公立はこだて未来大学 2020 年度 システム情報科学実習
グループ報告書

Future University-Hakodate 2020 System 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

メールアドオン班

Group Name

Mail Add-on Team

プロジェクト番号/Project No.

15-A

プロジェクトリーダ/Project Leader

酒井竜馬　Ryouma Sakai

グループリーダ/Group Leader

佐藤隼斗　Hayato Sato

グループメンバ/Group Member

菅文人　Fumihito Kan
酒井竜馬　Ryouma Sakai
佐藤隼斗　Hayato Sato
吉田琉夏　Ruka Yoshida

指導教員

白勢政明，由良文孝

Advisor

Shirase Masaaki，Fumitaka Yura

提出日

2021 年 1 月 14 日

Date of Submission

January 14, 2021

概要

本プロジェクトは，主に暗号技術を用いて，セキュリティに関する分野の理解を深め，実際に体験することを目的としたプロジェクトである．本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てきている．ここで重要になってくるのが，情報を守り，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方法や現在の対策について学習し，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する．

キーワード　PGP 署名，S/MIME，ID ベース署名

（※文責: 佐藤隼斗）

Abstract

The purpose of this project is to deepen understanding of security related fields by using encryption technology and to experience them in practice. This year, with the increase in online lessons and remote work due to the influence of the new coronavirus, information management has become even more important. What is important here is security technology that protects and manages information, and crisis management for our users who handle it. Therefore, in this year's activities, we learn about attack methods with security vulnerabilities and current countermeasures, divide the members into two groups, deepen their understanding, and propose more effective countermeasure methods and raise awareness an the final goal.

Keyword PGP(Pretty Good Privacy), S/MIME, ID-based signature

（※文責: 佐藤隼斗）

目次

第 1 章　背景

1.1　背景

昨今，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取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く離れている人との意思の疎通・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えている．このような攻撃の一つは標的型攻撃 (APT) と呼ばれており，関係者を装い電子メール等に添付されたウィルスで組織や個人の内部システムを攻撃することである．そして，情報処理推進機構によると，標的型攻撃は「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 [1]．この攻撃の対策としては，一般の利用者に対しては電子メールに重要なもののみではなく，全てのファイルの添付を止めるような喚起や，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，電子メールの認証や電子署名の検証を行うことで攻撃を防止している．しかし，対策から生じる電子メールの不便さやヒューマンエラー，署名生成や署名検証の煩さ・イニシャルコストの高さにより，標的型攻撃の被害は増え続け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．

（※文責: 酒井竜馬）

1.2　目的

本プロジェクトの活動では，標的型攻撃を防ぐことが出来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 [2] によって提案された公開鍵暗号方式の一種である ID ベース暗号を用いた過去の卒業生の研究をさらに進めることを目的とする．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煩雑さを解消出来ると考えられる．このことから，過去の研究では ID ベース暗号による鍵生成および電子署名の正当性や安全性についての活動が行われていた．具体的には，電子メールのメッセージの暗号化および復号による正当性の評価，また，メールアドレス等の公開鍵と鍵生成局のマスター鍵を用いて秘密鍵を生成し，電子メールを送る際に，その秘密鍵を用いて署名生成，および公開鍵を用いて署名検証を行うことである．この署名生成および署名検証によって，電子署名の煩雑さを抑え，標的型攻撃による被害を防止することが出来ると考える．本プロジェクトでは，このシステムを利用したメールクライアントソフトの開発による標的型攻撃への対策手法の確立を目指す．

（※文責: 酒井竜馬）

1.3　従来例

従来の電子メールの通信には，通信の秘匿性の保証や，なりすまし検知のために S/MIME とよばれるセキュリティ技術が利用されている．S/MIME(Secure / Multipurpose Internet Mail

Extensions) とは，電子メールのセキュリティを向上する暗号化方式の一つで，電子証明書を用いてメールの暗号化とメールへ電子署名を行うための技術である．S/MIME の方式を用いるには，送信者と受信者の両方が S/MIME に対応する電子メールソフトを使用している必要がある．S/MIME で使用されている電子署名は，公開鍵暗号方式に基づいて実現されている．

電子署名の技術には，鍵生成アルゴリズム，署名生成アルゴリズム，署名検証アルゴリズムの 3 つのアルゴリズムがある．鍵生成アルゴリズムは，公開鍵と秘密鍵を生成するアルゴリズムであり，実行する際，セキュリティパラメータと呼ばれる値をこのアルゴリズムに入力する．セキュリティパラメータは，署名文を偽造することの困難さを表した尺度である．さらに鍵生成アルゴリズムには乱数も入力され，実行するたびに異なる乱数が選ばれるため，ユーザ毎に異なる公開鍵と秘密鍵が割り振られることになる．秘密鍵は署名生成に使われ，公開鍵は署名検証に使われるため，秘密鍵，公開鍵はそれぞれ署名鍵，検証鍵とも呼ばれる．電子署名を行う際に，署名生成アルゴリズムを実行する．生成した二種類の鍵のうち，秘密鍵を使用して署名文を生成する．送信したいデータと秘密鍵を用いて，署名を生成し，データと署名を相手に送信する．データと署名を受け取った相手は，署名検証アルゴリズムを実行することで，署名が正しいかどうかを検証する．署名検証アルゴリズムは，送信者の公開鍵を用いて検証を実行する．

送信者は署名を生成する際，データとともに自分の秘密鍵を使用する．送信者の秘密鍵を知っているのは署名を生成した送信者本人だけなので，送信者以外の人は同じ方法で同じ署名を作成することは出来ないことになり，この性質が電子署名を付した電子文書の作成者を識別する根拠になる．署名検証をする際，公開鍵が有効かどうか調べる必要がある．そのために，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．データと署名を送信する際，電子証明書も一緒に送信する．それらを受け取った受信者は，電子証明書が有効であるかどうかを第三者機関に確認する．有効であった場合，公開鍵を使用して署名検証を行う．

電子証明書の発行および検証を行う第三者機関は，認証局 (CA:Certification Authority) と呼ばれる．認証局は，電子証明書の申請者が提出した所有者情報を審査する機関である登録局 (Registration Authority)，登録局からの要求に基づいて実際に電子証明書の発行や失効を行う機関である発行局 (Issuing Authority)，ならびに認証局に関する情報や電子証明書の有効性に関する情報を提供するリポジトリから構成されている．受信者が送信者の公開鍵を使って署名検証を行うという S/MIME を利用する上では，認証局の存在が必須である．

（※文責: 菅文人）

1.4 従来の問題点

S/MIME の導入には以下のような問題点がある．

- 年間にかかる費用が高い
- 導入や運用の手間やコストがかかる
- 送信者と受信者の両方が S/MIME に対応している必要がある

S/MIME を利用するためには，信頼できる第三者機関から S/MIME 証明書を発行してもらう必要がある．GMO グローバルサイン株式会社 [3] が提供する S/MIME 証明書を使用する場合，有効期間 1 年の証明書において 1 メールアドレスに付き 52,000 円の費用がかかり，全学生及び全職員分の証明書を取得すると多額の費用がかかってしまう．また，有効期間は 1〜3 年の間で選択

するため，学部 4 年間の中で必ず 1 度は更新作業をしなければならない．また，メールを利用するために全員が S/MIME に対応したメールソフトを使う必要がある．

