではポスター画像の作成を担当したほか, 当日の発表も行った. 十分な聞き取りやすい声量で話すことはできたが, 話す内容を飛ばしてしまい, また質疑応答では若干質問に適切な回答をすることができなかった部分があった.

（※文責: 岡本英太）

4.5 北山奏

前期

前期は暗号についての知識がなかったため, プロジェクト内での暗号についての講義や知識習得の場面で積極的に学習に励んだ. そこで RSA 暗号やシーザー暗号などの代表的な暗号技術についての知識を学んだ. 成果物については暗号班の一員となり, 電子署名作成のために必要な Chrome 拡張機能や ID ベース暗号,JavaScript,HTML の学習を行った. また中間発表に向けてスライドの作成を担当し, 聴講者に見やすく分かりやすいスライドの作成を心掛け, 内容が簡潔に伝わるような原稿の作成にも取り組んだ. 発表当日は機材のセッティングや発表のリハーサルを行うなど発表準備を積極的に行い, 発表は聞き取りやすい声量や速度で発表することを心掛け, 公表を得た. また, 中間報告書は到達目標についての記述を担当した.

後期

後期は成果物作成に着手し, 暗号班をさらに 3 つのグループに分け, 私はメールに電子署名を添付する作業を担当した. そこで, 前期で学習した JavaScript の知識を活用した. まず任意の文字列をメールの末尾に挿入する機能を作成し, その文字列をテキストファイルにする機能も作成した. そしてそのファイルを添付するために Chrome デベロッパーツールを開き, そこから Gmail に添付するコードを読み取ろうとしたが, 実際に添付しないとデベロッパーツールの Element 要素に表示されなかったので, その部分を我々が書き足して添付できるようにしようとした. しかし, 各メールに割り当てられるメッセージ ID を独自に設定すると, ファイルをサーバーにアップロードすることができなかった. そこでもう一人のグループメンバーに別のアプローチを試してもらい, 私は Gmail を構成するファイルの中から, ファイル添付についての記述があるコードの読み取りを行った. しかし, 膨大な数のファイルから添付についてのコードを探し出すことができなかったため, 私も別のアプローチに切り替えた. その方法が GoogleAppScript を使ったコーディングだ. これは Google が提供するサービスで,Google のアプリケーションをカスタマイズするのにとても適しているツールだ. これを用いて私たちのグループは任意のメールのメッセージ ID を取得することに成功した. そして, 任意のメールにファイルを添付する機能を完成させることができた. また, 各グループで作成したプログラムをマージする作業では, 他のグループが作成したプログラムと同じようなコードが存在した箇所があったため, その部分を簡潔にまとめることができた. 学習成果発表会では, 発表準備としてスライド作成に必要な素材を準備し, 当日は機材の設置をして, 発表に向けてリハーサルを行った. 発表では, 聴講者に分かりやすい説明や聞き取りやすい発表になるよう心掛けた, 概ね好評を得た. また, 最終報告書では, 到達目標についての記述を行った.

（※文責: 北山奏）

4.6 森谷史奏

前期

本グループでは,GoogleChrome の拡張機能を用いて行う予定であったため, まず初めにプロジェクト全体として暗号の知識についての講義を受け,RSA 暗号やシーザー暗号などの暗号技術についての知識の習得を行った. その後グループに別れたのち,GoogleChrome の拡張機能への ID ベース暗号を用いた電子署名の実装のため,Chrome の拡張機能,ID ベース暗号,JavaScript,html の知識習得をグループメンバーと共に行った. 中間発表では, 主にスライド作成を担当し, スライド作成についてはそれぞれがスライドのどこを担当するかを決め, 私はスケジュール部分の担当をした. その他にも, 時間制限の範囲に収まるように発表練習や, 発表原稿などにも貢献した. 中間報告書では到達目標の部分を担当しており, グループがどのようなプロセスで目標達成を行うの整理を行い, 報告書の作成を行なった.

後期

後期では, 成果物作成に本格的に着手し, グループ内で 3 つの班に割り振られ, 私は電子署名作成と, 署名検証の部分を担当した. 具体的な活動内容としては前期で学習した JavaScript の知識を用いて,Chrome 拡張機能での電子署名の作成と署名検証の関数を同じ担当メンバーと共に作成した. この関数作成のために必要な情報探索を Web サイトや図書室などを用いて行い, 最終的には mcl

ライブラリを用いて, 電子署名の作成と署名検証の関数を作成した. また, 成果報告会では, スライド作成と発表原稿の作成を担当し, 中間発表のスライドをもとにメンバーとコミュニケーションを取りながら発表スライドの作成に取り組み, 成果報告会当日では, 実際に発表も行った. 期末報告書では中間報告書同様, 到達目標の部分を担当しており, グループがどのようなプロセスで目標達成を行うの整理を行い, 中間報告書の作成したときより, より詳細に報告書の作成を行なった.

（※文責: 森谷史奏）

4.7 野澤真生

前期

本プロジェクトで班ごとに担当する分野を決めたのち, 暗号班では白勢先生の指導の下, 暗号技術に関する知識を学んだ. また,Google Chrome 拡張機能を用いた Gmail への ID ベース署名機能の実装のため,Gmail への拡張機能の追加や ID ベース暗号, 共同開発環境の構築,javascript 等の基礎知識についてメンバーとともに学び, 先行研究や昨年のプロジェクト学習の内容なども調べた.

中間発表に関しては, ポスターの製作を行った. ポスター制作については, 担当したメンバー同士で意見を出し合い, レイアウトなどを変更し, 見やすいように修正や工夫を考えた. 中間報告書に関しては, もう 1 人の担当者と共にまとめの部分を担当し, 前期の時点で必要となると考えた今後の課題についての記述を行った.