（※文責: 菅文人）

1.5 課題点

上記の問題点を解決するための具体策として，ID ベース暗号を用いた ID ベース署名方式がある．ID ベース暗号とは，メールアドレスなどの ID を公開鍵とした公開鍵暗号方式である．ID ベース署名方式では，ID ベース暗号方式に基づいた公開鍵と秘密鍵を利用する．公開鍵にはメールアドレスなどの ID を使用し，秘密鍵には鍵生成局が生成した鍵を使用する．鍵生成局を，大学内で管理できれば第三者機関の認証局は必要なくなり，費用がかからない．また，公開鍵はメールアドレスそのものであるため，公開鍵が有効であることを示す電子証明書も不要になる．大学のメールでは，全員が同じ Web メールを使っているため，ID ベース署名の機能を有した Web メールシステムを構築することができれば，大学内間通信において標的型攻撃を防ぐことが出来る．Web メールシステムを構築するには，Web サーバやメールサーバの構築設定が必要となり，鍵生成局の運用もしなければならない．プロジェクト学習の期間を考慮し，今回はブラウザ拡張機能として ID ベース署名システムを実装する．

（※文責: 菅文人）

第 2 章　到達目標

2.1　問題設定

1. 1 節で述べた通り，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．しかし，既存の対抗技術である S/MIME(電子署名) は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こと，送信者と受信者の両方のメールシステムが対応している必要があるにも拘わらず，相手のメールシステムが対応しているか判らないことなどからあまり普及していない．そこで，本グループでは，S/MIME 導入の障害となっている上記 2 つの理由「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」に着目し，電子署名が普及していないことで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ことを問題として設定した．

（※文責: 佐藤隼斗）

2.2　課題設定

2. 1 節では，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した．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した．その結果，暗号技術を学ぶために並行して行っている 2019 年度の卒研生の発表資料修正から着想を得て，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．そこで，本グループでは，ID ベース署名機能を搭載したメールシステムを作成することを目的として活動していくことになった．

（※文責: 佐藤隼斗）

2.3 ID ベース暗号について

2.3.1 概要

ID ベース暗号は，任意の文字列を公開鍵として暗号文を作成可能な暗号化技術であり，1984 年から Shamir[4] を始めとして研究が行われていた．しかし，当時の ID ベース暗号の一部は暗号化のために膨大な計算時間を費やしてしまうため，ID ベース暗号の実用には至らなかった．その後，実用的かつ安全性のある ID ベース暗号が研究され，さらに 2001 年には，Boneh，Franklin らによる ID ベース暗号が提案されており，BF 方式と呼ばれている [2]．この方式は，双線形ペアリングを用いており，メッセージの暗号化および復号を行うことができるアルゴリズムを提案している．ID ベース暗号における公開鍵には住所や氏名，メールアドレス等の ID の文字列が使われる．この時，利用者が有限であったり，組織がオープン化されていない範囲内であれば，公開鍵の所有者が明確となる．そのため，認証局の公開鍵証明書の発行および管理の必要がなくなり，従来の PKI が不要となる．

秘密鍵は，公開鍵である ID から生成される．生成には，公開鍵のほかに，鍵生成局が持つマスター鍵が必要となる．鍵生成局に公開鍵を渡すと，鍵生成局のマスター鍵に対応する秘密鍵が生成される．ID ベース暗号を用いた電子署名では，鍵生成局から生成された秘密鍵からの署名の生成や，公開鍵で署名の検証を行うことができるため，メール送信相手のメールアドレスを公開鍵として署名検証を行うことで，なりすましメールを防ぐことができる．また，宛先のメールアドレスを公開鍵としてメール本文や添付ファイルを暗号化することで，メールのデータが漏洩しても，復号されない限り情報は守られる．

（※文責: 菅文人）

2.3.2 ID ベース暗号の理論

ID ベース暗号を構成する暗号方式は双線形ペアリングを用いる楕円曲線暗号で，楕円曲線上の 2 つの点の組からある有限体の写像を用いる手法が用いられる．ペアリングとは，2 入力 1 出力の双線形性を持つ写像である．ペアリングに関する数学的な説明をする [5].

G_1,G_2 を加法に関する巡回群，G_3 を乗法に関する巡回群とし，以下の写像 e が双線形性および非退化性を満たす時，e はペアリングと定義される．

$$e : G_1 \times G_2 \to G_3 \tag{2.1}$$

次に，双線形性と非退化性をもつペアリングについて説明する．ペアリングの双線形性は

$P_1, P_2 \in G_1$，$Q_1, Q_2 \in G_2$ に対して，以下の式を満たす．

$$e(P_1 + P_2, Q_1) = e(P_1, Q_1)e(P_2, Q_1) \tag{2.2}$$

$$e(P_1, Q_1 + Q_2) = e(P_1, Q_1)e(P_1, Q_2) \tag{2.3}$$

ペアリングの非退化性は $P \in G_1$，$Q \in G_2$ が存在し，以下の式を満たすことである．

$$e(P, Q) \neq 1 \tag{2.4}$$

よって，このペアリングの定義から，$a,b \in \mathbb{Z}$ に対して，以下の式が成り立つ．

$$e(aP, bQ) = e(bP, aQ) = e(P, Q)^{ab} \tag{2.5}$$

式 (2.1) が G_1=G_2 の場合は対称ペアリングといい，$G_1 \neq G_2$ の場合は非対称ペアリングと呼ばれる．近年は非対称ペアリングが主に用いられるようになっており，対称ペアリングに対して計算の処理速度が速いという点で注目を浴びている．

（※文責: 菅文人）

2.3.3 暗号化・復号

次に，暗号化び復号のアルゴリズム [2][6] について説明する．

1. 楕円曲線 E/F_q において，$E[n] \subset E(F_{q^k})$ があるとする．
2. 鍵生成局はマスター鍵 $s \in Z_n^*$ を選択する．また，$P \in E[n]$ を選び，Q=sP を計算して P と Q を公開する．なお，マスター鍵は一定期間変更しない．
3. ハッシュ関数 H_1，H_2 を公開し，選択する．

$$H_1 : \{0,1\}^* \to E(F_q), H_2 : E(F_{q^k}) \to \{0,1\}^n \tag{2.6}$$

4. Alice の公開鍵を P_A=$H_1(ID)$ とする．

秘密鍵生成:

Alice の秘密鍵を S_A=sP_A とする．

暗号化:

Bob は Alice の公開鍵 P_A を用いて，暗号文 C を生成する．また，乱数 $x \in Z_q^*$ を選択する．

$$C = (C_1, C_2) = (xP, m \cdot H_2(e(Q, xP_A))) \tag{2.7}$$

復号:

Alice は秘密鍵 S_A を用いて，暗号文 C を復号する．

$$m = C_2 / H_2(e(S_A, C_1)) \tag{2.8}$$

（※文責: 菅文人）

2.3.4 署名生成・署名検証 (対称ペアリング)

次に，署名生成・署名検証のアルゴリズムを説明する [7].

1. G_1 を素数 q の群とする．また，P は G_1 の生成元とする．
2. 暗号化ハッシュ関数は以下のように選び，選択する．

$$H_1 : \{0,1\}^* \to G_1, H_2 : \{0,1\}^* \to Z_q, H_3 : G_1 \to Z_q \tag{2.9}$$

3. 鍵生成局は，マスター鍵 $s \in Z_q^*$ を選択する．また，鍵生成局の公開鍵 P_{pub}=sP を計算する．なお，マスター鍵は一定期間変更しない．

秘密鍵生成:

Alice の公開鍵 ID を用いて，計算に用いる Q_{ID}=H_1*(ID)* と，Alice の秘密鍵 S_{ID}=sQ_{ID} を計算する．

署名生成:

Alice は秘密鍵 S_{ID} を用いて，メッセージ m に署名を行う．また，乱数 $k \in Z_q^*$ を選択する．ここで R=kP とし，メッセージ m の署名は *(R,S)*$\in G_1 \times G_1$ とする．

$$S = k^{-1}(H_2(m)P + H_3(R)S_{ID}) \tag{2.10}$$

署名検証:

Bob は Alice の公開鍵 ID を用いて，以下の計算が成り立つ場合メッセージ m の署名 *(R,S)* は検証が通る．

$$e(R,S) = e(P,P)^{H_2(m)} \cdot e(P_{pub}, Q_{ID})^{H_3(R)} \tag{2.11}$$

（※文責: 菅文人）

2.3.5　署名生成・署名検証 (非対称ペアリング)

2.3.4 では，対称ペアリングを用いた署名生成・署名検証のアルゴリズムを説明した．2.3.4 のアルゴリズムを非対称ペアリングに変換した署名生成および署名検証のアルゴリズムを説明する．[7].