後期

前期よりも成果物の構想が具体的になったため, それに必要な Google 拡張機能についての学習や,Google Apps Script（GAS）についての学習を行い, 本格的に自分が担当した Gmail 送信者側のプログラムを組んだ. まず, 拡張機能側の JavaScript を使用して Gmail 及び Google Drive へアクセスすると,Google のサービス側でセキュリティ関連の設定を行う必要があるため,Google Chrome 拡張機能と Google の各サービスをつなぐ役割として GAS を使用した.Gmail 本文の抽出や Google Drive へのスプレッドシート作成など,Google サービスに対して直接処理を行う部分は GAS を Google Chrome 拡張機能が呼び出して処理を行うため,GAS で, メール下書きの本文抽出, 抽出した本文のハッシュ化,Google Drive へアクセスしスプレッドシートを作成, ハッシュ値をそのスプレッドシートへ書き出すといったプログラムを作成した. また, 今回の進捗や次回の予定, 参考にした URL などの情報を共有 Drive に作成した日報へ記録しておくことで, 自分の進捗状況をメンバーがいつでも見られるようにした.

成果発表に関しては, ポスターの印刷の手伝いやスライドの作成などを行い, それぞれの担当メンバーと共に積極的に意見交換をし, より良い発表資料作りを行っていた. 期末報告書に関しては, 結果と各発表会の評価, まとめを担当し, 成果物の制作において生じた問題点の解決手順とその評価や成果発表会における評価, 今後の課題についての記述を行った.

（※文責: 野澤真生）

第 5 章　結果

5.1　成果

5 月の時点では, 教員の講義によって暗号技術についての基礎知識を PARIGP を用いて学習した. また, 昨年のプロジェクトの成果物や報告書から,ID ベース暗号や学内メールにシステムを構築する方法について前提知識を得ることができた.

中間発表では, 私たちの課題設定やその解決のプロセスを広く紹介しました. 発表においては, フィードバックや質問など, 様々な反応をプロジェクト外から得ることができた. このような反応を通して自分たちの活動方針を見直すことができ, その後の活動方針をより良いものとできた. また, 発表するにあたって私たちの活動方針を論理的な形で整理することができた. このことはのちの活動においてのぶれない目標を定める助けとなった. また, 発表資料を作成するにあたって暗号に関する知識がわからない人にも理解が容易であるように説明を心掛けた.

これまでの本プロジェクトの成果物は本文を暗号化する試みは行われていたが, 電子署名についてはまだまだ開拓の余地が感じられた. また, 電子署名技術が未だ世間に一般的に浸透していないことからも, 学内メールに電子署名システムを実装することを最終成果物として設定した.2022 年度から学内メールシステムが Gmail に変わったことを受け,Chrome 拡張機能と Google Apps Script によって電子署名システムを実装するという決定をしたうえで,Gmail の本文をスプレッドシートに取得するグループ,ID としたメールアドレスとメール本文から電子署名を作成・また電子署名の正当性を検証するグループ, 作成した電子署名をメールに添付するグループに分かれた. それぞれ必要になる知識が異なるため, 分かれて作業することで効率的に進めることができた. また, 各グループがこまめにコミュニケーションをとることで有用な知識を共有することができた. 電子署名を作成・検証するグループでは, まず, 仮のマスター鍵・ID・メッセージから Chrome 上で電子署名を作成検証するデモプログラムを作成した. ここでは作成したプログラムを Google Chrome 拡張として実装する時と同様に, ペアリング暗号化ライブラリである mcl と,Javascript を用いて作成することで, 本実装でもそのまま流用することが可能であったほか, これによって各実装機能についての理解をさらに深めることができたのではないだろうか.

最終発表では中間発表でのフィードバックや質問点からさまざまな改良をを行った. まず, 中間のフィードバックや質問等から理解が難しかったと思われる点をさらに簡単な説明とし, 説明が必須でない前提知識は省略した. また, 自分たちが何をしたのか客観的に説明することを通して, 自分たちの活動の特徴点や改善点を見出すことができた. また, 最終発表の場での教員からの指摘は, 今回の最終報告書執筆にも大いに役立てることができた.

（※文責: 岡本英太）

5.2 解決手順と評価

5.2.1 ID ベース暗号

学内の Gmail に電子署名を実装するために ID ベース暗号を利用した.ID ベース暗号とは公開鍵暗号の 1 種である.ID ベース暗号では公開鍵として利用者の学籍番号やメールアドレス, 利用者自身の名前等の任意の文字列を使用できるという特徴がある. よって公開鍵が正しいものであるかどうか公開鍵証明等で保証する必要がない, 学籍番号, メールアドレスといった利用者が容易に知ることができる文字列を公開鍵にすると公開鍵をあらかじめ配布する必要がない等のメリットが存在する. ゆえに従来の電子署名よりも導入負担が軽い電子署名の開発に適していると考えられる. 一方で ID ベース暗号には鍵生成局が秘密鍵を生成するため鍵生成局が任意のメッセージの復号, 署名が可能であるという欠点が存在する. しかし私たちが実装した電子署名では秘密鍵を利用者のコンピュータで生成するためこの点は問題にはならないといえる.