1. G_1 と G_2 を 2 つの素数 q の群とする．また，P_1 は G_1 の生成元，P_2 は G_2 の生成元とする．
2. 暗号化ハッシュ関数は以下のように選び，選択する．

$$H_1 : \{0,1\}^* \rightarrow G_1, H_2 : \{0,1\}^* \rightarrow Z_q, H_3 : G_1 \rightarrow Z_q \tag{2.12}$$

3. 鍵生成局は，マスター鍵 $s \in Z_q^*$ を選択する．また，鍵生成局の公開鍵 $P_{pub} = sP_2$ を計算する．なお，マスター鍵は一定期間変更しない．

秘密鍵生成:

Alice の公開鍵 ID を用いて，Alice の秘密鍵 $S_{ID} = sH_1(ID)$ を計算する．

署名生成:

Alice は秘密鍵 S_{ID} を用いて，メッセージ m に署名を行う．また，乱数 $k \in Z_q$ を選択する．ここで $R = kP_2$ とし，メッセージ m の署名は *(S,R)*$\in G_1 \times G_2$ とする．

$$S = k^{-1}(H_2(m)P_1 + H_3(R)S_{ID}) \tag{2.13}$$

署名検証:

Bob は Alice の公開鍵 ID を用いて，以下の計算が成り立つ場合メッセージ m の署名 *(S,R)* は検証が通る．

$$e(S,R) = e(P_1,P_2)^{H_2(m)} \cdot e(H_1(ID), P_{pub})^{H_3(R)} \tag{2.14}$$

（※文責: 菅文人）

2.4　到達レベル・具体的な手順

2．2 節より，電子署名を普及させるためには低コストな電子署名が必要であると考えた．そこで，公開鍵証明書の必要ない ID ベース署名機能を搭載したメールシステムの実現が目標となった．そのための手法として，私たちのグループではメールクライアントでの実装を行うことになった．今年はプロジェクト学習の始まりが遅かったことも影響し，前期活動では設計までしか行えなかったため，開発は夏季休暇中に行った．しかし，後期活動に入りプログラムを統合しようとした際に問題が発生したため，メールアドオンでの開発に仕様変更をした．詳細を下記に示す．

（※文責: 佐藤隼斗）

2.4.1　前期活動

ID ベース署名機能を搭載したメールクライアントを作成し，問題なくメール本文及び添付ファイルの送受信ができることを目標とする．なお，開発環境は Visual Studio 2019 を使用し，対応 OS は Windows のみとする．また，ベースとなるメールクライアントとしてオープンソースソフトウェアである「nPOP」を使用する．作成するメールクライアントはハイブリッド暗号方式を採用し，本文と添付ファイルの暗号化には OpenSSL の AES を用いる．また，共通鍵の暗号化と電子署名には ID ベース暗号を用いる．この時，ID ベース暗号のプログラムは卒研生が実験に使用したプログラム [5] を参考に作成する．

（※文責: 佐藤隼斗）

暗号化手順

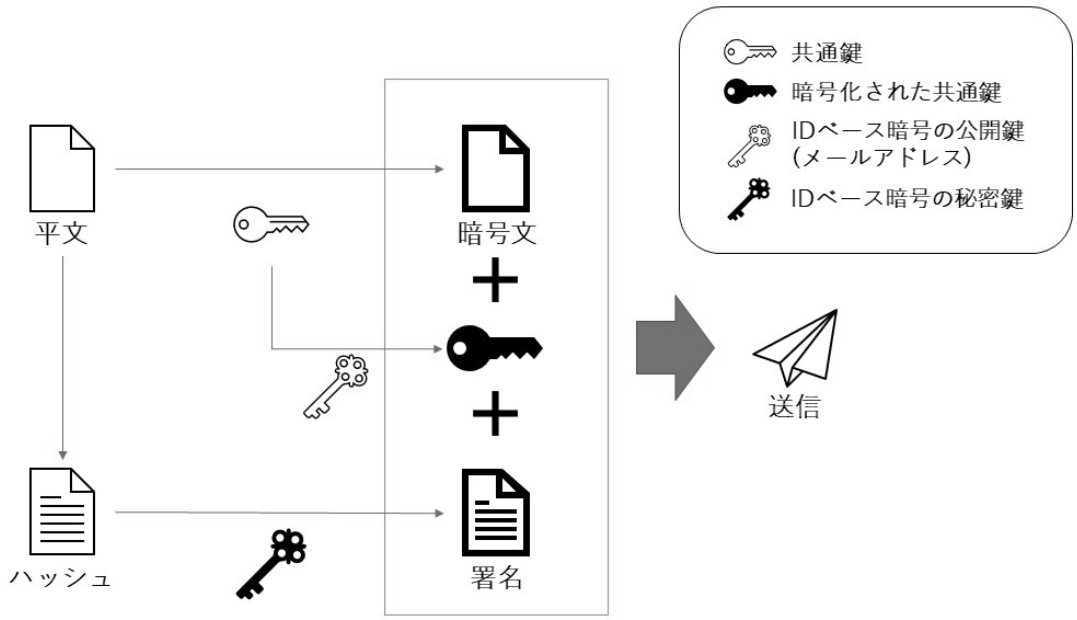

図 2.1　暗号化手順

1. 平文があることを前提とする
2. 平文からハッシュ値を計算する
3. 得られたハッシュ値を ID ベース暗号の秘密鍵で署名生成する
4. ランダムに共通鍵を生成する
5. 平文を共通鍵で暗号化する
6. 共通鍵を ID ベース暗号の公開鍵で暗号化する
7. 暗号文に暗号化された共通鍵を付ける
8. 署名を暗号文の文末に追加する
9. 暗号文を送信する