（※文責: 青山慎太郎）

5.2.2 ID ベース署名

昨今増加する標的型攻撃への対策に電子文書に対して署名を付与し送信者本人の確認とデータ改ざんを防止する電子署名が存在する. 現在, 電子署名は S/MIME という暗号化方式が利用されているが S/MIME は普及しているとは言い難く標的型攻撃への対策として十分ではない. よって私たちはより導入負担が軽く学内の Gmail で利用できる ID ベース署名を実装することとした.ID ベース署名を学内の Gmail に実装するためメールを送信する際に必要になる送信先のメールアドレスを公開鍵とした. よって, 私たちが実装した ID ベース署名は既存の電子署名よりも容易に公開鍵を得ることができる. また,ID ベース暗号を利用した電子署名であるので既存の S/MIME を利用した電子署名よりも受信者側の導入負担が軽い. 以上より ID ベース署名は電子署名を既存のものより普及しやすく標的型攻撃への対策として十分であるといえる. 今後は Gmail 以外のメールサービスでの実装が必要であると考える.

（※文責: 青山慎太郎）

5.2.3 Google Apps Script

Google Chrome 拡張機能側の javascript から Gmail へのアクセスをするためには,Gmail 側で 2 段階認証やパスワードの生成などのセキュリティ設定をする必要があり, 使用者に負担を強いることになってしまう. そのため, メール本文の取り込みやメールへのファイル添付などの Gmail へのアクセスが必要な処理は Google Apps Script を使用することにした.Google Apps Script とは,Google が提供する各種サービスの自動化や連携を行うためのローコード開発ツールであり,Google Apps Script を使うと Gmail や Google スプレッドシート,Google ドライブなどの Google が提供する様々なサービス上で処理を自動化したり, 複数のサービスを連携させたりできるものである.Google Apps Script の開発は Web ブラウザで動作するため, 開発環境の構築が不要であり, 使用言語が javascript を基に作られているため,javascript を使用している場合は比較的簡単

に使うことが出来る. そのため, それ以前まで記述していたプログラムをほぼそのまま用いることが出来,Google のサービスの 1 つである Gmail に対するアクセスにも, 認証等を行う必要がなくなるため, 拡張機能と Gmail を結びつけるのに最適だと判断した. 拡張機能から Google Apps Script を呼び出すことで,Gmail から直接メールの本文取り込み, 添付が可能となり, さらに Google Drive へのアクセスもセキュリティ設定を行うことなく可能となったため, 機能の使用や実装の容易さという点においてかなり重要な役割を果たしたと考えられる.

（※文責: 野澤真生）

5.2.4 Google Chrome 拡張機能における実装

機能の使用や実装の容易さという観点を重視した結果,Google Chrome 拡張機能を用いての実装を行うことにした. しかし, 拡張機能側の javascript から Gmail にアクセスする処理を行うにあたって, 認証等セキュリティに関する設定を Gmail 側で行う必要がある関係上, 使用者が機能を容易に使用できるという観点から実装が不可能, もしくは困難であった. そのため,Google Apps Script を用いて Gmail からメール本文やアドレス等の必要な情報を抜き取り, 拡張機能側の javascript にそれを渡して暗号化を行い, また Google Apps Script に渡してメールに暗号文を添付するといった方法をとった. これにより, セキュリティ関連の設定をすることなく拡張機能から Gmail へのアクセスが可能となり, 容易な使用や実装といった目標が達成することができ, 当初の計画通りに,Gmail に対する電子署名機能を拡張機能として追加することが可能となった.

（※文責: 野澤真生）

第 6 章　各発表会の評価

6.1　中間発表会における評価

中間発表では暗号班,Web 班,CTF 班がそれぞれが作成したスライドを結合し, その結合したスライドを一人がすべて読むという形式で発表した. 発表のあと質疑応答の時間を取り質問が出た際はその質問の対象であるグループの担当者が質問に答えた.

また, 中間発表会で Google Form を使用して発表評価を実施し 40 件の評価をいただいた. 発表技術についての評価は平均で 7.025 であった. 発表技術に関してのコメントでは「1 人が全て話すのではなく, 役割を分担して, 班ごとにその班の人の発表を聞きたかった.」,「原稿を読んでいるだけのように感じて, 聴衆者を意識したほうが良いと思う」,「声が聞こえにくい」といったコメントが見られた.1 つ目のコメントに対しては班ごとに作成したスライドをそれぞれの班の担当者が発表を行うという形式に変えることで改善できると考えられる.2 つ目のコメントにはより発表練習を重ね, 話す内容を暗記し発表中は定期的に聴衆者に目を向けることで改善を図ることができると考える.3 つ目のコメントに対してはそもそも会場が広く声が響きやすい, 隣のプロジェクトとの距離が近いという問題があった. しかしもっと声量を上げる, 発表者の立ち位置を変える等の方法をとることで声が通りやすくすることは可能であったと考える.

発表内容についての評価は平均で 7.725 であった. 発表内容に関するコメントでは「それぞれの個別のグループの課題とか, 解決にあたって特徴的な部分などをより明確に示せれば良いと思う」,「説明が冗長に感じた」といったコメントが見られた.1 つ目のコメントに関しては具体例を交えて課題を分かりやすく説明する, 私たちの成果物が既存のものと比べてどこが優れているのか説明するといった改善案が考えられる.2 つ目のコメントに対しては発表内容を理解するために ID ベース暗号や電子署名等の基礎知識の説明が必要であるのでどうしても説明が長くなる. よって, イラストや図を効果的に活用することで冗長に感じさせない工夫が重要だと考える. 以上のように中間発表の評価では問題点や改善すべきポイントに対して指摘するコメントが散見された. 一方で「どの班も内容がおもしろそうでした. ウェブページができたら見てみたいと思います. 頑張ってください.」「暗号にすごく曖昧な理解しかしてなかったので, 具体的な説明があり分かりやすかった.」等の好意的なコメントも多く存在した. よって, 成果物発表会では中間発表会でのコメントを参考に発表に使用するスライドの内容や発表形式を改善し, 中間発表よりも時間を取り発表練習を行おうと考えている.