（※文責: 佐藤隼斗）

復号手順

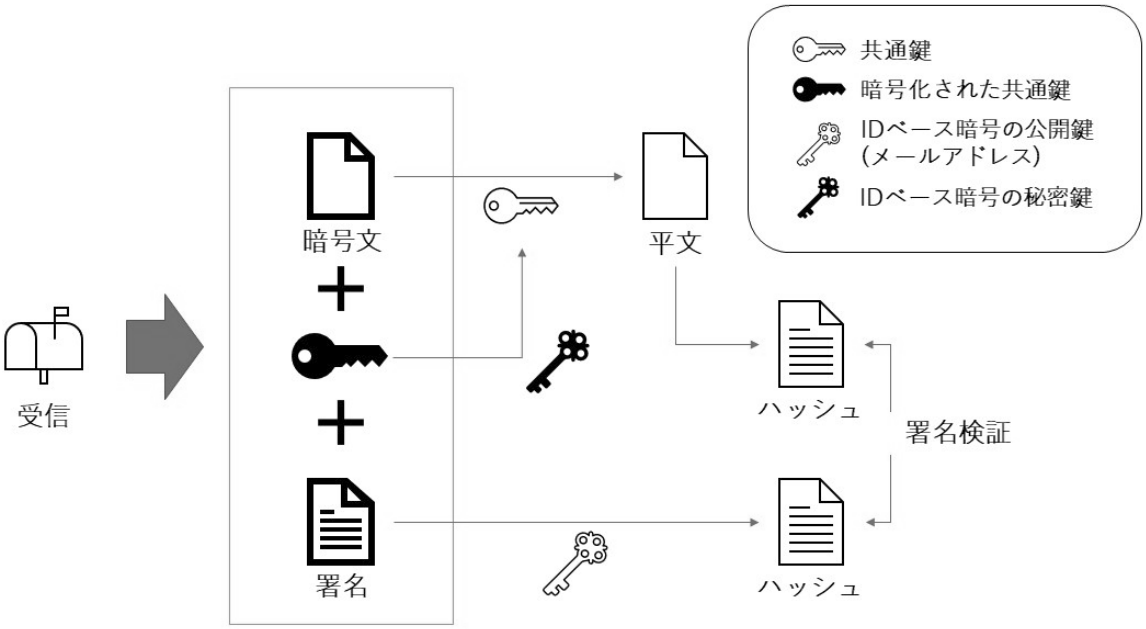

図 2.2　復号手順

1. 暗号文を受信する
2. 暗号文の文末から署名を切り取る
3. 暗号文から暗号化された共通鍵を切り取る
4. 暗号化された共通鍵を ID ベース暗号の秘密鍵で復号する
5. 暗号文を共通鍵で復号し，平文を取得する
6. 平文からハッシュ値を計算する
7. 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
8. ハッシュ値を比較する (署名検証)
9. 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: 佐藤隼斗）

課題の割り当て

各人の得意分野及び関連性，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．

1. 暗号化・復号グループ (佐藤・吉田)
   メール本文と添付ファイルの暗号化・復号を行う．なお，ファイルの暗号化・復号には OpenSSL の AES を使用し，共通鍵の暗号化・復号のみ ID ベース暗号を用いる．
2. 電子署名グループ (酒井・菅)
   メール本文と添付ファイルの電子署名を作成する．この時，電子署名は ID ベース署名を用いることで，公開鍵証明書が必要のない状態にする．

（※文責: 佐藤隼斗）

2.4.2 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深め，１年間の活動の指標を決める足掛かりとして，前年度の卒研生の作成したスライドの修正を行なった．本グループの前期の活動計画としては，ID ベース署名機能を搭載したメールクライアントを作成し，問題なくメール本文及び添付ファイルの送受信ができることを目標として活動した．なお，開発環境は Visual Studio 2019 を使用し，対応 OS は Windows のみを暫定的な目標として活動を開始した．前半の活動では ID ベース暗号やそれを用いた電子署名の仕組みを，先行研究として卒研生の論文を読み具体的なプログラムや検証方法を学習した．しかし，メールソフトに関する事前知識や理解が乏しかったことやプログラムの記述が追いついていなかったためにオープンソースソフトウェアを基にしたメールクライアントソフトの実装には至らなかった．夏季休暇中に暗号化実装部分や署名検証などのプログラムの担当を割り振り，後期初めでの組み込み，動作を目標として前期の活動は終了した．中間発表では，発表内容に関しては及第点であったが，発表技術や発表物に関して，発表後に実施したアンケートではあまり良い反応ではなかった．発表に際して使用したのはポスターと発表用の Web サイトであった．プロジェクト全体の活動で作成した修正後のスライドも同 web サイトに掲載した．初期段階での活動で使用した具体的なコメントでは，「表を活用してもう少しグラフィカルに」「内容をかいつまんで簡潔に」などが上がっており，質疑応答の際も，質問の回答に時間がかかってしまったり，適切な回答をすることができなかったりなど，全体を通して良い出来であったとは言えなかった．これらの点を把握し，中間発表で正確に回答することができなかった質問，意見と合わせて，後期の活動あるいは最終発表に生かせるようにプロジェクト全体での共有を図った．スライド修正に関しては特に指摘やコメントがなかったため，細かい体裁の修正ののち後期での修正作業は必要ないと判断した．

（※文責: 酒井竜馬）

2.4.3 後期活動

後期の活動にあたり，前期終了前に割り振ったプログラムを OSS に組み込み動作確認を試みたが，予想している結果・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．具体的には，32 ビット版と 64 ビット版での，メモリーやドライ

ブ（HDD など）の容量の上限が挙げられる．このままでは当初の目標である Windows のみでの動作もままならないと判断し，この実装方法を放棄し，代替案による解決を行うこととした．いくつかの案を出し合い，議論したのち，最終的には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を利用することで ID ベース暗号による電子署名を実装することとした．これによって，OS による実装方法の違いや，挙動の不備を軽減することができた．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．また，学内メールによる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る．また，機能面では，CC や BCC を用いた一斉送信には対応しておらず，使用できるブラウザも Google Chrome のみの 1 つとなってしまった．

（※文責: 酒井竜馬）

署名生成

1. 署名生成および署名検証に必要な公開パラメータと乱数を生成する
2. Firebase 認証にログインし，鍵生成局へのアクセストークンを取得
3. アクセストークンを鍵生成局へ送信し，自身の ID に対応した秘密鍵を取得
4. 公開パラメータと乱数と秘密鍵を使用し，メール本文の署名文を生成する
5. 署名検証に必要な公開情報と署名文を JSON データに変換
6. JSON データを文字列に変換し，メール本文の末尾に付け加えて送信する

（※文責: 菅文人）

署名検証

1. Firebase 認証にログインし，鍵生成局へのアクセストークンを取得
2. 受信したメッセージの末尾についている文字列から JSON データを読み取る
3. JSON データから署名検証に必要な公開パラメータを取得
4. アクセストークンと公開パラメータの情報を鍵生成局に送信し，鍵生成局の公開鍵を取得
5. 取得した公開情報とメール本文をもとに署名検証を行う

（※文責: 菅文人）

2.4.4 後期活動のフィードバック

後期活動では，夏季休暇中に作成した ID ベース暗号を使用した暗号化・復号プログラム及び署名生成・署名検証プログラムを nPOP に実装しようとしたが，プログラムに必要な mcl ライブラリと nPOP のビット非互換により実装することができなかった．そこで話し合いを行い，メールクライアント作成からメールアドオン作成へと仕様変更をすることにした．これにより，mcl ライブラリと nPOP のビット非互換だけでなく，mac 版・linux 版での対応も解決することができた．仕様変更によりスケジュールが厳しくなると思われたが，事前に作成していた c 言語のプログラムを JavaScript 用に書き直し流用することでスムーズに作業を進められた．また，最初期は想定していなかった鍵処理や鍵の更新処理まで実装することができたため，当初予定していたものより実

用的なシステムになった．しかし，ID ベース署名をブラウザ拡張機能で実装したことによる弊害も発生した．この件に関しては，4．2 節で述べる．

最終発表では，セキュリティの勉強の際に使用したスライドと自分たちで作ったプログラムの動作を交えた説明動画を事前に公開しておき，発表時間には質疑応答を中心として発表した．質疑応答の前にプロジェクトの簡単な説明がある点と質疑応答の際に適切な回答をしている点で高評価を得ることができた．また，発表後はアンケートの結果からフィードバックを行った．スライドが小さくて見づらい，噛んだ場合は動画を取り直した方が良いなどの意見があったため，次に発表を行う際の反省点とした．

（※文責: 佐藤隼斗）

第 3 章　プロジェクト内のインターワーキング

3.1　菅文人

前期

ID ベース署名を実現するメールシステムの構築方法の提案を行った．ベースとなるメールクライアントソフトの調査や，開発環境の整備に関する情報共有を行った．7 月の中旬に行われたプロジェクト学習中間発表に向けて，プロジェクト紹介用ホームページの製作を行った．ホームページの構成やコンテンツを制作し，プロジェクトのメンバーにフィードバックを受けながら修正を繰り返した．

後期

後期活動の初めに，メールシステムの仕様変更を行った．前期までに予定していた方法は nPOP というオープンソースのメールクライアントソフトに ID ベース署名機能を追加するという方法だったが，nPOP と ID ベース署名の実装に必要な mcl ライブラリのビットバージョンに互換性がないため，ブラウザ拡張機能として実装することになった．仕様変更により新たに必要となった鍵生成局の設計から構築までを行った．鍵生成局から鍵を取得する際に，ユーザを認証するための認証基盤が必要となるが，学内メールシステムの認証基盤は使用できないため，Firebase というサードパーティ製の認証基盤を使用し，鍵生成局の認証システムの実装を行った．また，拡張機能と鍵生成局で鍵をやり取りする際のデータフォーマットの決定や，鍵生成局側で鍵を管理するデータベースの設計構築，メール送信側の署名生成拡張機能の開発を行った．

（※文責: 菅文人）

3.2　酒井竜馬

前期

昨年度の卒業研究発表スライドの修正をメンバーと分担・協力しつつ行った．自分はＩＤベース暗号によって実現可能なことについてまとめた．修正前では順序があまりわかりやすいものではなかったので，内容をさらに細かくスライドで分割し，それについて簡潔にまとめることでより伝わりやすいものになるように工夫した．プロジェクトリーダとして積極的に議事を進め，全体での活動の方針をまとめ，具体的な開発環境や活動の方法を決定した．プロジェクトの開始と終了時に全体で集まる際には，今日の活動内容と到達目標，実際に活動しての進捗状況，次回までの課題や各提出物の期限の確認などを毎回細かく行なった．また中間発表に関わるポスターの作成を Canva というデザインサイトを用いて作成した．中間発表の評価では全体的に見づらいとのコメントがあったので，後期制作の際にはグラフや余白，読み手の視線の動きなどを意識してデザイン・制作を心がけたい．全体のスケジュールの計画を行なった．これは各グループリーダとも協力し合いながら，ある程度の余裕を持ったものにするようにした．最終的な成果物をここで決定してしまいそれに縛られることになると，柔軟な活動ができないと判断したため，途中での修正がなるべく行えるようにした．

後期

前期に引き続きリーダとして全体での司会・進行と各グループでの進捗，活動内容の確認を行なった．最終成果物である ID ベース暗号を用いた署名検証の主に署名の検証，暗号の復号についてのプログラム記述を行った．プログラムの記述については，個人での学習不足と技術不足により，メンバに助けられ，成果物にはあまり貢献することができなかった．また最終発表会でのメインポスターの制作を Adobe Illustrator を用いて行なった．中間発表時に作成したポスターと，その際の評価を踏まえ，細かい修正や調整が可能な Adobe Illustrator を採用した．今まで使用した経験がなかったため，ライセンスは個人で購入し，学習サイトや Web サイトを活用し技術の習得をしつつ制作に取り組んだ．また，前期での反省点を生かし，読み手の視線の流れを上から下，左から右というようになるように内容のまとまりを整理し，そのまとまりごとの間隔を工夫し，見やすいものになるようにした．

（※文責: 酒井竜馬）

3.3 佐藤隼斗

前期

グループリーダとして，制作物の提案やメンバーとの意見交換，スケジュール管理を積極的に行った．また，セキュリティの勉強の一環として行った卒研生の発表スライドの修正では，内容だけでなくデザインにも気を遣って修正した．この時作成したスライドは中間発表や成果発表の際に役立てることができた．前期後半及び夏季休暇中は，グループメンバーである吉田と共に，メール本文と添付ファイルの暗号化・復号プログラムを作成した．ペアとしては，サブプログラマとして主に細かい部分の修正や加筆を行った．この時作成したプログラムは後期の仕様変更の影響で直接使うことはできなかったが，JavaScript に書き直しを行い流用することで活用することができた．

後期

主に担当した部分は，スケジュール管理とプログラムの統合及び修正である．後期に入りメールクライアント開発で問題が発生したため，吉田と菅の主導でメールアドオン開発に仕様変更をした．再びスケジュールを見直し，進捗確認をしながら役割分担を行うことで柔軟に開発を進めることができた．プログラムで担当した部分はメールの暗号化・復号のベース作りとファイルの暗号化・復号アドオンへの ID ベース署名機能の実装などである．他にも，プログラム全体の統合やテストなども担当していた．成果発表会では，発表資料の作成を吉田と菅と共に行い，もう一方のグループと動画撮影を行った．

（※文責: 佐藤隼斗）

3.4 吉田琉夏

前期

昨年度の卒業研究発表スライドの修正をメンバーと分担・協力しつつ行った．自分は実験方法と結果についてまとめた．プログラム開発を行う以前の環境構築や実際のアプリケーションでの手順

等をメンバーに報告し，同一の環境下で開発を行えるようにした．また，ID ベースを用いたハイブリッド式ファイル暗号化復号のプログラムを記述した．

ID ベース暗号に関するスライドの修正を通して，ID ベース暗号を用いたシステムがどのようなメリットを持ち，開発を進める必要があるのか等を別のプロジェクトチームに発表するため，中間発表用の資料を作成するなど，後期からの活動に向けた説明を行った．

夏季休業からは mcl を用いた C 言語での ID ベース暗号を用いたファイルの暗号化と復号の機能をもつプログラムの開発を進めた．

後期

それぞれが作成した暗号化や署名の関数を nPOP に組み込もうとしたが，アーキテクチャが合わず，そのままでは非常に手間のかかる作業となることが判明した．そのため，後期の初めの週から代替案を模索し，Web メールに利用できるよう，ブラウザのアドオンとして開発する案をグループに提案し，採用された．

前期の開発で用いたライブラリである mcl の開発者は JavaScript で動作する mcl-wasm というライブラリを公開していたので，前期中に C 言語で開発した関数や流れを流用することができた．メッセージやファイルを暗号化したり復号する処理は容易にかけるのだが，実際にブラウザのアドオンとして実装すると動作しなかったり，細かなバグが生じるなどの動作が見られたため，10 月や 11 月ではそれらの対処を行った．自分は基本的には添付ファイルの暗号化と復号の処理を担当した．

発表用動画やスライドを作成するために，グループで開発したアドオンのスクリーンショットを記録したり，実際の操作方法について詳しく解説を行った．また，全体の流れを見て，まとめのスライドを作成した．

（※文責: 吉田琉夏）

第 4 章　結果

4.1　成果

前期の初めに行った ID ベース暗号に関する過去の卒業研究生の発表用スライドの修正を行うことによって，ID ベース暗号という方式の仕組みやメリットを理解することができ，実際に ID ベース暗号を用いた電子署名などのシステムを構築するための前提知識を得ることができた．

ID ベース暗号方式を用いた暗号化と署名検証でチームを分けることとし，それぞれのチームで関数の作成を行った．前期まででは両チームとも C 言語での暗号化や復号，電子署名の関数を作成することができた．

中間発表では自分たちのチームが作りたいシステムをほかのプロジェクト学習の班に紹介することによって，自分たちの目標や他の人からの質問を受け答えする中で，見つめなおすことができ，後期からのシステム開発の材料になったと考える．また，発表を行うにあたって，ID ベース暗号を知らない人にわかりやすく説明するための資料作りなどを行うことができた．