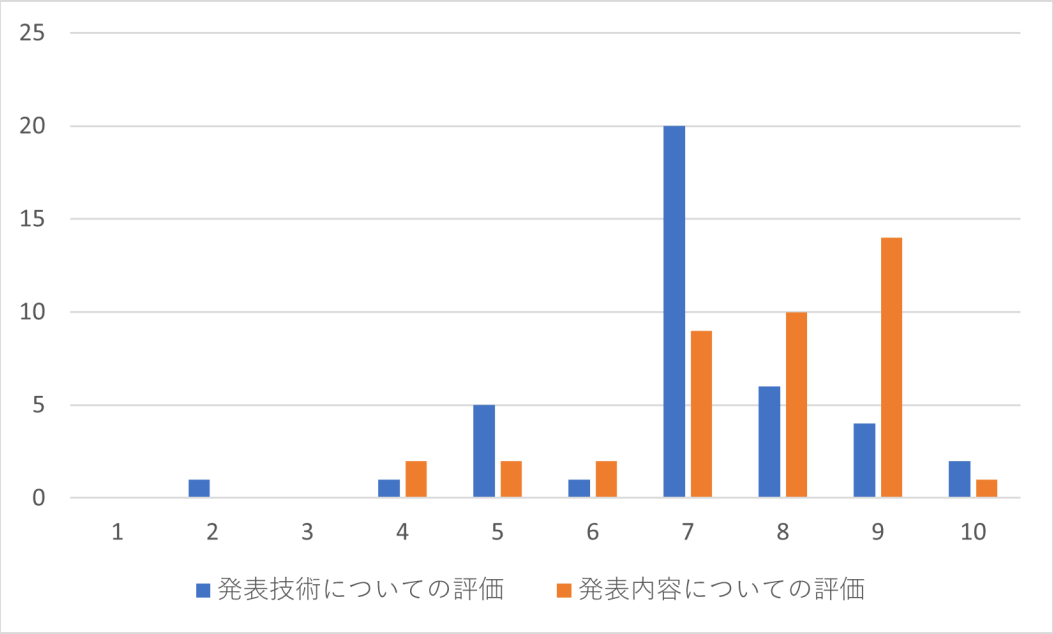

図 6.1　中間発表会アンケート結果

（※文責: 青山慎太郎）

6.2　成果発表会における評価

成果発表会における発表評価の集計には Google From を使用し,39 件の評価を頂いた. 発表技術についての評価の平均はおよそ 6.67 であった. 発表技術についてのコメントでは,「発表の際の声量が小さく, 聞き取れない箇所が多々あった」,「スマホで原稿を見すぎていて, もっと顔を上げながら発表した方が良いと思った」,「スライドの配色関係で見づらい箇所があった」,「差し棒を使用しての発表は分かりやすかった」,「難しい単語を 1 つ 1 つ説明していて良かった」,「班ごとに分けて発表していたのは分かりやすかった」などの意見が寄せられた.1 つ目のコメントに関しては中間発表の場所とは異なり, 体育館での発表となったため, 練習の際に声量をより出して練習する必要があったと考える.2 つ目と 3 つ目のコメントに関しては, 成果発表に対しての意識が低く, 資料作成や発表練習の際に聞き手への配慮を疎かにしてしまったためと考えられる.4 つ目と 5 つ目のコメントに関しては, 中間発表での反省を生かし, 理解が難しい部分を重点的にスライドにまとめて説明し, 読んでいる箇所が分かりやすいように差し棒を使用したことが良い結果につながったと考えられる.6 つ目のコメントに関しては, 中間と同様に班ごとに行ったことを細かく発表することによって, 各班の活動が分かりやすく説明することが出来ていたと考えることが出来る.

発表内容についての評価の平均はおよそ 7.67 と発表技術よりも高い評価を得られていた. コメントとしては,「具体的な成果物がどの程度出来ているのかが不明瞭であった」,「目標を十分に達成できていたのか理解出来なかった」,「疑似体験できるサイトを作ったり,CTF のサイト作っていたりなど, 実際に動かせる成果を出せていたのは良いことだと思いました」,「中間発表の時よりも全体的な完成度が上がっていたので良かった」などの意見が寄せられた. 本プロジェクトで扱った内容が比較的難しく, 何をしたのか伝わってこないという意見は一定数あり, これに関しては仕組み等を 1 つ 1 つを細かく説明したり, 図を積極的に用いる等, 分かりやすく説明するための工夫の検討を今後も引き続きすべきだと考える. 特に, 今回は成果物の実演よりも技術の説明のほうを重視

した発表を行ったため, 文章で仕組みや成果物の動きを想像しながら聞くことになってしまい, 使用した技術, 及び成果物における理解が追い付かなくなってしまったと考えられる. しかし, 評価全体でみると「将来性のある内容で良かった」,「プロジェクト学習としては良い成果と思われる」,「背景やアプローチの方法は面白かった」などの肯定的なコメントが多く, プロジェクトとしての方向性は良いものであったと言える.