後期からは前期で作成した C 言語での関数を nPOP というオープンソースのメールクライアントソフトに組み込むことを想定して活動を始めたが，1 週目で mcl と nPOP の互換性が無く，修正に膨大な時間がかかると予測された．このことから代替案をメンバーで出し合い，Web メールに ID ベース暗号を用いるため，ブラウザのアドオンとして開発する案が採択された．このことから，大幅な仕様変更に対しても柔軟な発想を行い，対処できる力が身についたと考える．

javascript で動作する mcl-wasm というライブラリが開発者がオープンソースで提供されていたため，基本的な流れや関数名は前期で開発した関数をそのまま流用することが可能であった．

ブラウザアドオン開発でも暗号化と電子署名のチーム分けを行い，それぞれの担当した機能を実装する形とし，最終的にすべてのアドオンをブラウザにインポートすることによって，ID ベース暗号を用いた署名検証や暗号化を施すことができるようになった．

ファイルの暗号化と復号に関する処理ではすべてに ID ベース暗号を用いると，CPU の使用率が高くなり，動作が重たくなるので実際のファイルの暗号化には”crypto-js”というオープンソースの暗号ライブラリを用いて，共通鍵暗号方式で暗号化を行った．共通鍵となる情報を ID ベース暗号に用いた mcl で暗号化することによって，実質的にハイブリッド暗号方式を実装した．

ファイルの暗号化・復号機能にもファイル送信者の正当性を検証するべく，電子署名の検証機能を実装した．メールの署名検証機能では，大学の Web メールを用いて電子署名の機能を実装する仕様として開発を行った．

メール本文を別のプログラムのエディタで書いて署名を生成するソフトウェアが多く存在するが，今回のプロジェクトでは「標的型攻撃」に対抗するシステムの開発であるため，暗号に詳しくない人でも簡単に，気軽に利用できるようにするべく，いつも利用するメール作成画面から「ID 署名付きで送信」を押すだけで電子署名を添付したメールを送信できるようにした．

また，署名付きのメールを受け取った際にも，メールの本文を別のウィンドウにコピー＆ペーストすることなく，受信メッセージ上部に設置された「ID ベース署名検証」というボタンをクリックするだけで有効な署名かどうかを検証できる，ユーザーフレンドリーなシステムの構築を行った．メール本文フィールドを自動的に検出して処理するプログラムは javascript では容易に実装す

ることができた.

ID ベース暗号では利用者からみると，名前やメールアドレス自体が公開鍵となるため，鍵の存在を意識せずにセキュリティの向上を図ることができるが，受信者は秘密鍵を管理しなければならない．これではユーザーフレンドリーとは言えず，ユーザーそれぞれがカギの管理をしなければならないため，鍵生成サーバーと同時に鍵管理サーバーの構築を行った． 鍵管理サーバーを用いると，利用者は自分の ID となる情報とパスワードを記憶することによって，手軽に ID ベース暗号を用いた暗号化や署名検証を行うことができる．サーバーには Firebase を用いることによって，本格的な認証を行えるようになった.

ブラウザのアドオンとサーバーで通信させるために javascript の非同期処理などを理解し，実装する必要があったが，電子メールの署名検証はもちろん，ファイルの暗号化・復号のプログラムにも組み込むことができた.

（※文責: 吉田琉夏）

4.2 解決手順と評価

ID ベース暗号

ID ベース暗号を用いた電子署名 (ID ベース署名) を用いることで，低コストな電子署名をメールシステムで実現することができた．私たちが作ったアドオンはメール送信用・メール受信用・ファイル暗号化及び復号用の 3 つである．全てのアドオンに対して ID ベース署名を実装することができたため，要件定義である低コストな電子署名の実現は達成できた．しかし，メール送信用・受信用に関しては，本文の暗号化を行っていないため機密性が低い．これは，暗号化を実装した際に送信済みメールの復号が必要であったり，返信する際に暗号化されたメールが引用されてしまうなどの拡張機能で実装したことによる弊害が発生したためである．しかしながら，通信中の盗聴については TLS 通信の使用が対策となるため，使用する上での問題はない．仮に拡張機能による弊害を避けるとすると，予めメールシステムに組み込むか専用のメールクライアントを作るなどの対処が必要であると思われる.

（※文責: 佐藤隼斗）

ブラウザ拡張機能としての実装

前期活動では ID ベース署名機能を搭載したメールクライアントの作成を目指していたが，ペアリングライブラリである mcl とベースとして利用しようとしていた nPOP の対応ビットが異なり，ビルドすることができなかった．そのため，メールクライアントの作成からブラウザ拡張機能 (アドオン) へと仕様変更を行うことにした．これにより，対応ビットの解決だけでなく，当初予定していなかった mac や linux への対応も行うことができた．しかし，上記の通りブラウザ拡張機能で実装したことで問題が発生してしまったため，より現実的なシステムを作る際にはメールシステムに組み込んだり，対応のメールクライアントを作成したりなど方法を変更する必要がある.

（※文責: 佐藤隼斗）

鍵処理と鍵の更新処理

後期活動では，鍵処理と鍵の更新処理まで実装することができた．前期の予定では，秘密鍵は事前に持っていることが前提となっており，ID ベース暗号機能を搭載することだけを考えていた．後期の活動では，仕様変更後の開発が順調に進んだため，秘密鍵と公開鍵の受け渡しをするサーバまで考えることができた．また，サーバ内では秘密鍵の更新機能も実装した．鍵の安全な受け渡しは難しく，よく議論される内容であるため，当初の予定よりも一歩進んだ開発ができたといえる．

（※文責: 佐藤隼斗）

既存の電子署名との比較

今回実装した ID ベース署名と既存の電子署名である S/MIME 及び PGP 署名との違いを記載する．S/MIME との違いは公開鍵証明書の有無である．ID ベース署名では，メールアドレスなどの ID そのものを公開鍵とするため，公開鍵の持ち主が本人に限定され，公開鍵証明書が必要ない．従って，認証局が必要ないため，コストを安く抑えることができる．また，同じく認証局を必要としない電子署名として PGP 署名が存在する．しかし，PGP 署名では，本来認証局が署名を行う証明書に，誰でも署名をすることができるため，安全性が低くなってしまう．以上のことから，既存の電子署名と比較すると，ID ベース署名は安全性を保ちながらコストを安く抑えることができる電子署名であるといえる．

（※文責: 佐藤隼斗）

4.3　中間発表会での評価回収フォームのデータ

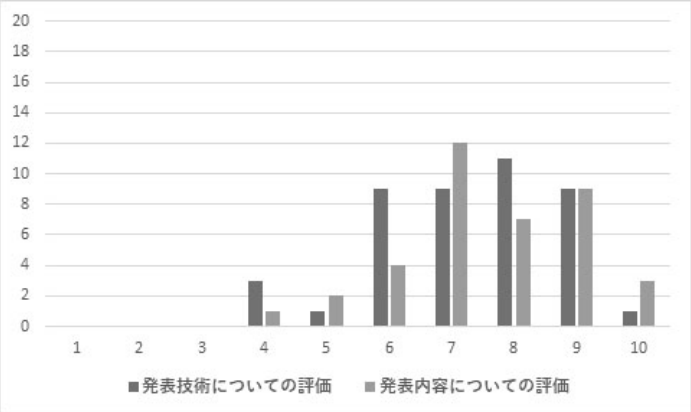

図 4.1　中間発表会アンケート調査結果

中間発表の際に実施した発表評価の集計には，Google Foams を使用し 38 件の評価をいただいた．発表技術の評価では，平均で 7.05 であった．発表技術についてのコメントでは，「ポスター，サイトがほぼ文字ばかりで少しわかりにくいと感じました．できるようであればうまく図解して説明できたら良いと思います.」「サイトを作成したのは良いと思いました．全体ポスターで前期成果をもっとアピールできると良いですね.」など作成物に関してのコメントが多く寄せられた．実際に，文字による表現が多くなってしまい，読者としては非常に見づらいものになってしまってよう

に感じた．最終発表では，グラフやレイアウトをもう少し意識し，多くの人が見やすいような工夫が必要になる．発表内容については，7.60 と発表技術よりはやや高い評価を頂けた．コメントとしては「成果物の内容はわかるがどういった形式のものができるのかよくわからなかった.」「なぜ ID ベース署名を使うのか，なぜメールなのか，もう少し踏み込んだ説明があると良かったでしょう.」など，内容はしっかり伝わっていたが，理由づけやその経緯が少し不足している印象を受けた．中間発表時点ではまだ完成形を具体的に想定できていなかったということもあるが，その点についても発表の際にもう少し込み入った説明を加えるとなおよかったと感じた．スライド修正に関しては，評価回収フォームに独自の質問項目をもうけ，修正前と修正後での見やすさ，理解のしやすさを発表技術や発表内容と同様に 10 段階評価で評価してもらった．結果としては，7.15 と，悪くはない評価だった．具体的にどの点がわかりやすい，わかり辛いなどのコメントによる項目を設けていなかったため，具体的な修正を行うことはできなかったが，少しの内容の修正とレイアウトの統一を図る程度で十分だと判断した.

（※文責: 酒井竜馬）

4.4　最終成果発表会での評価回収フォームのデータ

4.4.1　回収した評価の件数と平均点

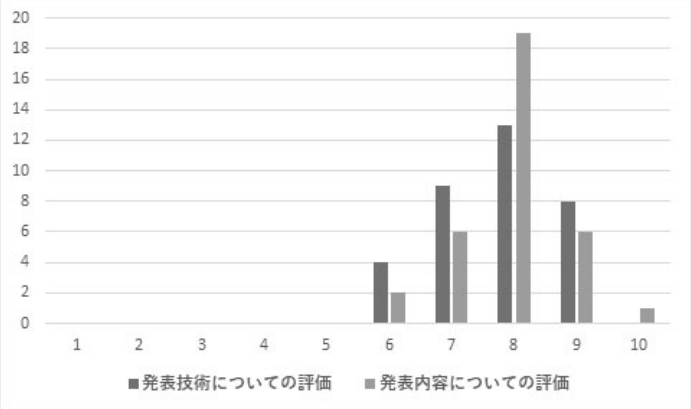

図 4.2　最終成果発表会アンケート調査結果

発表評価の集計には Google Foams を使用し 34 件の評価を頂いた．発表技術についての評価では平均 7．69 の評価を得ることができた．また，発表内容についての評価は 7．94 であった．発表技術についてのコメントでは，動画に関する意見としてノイズや発言途中の噛みが気になったとの感想があった．また，発表スライドの文字が多い，アンケートの円グラフが見にくいかったというコメントも頂いた．暗号とセキュリティというプロジェクト上，内容が難しくなってしまうので文字数が多くなってしまうのは仕方がないが，他の部分については直すことができるのでプロジェクト終了までに修正していきたいと思う．他に，デモを画像ではなく動画でしてほしかったという要望があった．実は，私たちも最初は動画を撮影しようとしていたが，問題が発生したため画像で代替えをしたという経緯がある．動画の方がイメージが伝わりやすいため，可能であれば動画に変更したいと思う．発表内容に関するコメントでは，「プロジェクトの経緯に納得できた」「事前動画と実際の発表で一貫性があり理解しやすかった」などの感想を頂いた．発表に関して重視していた部分だったので，伝えることができて良かったと思う．また，12 月以降のスケジュールがないの

が気になったという意見があった．12 月以降はプロジェクト報告書の執筆を主に行い，終わり次第コメントをもとにした改善やプログラムのリファクタリングを行う予定である．プロジェクト全体の意見として，「両グループの取り組みを別々のものとして扱うのではなく，統合して何が言えるのかをまとめてもらえればなおよかった」というコメントを頂いた．納得のできる内容だったため，他グループも含めて検討していきたい．

（※文責: 佐藤隼斗）

4.5　自分のグループの評価

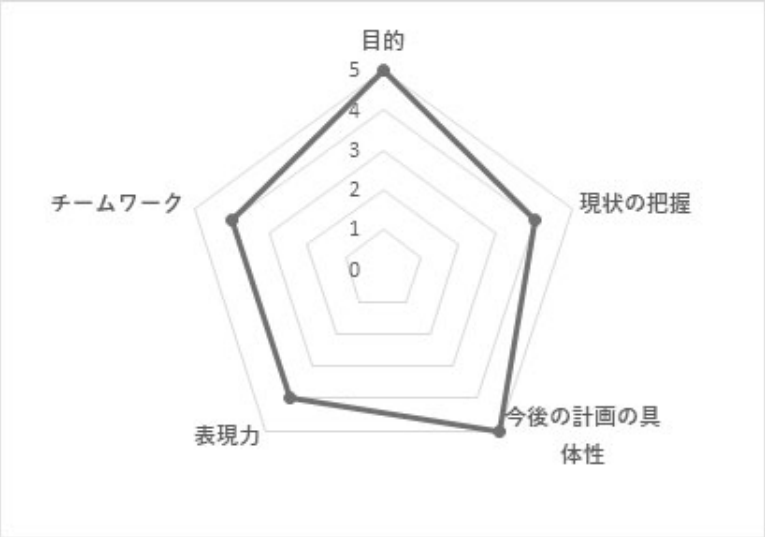

図 4.3　グループの評価

目的に関する項目は 5 点である．私たちは電子署名の普及を目指して，安全でコストの低い電子署名の実用化を目標として活動してきた．ID ベース署名機能を搭載したメールアドオンを開発したことで，目標は達成できたと考えることができる．現状の把握は 4 点である．機能分担して開発を行ったため，全体像を把握しているメンバーと概要しかわからないメンバーがいると感じる．メンバー間での情報の共有を行いたい．今後の計画の具体性は 5 点である．当初の予定であるメールクライアントの開発や今回作成したアドオンの firefox 対応などを考えている．また，学生証へ秘密鍵を内蔵して，暗号化・復号を行うなどの今後の展望も考えている．表現力は 3 点である．発表する内容は良かったが，発表技術で足りない点があったと思う．具体的な改善は上記の 4．3．2 節を読んでもらいたい．チームワークの評価は 4 点である．メンバーの状況を見ながら担当分けし，忙しいときは互いを助け合いながら進めてくることができたと思う．

（※文責: 佐藤隼斗）

第 5 章　まとめ

5.1　プロジェクトの成果

チームで一つのシステムを開発する作法を実際に体験することによって，作業の割り当てやスケジュールの管理などを行い，成果発表会というマイルストーンに向けて目標のシステムをを構築し，発表することができた．

また，最近は Web アプリケーションが増え，JavaScript などを用いることが社会に出てからあるかと思う．大学では基本的に C 言語を用いることが一般的であり，テキストベースなプログラムを作成することが多い．今回のプロジェクト学習を通して，Web アプリケーションの設計や JavaScript を用いたプログラミングなどを実際に体験して，アプリケーションの開発について身に着けることができた．

また，ID ベース暗号方式は公開鍵暗号方式の応用的な手法であるため，基礎となる暗号技術についての知識を身につけなければ開発を進めることができないと考えられる．このことから，セキュリティや暗号に関する基本的な知識はメンバー全員が身に着けることができており，開発を進めることができたと考える．