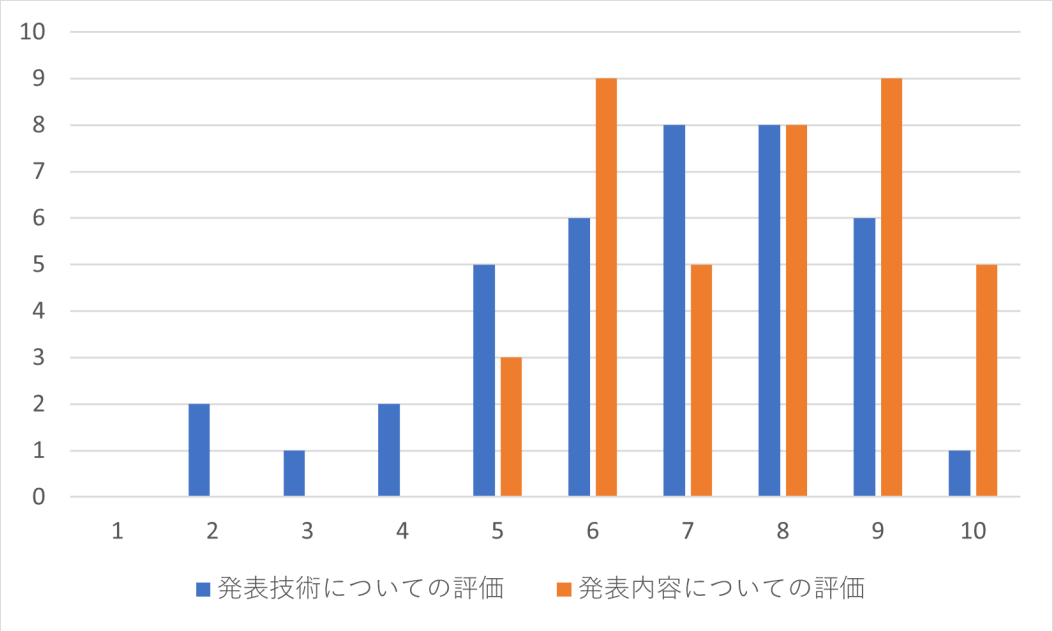

図 6.2　成果発表会アンケート結果

（※文責: 野澤真生）

第 7 章　まとめ

7.1　プロジェクトの成果

最初に, プロジェクトメンバー全員で暗号に関する知識の習得,CTF を用いた基本的なセキュリティ技術の習得を行った. その後, メンバー全員で本プロジェクトの目標を定め Google 拡張機能を利用した電子署名の実装を目指す暗号班, セキュリティ意識を向上させるための Web ページを作成する Web 班,CTF を通してセキュリティに関する知識と技術の底上げを目的とした CTF 班の 3 つのグループに分かれ活動を行った. 暗号班は Gmail に電子署名を実装するため Google 拡張機能や JavaScript について学習し, 共同開発の円滑化のために GitHub について理解を深めた.

暗号班では Google 拡張機能を効率よく開発するために Gmail 本文の取得, 電子署名の作成・検証,Gmail への電子署名の添付・取得の 3 つのグループに分かれて Google 拡張機能の開発を行った.Gmail の本文を取得するグループと Gmail への電子署名の添付・取得を行うグループでは JavaScript や Google Apps Script,HTML といった拡張機能や Web アプリケーションを開発するための技能や知識を習得することができた. 電子署名の作成・検証を行うグループでは上記の拡張機能開発に必要となる知識以外にも電子署名の作成・検証に使用する ID ベース暗号の知識を詳しく習得できた. さらに,Google 拡張機能や ID ベース暗号に関する知識, 技術以外にも共同開発におけるスケジュール管理や進捗状況の報告,Google 拡張機能の開発に関する情報の共有などメンバー間でのコミュニケーションをとることの重要性を学ぶことができた. また, 成果発表会では暗号について知識が乏しい人でも理解できるよう分かりやすくまとめる技術を培うことができた.

暗号班の具体的な成果物としては ID ベース暗号を用いた電子署名を Google 拡張機能で Gmail に実装した. 私たちが実装した電子署名は既存の電子署名と違い ID ベース暗号を利用しているため送信者の公開鍵が容易に取得可能であり, 導入負担が少ない. よって, 既存のシステムよりも世間への普及が容易くより強力なりすまし防止効果が期待できる. 以上より私たちの成果物は 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.

（※文責: 青山慎太郎）

7.2　プロジェクト内の自分の役割

7.2.1　東未来翔

前期

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担当した. また, 中間発表においては電子署名の説明および全体の編纂を担当した. 中間報告書作成においては, 報告書の理解に必要な前提知識の解説部分を中心に執筆を担当した.

後期

前期に引き続き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担当した. 特に進捗管理においては, 各メンバーへのイアリングを意識的に行い, 各メンバーが障害を乗り越えることの一助となることを特に意識した. また, 成果物作成においては電子署名の生成と検証にかかわる部分を担当した. 成果発表においては, 発表資料の校正および発表環境構築を担当した. 最終報告書作成においては, 中間報告書と同じく報告書の理解に必要な前提知識の解説部分を中心に執筆を担当した.

（※文責: 東未来翔）

7.2.2 中村碧

前期

前期はプロジェクトリーダーとして, グループごとの進捗の把握や中間発表に向けてのスケジュール確認, 提出物の確認など, プロジェクト全体として共有する必要のある情報や進捗を全員に伝えてきた. 認識を確認した後は, 各グループリーダーに進捗管理を任せ, 活動終了前にその日の活動内容を報告してもらい, 提出日の調整や必要であれば詳しく話を聞き, なぜうまくいかないのか問題点を話してもらった後, 解決の手助けを行った. 主にプロジェクト全体の進捗管理の担当を担っていた.

また, 暗号班では 1 メンバーとしてグループリーダーと意見を交換しながら, チーム開発を効率的に進めるための手法や提出物の確認, 週報の提出の代役など補佐役として活動した. チーム開発を効率的に進める手法として Github の活用を提案し, チームメンバーに Github の活用方法の学習を行った. 中間発表では, 主にポスター作成を担当し, 例年のポスターデザインに学びながらポスターを作製した. さらに, ポスターに記載する文章の作成,WEB 班と CTF 班からポスターの文章の提出管理, 査読を行いプロジェクトとして提出するポスター作製全般にかかわった. 後期では, グループ活動として使用言語の学習, プロジェクト全体としては各班の進捗報告の確認を行いたいと考えている.

後期

後期もプロジェクトリーダーとして, グループごとの進捗の把握, 成果発表にむけてのスケジュール確認, 各提出物の確認など, 前期同様にプロジェクト全体として共有する必要のある情報を全員に伝えてきた. こちらも前期と同じで, 全員の認識を確認した後, 各グループリーダーに進捗管理を任せる形でプロジェクトを進めた. 前期と異なったところは, 各グループで問題が起きることなくスムーズに進めたという点である. これは各グループリーダーが完璧に進捗管理を行っていてくれたおかげである.

そして, 暗号班では 1 メンバーとしてソフトウェア開発を行った. その中で私は GAS を使って送受信者のメール本文の取得とメールアドレス取得の機能の追加を担当した. 成果発表会では前期同様にポスター作成, 印刷を担当し, 暗号班の文章の更新とほかのグループの文章の更新を依頼しポスターに反映させた. 発表会当日は, プレゼンテーションをスライドを使って行い, 打合せの時間より長くなってしまったが, できるだけ補助資料を読まないことを意識して発表を行った.

（※文責: 中村碧）

7.2.3 青山慎太郎

前期

前期はプロジェクトメンバー全員で暗号について Pari/GP や CTF を用い学習した. その後暗号班として Google 拡張機能,JavaScript,GitHub など ID ベース暗号を用いた電子署名の開発に必要な基礎知識について学習した. 加えて実際に Web サイトの背景色を変更する, 短い文章をメモするといった簡単な Google 拡張機能を JavaScript や Google Apps Script を用いて作成することで Google 拡張機能を開発するための実践的なスキルを身に着けた. 中間発表ではスライドの ID ベース暗号の説明を行う箇所を図やイラストを用いて作成した. それに伴い同箇所の台本の作成も担当した. また, 中間発表会に向けて練習を重ね発表者として聴衆が聞き取りやすい発表を心掛けた. しかし電子署名を開発するには Google 拡張機能や ID ベース暗号について知識が不足していると感じるため後期は JavaScript や Google Apps Script についてさらに学ぶ必要があると考える. また中間発表会で得られたフィードバックを参考に成果物発表会では発表形式や発表内容をより分かりやすく改善するべきであると思われる.

後期

夏季休暇中に JavaScript について学習し実際に Google の検索結果のページで最下部までスクロールした場合自動で次のページに遷移するという Google 拡張機能を作成した. またこの拡張機能を開発したことで JavaScript だけでなく Chrome API に関して学習を行ったため, より高度な Google 拡張機能を開発できるようになった. 後期はまず ID ベース暗号を用いた電子署名を Google 拡張機能で Gmail へ実装するために担当する箇所を決める話し合いを行った. 結果,Gmail への電子署名の添付, 読み取り機能の開発を担当することとなった.Gmail への電子署名の添付・読み取り機能開発を通して JavaScript による下書きの本文取得や受信トレイ内のメールの ID 取得,Google Apps Script を用いた下書きへのファイル添付や読み取りについて学習した. また, もう一人の担当者と頻繁に進捗状況や開発に関する情報を共有することで機能開発の効率化に努めた. 成果物発表会では中間発表会での反省を踏まえ発表の担当箇所を分けて複数人で発表することとした. その結果, 前期に引き続き発表者として暗号班の成果物について発表した. 成果物発表会のフィードバックでは発表内容についておおむね好意的な評価が多かった. 一方で発表技術に関して改善点を指摘するコメントが散見された.

（※文責: 青山慎太郎）

7.2.4 岡本英太

前期

暗号やセキュリティについてプロジェクトメンバー全員で学んだ後, 暗号班に所属した. 引き続き暗号について学ぶとともに Google の拡張機能や javascript, 共同開発に使う github などに関する知識についても習熟させた. また, 暗号を用いた成果物について昨年の成果物などを踏まえて議論し, おおまかな見通しをたてた. 中間発表では主にポスター制作に関する役割を果たした. 印刷機の使い方を習い, 実際にポスターを印刷した. ポスターの内容においても文章の英訳や添付する画像の作成, 今後のスケジュールの部分を作成した. 当日の中間発表に関しては, 全面的にグループメンバーに任せる結果となった. 余裕を持ったスケジュールで中間報告書や中間発表の準備を進める

ことができたが, 成果物について具体的なプランはできていなかったため後期に持ち越した.

後期

Google の拡張機能を用いて学内メールに電子署名システムを実装することを最終成果とした. メール本文とメールアドレスから署名を作成, 検証する部分を主に担当した. ペアリング暗号ライブラリの mcl を使用することになり, また ID ベース暗号やそれを活用した電子署名の計算メカニズムに関する知識が足りていなかったため, コードを書くと同時に知識を習熟させていった. 署名に使用するハッシュ値やメール本文のハッシュ値の大きさを調節することに苦心した. グループメンバーとコミュニケーションを取り, 署名を生成・検証する部分のクオリティを高めることができた. 非常に時間がかかってしまったため, 成果物の完成を遅らせてしまったことに若干の申し訳なさがある. また, それによって, 成果発表の準備期間が短くなってしまった.

最終発表では, ポスターやスライドの画像の作成を担当した. 理解しやすい簡潔な図を作成することができた. 当日の発表も前期とは異なり一度行った. 聞き取りやすい声量で話すことができたが, 緊張によって原稿を飛ばしてしまったことが心残りである. 質疑応答においても正確な回答ができていなかったため準備不足を痛感した.

（※文責: 岡本英太）

7.2.5 北山奏

前期

前期はプロジェクトメンバー全員で RSA 暗号やシーザー暗号などの代表的な暗号について 学習した. また,Pari/GP を用いて実際に暗号化して復号するなどの動作を行ったり,CTF を用いて暗号を解読する作業を行った. その後, 暗号班として Google 拡張機能,JavaScript,GitHub など ID ベース暗号を用いた電子署名の開発に必要な基礎知識について学習した. 加えて実際に Web サイトの背景色を変更する, 短い文章をメモするといった簡単な Google 拡張機能を JavaScript や Google AppsScript を用いて作成することで Google 拡張機能を開発するための実践的なスキルを身に着けた. 中間発表ではスライドの作成を担当しプロジェクトの背景について記述した. それに伴い同箇所の発表原稿の作成も担当した. また, 中間発表会に向けて練習を重ね, 当日は発表のリハーサルを行い, 発表者として聴衆が聞き取りやすい発表を心掛けた. しかし電子署名を開発するには Google 拡張機能や ID ベース暗号について知識が不足していると感じるため後期は JavaScript や Google Apps Script についてさらに学ぶ必要があると考える. また中間発表会で得られたフィードバックを参考に成果物発表会では発表形式や発表内容をより分かりやすく改善するべきであると思われる.

後期

夏季休暇中に JavaScript について学習し実際に Gmail を開いたときにポップアップが表示される機能を作成した. 後期はまず ID ベース暗号を用いた電子署名を Google 拡張機能で Gmail へ実装するために担当する箇所を決める話し合いを行った. 結果,Gmail への電子署名の添付, 読み取り機能の開発を担当することとなった.Gmail への電子署名の添付・読み取り機能開発を通して JavaScript による下書きの本文取得や受信トレイ内のメールの ID 取得,GoogleAppsScript を用いた下書きへのファイル添付や読み取りについて学習した. グループメンバーがより高度な拡張機

能の技術を習得していたため, そのメンバーの意見を取り入れ, 話し合うことで開発は順調に行われた. ただ作業を分担したときに私の担当した部分の進行が遅かったため, 開発が少し遅れてしまった. 成果物発表会では中間発表会での反省を踏まえ発表の担当箇所を分けて複数人で発表することとした. その結果, 前期に引き続き発表者として暗号の成果物について発表した. 成果物発表会のフィードバックでは発表内容についておおむね好意的な評価が多かった. 一方で発表技術に関して改善点を指摘するコメントが散見された.

（※文責: 北山奏）

7.2.6 森谷史奏

前期

前期ではプロジェクトメンバー同士でコミューケーションを積極的に取り, プロジェクトメンバー同士が意見を積極的に出し合えるようになるようにおこなった. グループごとにわかれ暗号班に入ったのちは, どのような成果物の作成を行うか, そのプロセスをどう言ったものにするのか, どう言った知識や技術が必要になるのかの話し合いに貢献した. 成果物作成の準備として初めに,Google Chrome の拡張機能への ID ベース暗号を用いた電子署名の実装のため,Chrome の拡張機能,ID ベース暗号,JavaScript,html についてグループメンバーと共に知識の習得に取り組んだ. 中間発表では, スライド作成を主に担当しており, 中間発表では多くの人の目に触れることを心掛けより良いものになるように作成に励んだ. 中間報告書では達成目標の部分を担当しており, 自分達がどの部分に着手しており, 今後どういった作業が発生するのかの整理を行い作成した. 前期の時点では, 知識がまだ十分と言える状況ではなく, 成果物作成を行うための具体的なプロセスが出来上がっていなかったため, 後期では成果物作成の具体的なプロセスをグループメンバーと共に考えることから始める.

後期

後期では, 成果物作成に本格的に着手し, 成果報告会, グループ報告書作成を行った. 成果物では, グループ内で 3 つの班に割り振られ, 私は電子署名作成と, 署名検証の部分を担当した. 具体的な活動内容としては JavaScript を用いて,Chrome 拡張機能での電子署名の作成と署名検証の関数を同じ担当メンバーと共に作成した. 成果物作成のために必要な知識習得のために Web サイトや図書室などを用いて知識習得を行い, それと同時に関数作成に必要なライブラリの調査を行った. また, 成果報告会では, 成果物作成に時間を取られ, 限られた時間の中, スライド作成と発表原稿の作成を担当し, グループメンバーとコミュニケーションを取りながら発表スライドの作成に取り組んだ. 成果報告会当日では実際に発表も行い, 帰ってきたレビューでは好印象な回答が多く良い発表ができたと考えられる. 期末報告書では中間報告書同様, 到達目標の部分に携わり, グループがどのような目的をもって成果物の作成に取り組むかや, どのようなプロセスで目標達成を行うかの整理を行い, 中間報告書の作成したときより, より詳細に報告書の作成を行なった.

（※文責: 森谷史奏）

7.2.7 野澤真生

前期

前期はプロジェクトメンバー全員と積極的に交流し, 互いの意見を話しやすい環境作りを行った. 班ごとに分かれ, グループリーダーやプロジェクトリーダーが決定した後は, リーダーの人達が動きやすいように暗号班内で積極的に発言したり行動したりすることで, 話し合いがより円滑に進むような立ち回りを心掛けた.

前期時点での暗号班内の話し合いでは, 具体的な成果物の構想や共同開発の環境についてといった内容を取り扱い, 共同開発の手法として Github の利用を提案したり, メンバーが共有した ID ベース暗号や javascript,Google Chrome 拡張機能,Github 利用方法等の基礎知識についての学習を行った.

中間発表会ではポスター作成を担当し, 見出しや説明文のレイアウトや内容のチェックを行った. 同じくポスターを担当していたメンバーと情報を共有し, ポスターを見る人が見やすいように製作することを心掛けた.

前期の活動では, 成果物の構想があまり固まっていないので, 後期では前期に引き続き,ID ベース暗号や javascript 等必要な基礎知識の学習を続け, 個人としては実際にプログラムを組み, 期末提出物の確認, 作成を開始したいと考えており, プロジェクト全体としては成果物の方向性を定め, 実装に必要な部分の役割分担が行うことが出来れば良いと考えている.

後期

後期は前期と同様に, グループリーダーとプロジェクトリーダーを中心に他のメンバーと積極的にコミュニケーションをとり, 成果物の製作, 及びグループ報告書等の期末提出物の作成を行った. 前期での積極的な交流の結果, 特に大きな問題が生じることなく成果発表会を迎えることが出来た.

成果物作成に関しては, 暗号班として Google Chrome 拡張機能として動く ID ベース署名の作成を行った. その中で私はメール送信者側のプログラムを担当し, 受信者側を担当するメンバーとも連携して効率よく作業が出来た. 送信者側では,Google Apps Script を使用して送信する前の下書きの状態のメールから本文を抽出し, 得られた本文に対し SHA256 によるハッシュ化を行った. さらに, ハッシュ化によって得られた文字列を送信者側の Google Drive 上にあらかじめ作成したスプレッドシートに張り付けし, 他の部分を担当しているメンバーと結果を共有する形とした. また, 受信者側のメンバーには Google Drive 上にスプレッドシートを作成し, ハッシュ値を書き込むプログラムを提供し, 受信者側のメンバーからは Gmail のメール下書きを読み込むための条件式が提供されたりと, お互いが作業中に得られた有用な情報を共有できていた. こちらの進捗状況に対し日報のようなものを作り, 今日行ったことや次回行いたいこと, 参考にしたサイトの URL 等をできるだけ細かく記録することで, お互いの状況がオープンになり, プログラムが動かなくなったとしても対処しやすいように努めた.

成果物発表会ではスライドとポスターの両方の作成に携わり, スライドの内容や原稿に不備があるかどうかや, ポスターの印刷の手伝い等を行った. 発表練習の際にはスライドの原稿をよくすり合わせ, より良いものになるよう行動した.

（※文責: 野澤真生）

7.3 今後の課題

今回は, 標的型攻撃に対するセキュリティの強化を目的とした成果物の作成を行っており, 現在利用されている S/MIME よりもコストが低いシステムを構築することが目標であった. その目標を達成するために, 導入が容易である Google Chrome 拡張機能を用いての実装を行ったが, 拡張機能の特性上,Gmail から直接メール本文を抽出することや, メールに対して暗号化を行った結果ファイルを添付するといった際に,Google サービス側でセキュリティの設定を行う必要があることが判明した. この課題については,Google 側から提供されている Google Apps Script を拡張機能と連動させることで, セキュリティの設定を行うことなく目的としていた動作をさせることが可能となったため, 解決したと考えることが出来る.

Google Chrome 拡張機能と Google Apps Script を用いた方法では,Gmail に対する処理しか行うことが出来ない. したがって, メールというもの全てに対しての電子署名機能を実装するためには,Gmail のみならず,Outlook や iCloud 等の他のメールサービスにおいても同様の機能を持つシステムを構築する必要があり, ユーザーの使うメールサービスに関係なく利用できるシステムを作ることが求められると考えられる.

拡張機能と Google サービス間の処理を行うための開発に, 当初予定していた以上の製作期間を使ってしまい, ユーザーインターフェースに対する配慮を疎かにしてしまった. 機能に対する説明や今何を行っている状態なのか等を表示し, ユーザーがより安心して使える仕様にすべきであると考える.

メール送信者が元々ウイルスなどに感染していた場合は, 今回作成したシステムでは電子署名の有意性が低くなってしまう. セキュリティの強化という点においては, ユーザー側の状態を調べ, ウイルスに感染していた場合は安全性を確保できないなどの警告を出して, ユーザー側に対処を要請するといったシステムも実装できれば良いと考える.

昨年や一昨年と同様に,Google Chrome のブラウザ上で開発を行ったが,Firefox などの他のブラウザに対しての開発を行っていくことも実装の幅が広がるため必要であると考える.

（※文責: 野澤真生）

付録 A　新規習得技術

電子署名　公開鍵暗号
Javascript
GAS(Google Apps Script)
html CSS
ID ベース暗号
ID ベース署名

付録 B　活用した講義

講義名　情報機器概論, 情報ネットワーク
活動内容　暗号の仕組みの基礎知識として活用した.

参考文献

[1]（株）リケン. 当社サーバーへの不正アクセスに関するお知らせ（第三報）, 2022/12/23.
https://www.riken.co.jp/upload/2AGBAST-newsja$_f$*ile.pdf*

[2]（株）デンソー. デンソー独法人にサイバー攻撃　機密情報公開で脅迫か, 2022/12/23.
https://www.nikkei.com/article/DGXZQOFD1322C0T10C22A3000000/

[3] IPA. 情報セキュリティ１０大脅威, 2022.
https://www.ipa.go.jp/files/000096258.pdf

[4] トレンドマイクロ（株）. 国内標的型サイバー攻撃分析レポート, 2016.
https://www.trendmicro.com/content/dam/trendmicro/global/ja/security-intelligence/research-reports/sr/pdf-sr2016-annual-20170321-03.pdf