ID ベース暗号を用いたシステムでは，ユーザは相手の ID を知ることができれば暗号化や署名検証を行うことができる．S/MIME はコストが高く，OpenPGP ではユーザが鍵の管理を行うなど，セキュリティや暗号に詳しい人でなければ避けられてしまうことが多い．

暗号の応用に当たる技術は多く発案されているが，実際のサービスに利用されることは多くない．今回のプロジェクト学習を通して，ID ベース暗号という応用暗号技術を用いたメールの検証や添付ファイルの暗号化，署名検証を行うシステムの構築から，ユーザは便利に，また強固なセキュリティを利用することができるようになる．

（※文責: 吉田琉夏）

5.2　プロジェクト内の自分の役割

5.2.1　菅文人

前期

電子署名技術に関する情報の収集を担当した．また，本プロジェクトではじめに行った，昨年度の卒業研究の発表資料修正において，スライド中の公開鍵暗号方式の項目の修正を担当した．また，中間発表では，発表用 Web サイトの制作を担当しており，本テーマおよび発表スライドの概要を説明するための文章の制作等を行った．

後期

本グループでは，電子署名の機能を有したブラウザ拡張機能開発行うため，そのための開発方法の調査や，開発の指針の策定を行った．メールシステムの実現において，鍵生成局の構築が必要になったため，鍵生成局の設計構築および，秘密鍵と公開鍵の取得 API の設計と実装を担当した．

そのため，鍵生成局の管理や全体のデバッグ等を担当した．また，メール送信時の署名生成拡張機能の実装を担当した．

（※文責: 菅文人）

5.2.2 酒井竜馬

前期

プロジェクトリーダとして，各グループでの進捗を管理したり，具体的な活動方針やプロジェクト全体での意思決定をする際での進行役を担った．オンラインでの活動のため自分では些か力不足と感じる場面が多くあったが，後期は活動が本格化するので，より一層の努力が必要であるとの認識を強めた．後期を通して振り返ると，もう少し早めからアジャイル開発の手法など，具体的な手法を取り入れると，より効果的で有意義な活動が行えたのではないかと思う．活動に対する取り組みとしては，全員が顔を合わせることなくスタートし，意見などの発言も含め会話が全体的に少なかったため，自分が率先して話題を振ったり，一人に対して意見を求める行動を全員に行うようにして，全体での意見・発言がしやすい環境づくりを整えることに尽力した．結果として，全体での活動ではあまり成果は見られなかったが，グループ内の活動では，徐々にメンバでの話し合いが自然に行えるようになっていったと感じている．

後期

前期に引き続き，各グループの進捗の管理，最終発表に関わる提出物等の役割分担と期日の調整などを行った．後期に入り活動が本格化したことにより，前期よりも柔軟な対応を心がけ，なるべく全体でスムーズな活動が行えるようにした．具体的には，全体での各グループ，個人での活動の報告の際に自分で気になったことの詳細なヒアリング，成果物での進捗による提出物への参加の調整や，グループ間での成果の発表を行い各グループ間での活動内容の相互理解を深め，お互いに疑問点をフィードバックとして質問し合うことで発表技術，内容の向上を図った．グループ内のメンバとしての活動としては，プログラム等の記述においてあまり成果を出すことができなかった．これについては自分の技術不足，勉強不足が顕著になった部分であるため，今後の活動では反省点として生かしたいと思う．

（※文責: 酒井竜馬）

5.2.3 佐藤隼斗

前期

グループリーダとしての役割とプログラマとしての役割を兼任していた．リーダとしての役割では，積極的に意見を出し，話しやすい雰囲気を作ることで議論を円滑にすすめるサーバントリーダシップの考えで行動した．今年のプロジェクト学習はほとんどがオンラインで行われるため，対面で行われる場合と比べて意見を出しにくい雰囲気があった．質問を投げかけることで意見を引き出し，まとめることで議論を進めてきた．プログラマとしての役割では，吉田とともに ID ベース暗号を用いたメールとファイルの暗号化・復号のプログラム作成を行った．メインとしては吉田が活躍していたため，サブプログラマとしての修正や加筆を主に行っていた．

後期

前期と同じく，グループリーダとしての役割とプログラマとしての役割を兼任していた．前期に比べるとメンバーからの意見が多くなっており，意識しなくても議論が進むようになっていた．開発が始まっていたため，グループリーダとしては各個人の進捗状況の確認や全体のスケジュール調整を行っていた．また，スケジュールに余裕が出てきた際には追加で実装するシステムについての議論を行ったりした．プログラマとしては，メンバーが作成したプログラムの統合とテスト，テストした際に発生したバグの修正を主に行っていた．この際，自分が違うプログラムを担当していた際は，元の担当者に修正を依頼していた．成果発表会の準備では，菅・吉田と共に発表資料の作成を行った．また，他のグループのメンバーと共に事前作成動画の撮影も行った．

（※文責: 佐藤隼斗）

5.2.4 吉田琉夏

前期

プロジェクトリーダーやグループリーダーではなかったが，よりよいシステムにするために意見を出したり，担当となった機能のプログラミングなどに取り組んだ．

前期では ID ベース暗号についての過去の発表スライドを修正する作業から始まった．これを通して ID ベース暗号に関する基礎的な知識を身に着けることができたと考える．

次に C 言語での ID ベース暗号を用いたメールクライアントの機能を実装することを目標に，関数の作成を行った．自分は暗号化に関する処理を担当し，本文と添付ファイルの暗号化を行う処理を記述した．前期ではオンライン授業どころか，オンラインで見ず知らずの人と会話することに抵抗を持ち，なかなか自ら進んで発言することが難しかったが，できるだけ自分の意見を発表するために，Slack などから連絡をするように心がけた．

後期

前期や夏季休業中に作成した ID ベース暗号に関する関数を実際にメールクライアントソフトに組み込み，サービスを実現させようとしたが，ID ベース暗号に用いたライブラリが 64bit 版にしか対応していなく，メールクライアントソフトは 32bit 版だけであったので，整合性が取れず，修正に膨大な時間がかかると予測されたため，代替案を考えた．

私は以前からプライバシーに関して独自に調査を行ったことがあり，Web メールで OpenPGP を用いた暗号化や署名を行うことが可能である”mailvelope”というブラウザアドオンを利用していた．

ここから，ID ベース暗号を実現する方法として，ブラウザアドオンとして実装するという案を提案し，採択された．

Web メールを ID ベース暗号を用いて処理することによって，未来大生が皆保有しているメールアドレスを利用することが可能であり，ブラウザのアドオンを開発することによって，動作環境の依存が少なくなり，多くの端末や OS で動作させることができる．中間発表で質問に上がった，互換性に関する問題点を解決することができる．　ブラウザアドオンを開発することが決定し，JavaScript でのアドオン開発が始まったが，ID ベース暗号に用いた mcl というライブラリには C 言語以外にも JavaScript 版がオープンソースで公開されていたため，基本的な処理や順序は C 言

語で開発した関数を移植することができた.

私は前期と同じく暗号化，復号に関する処理のプログラムを担当した．また，ファイル暗号化に関する処理のプログラムを重点的に開発を行った.

ファイルの暗号化において，前期中に C 言語で実装したものではライブラリに OpenSSL を用いて AES 暗号を利用したが，JavaScript では OpenSSL が利用できない．そこで，Crypto-js という JavaScript で動作する OpenSSL 互換の暗号ライブラリを用いることにした．JavaScript での暗号ライブラリの中では比較的活動が活発であるという理由から選択した.

また，発表用に利用した実際のブラウザアドオンの実演方法を紹介するために資料に利用する画像などをキャプチャし，資料の作成を行った．発表後アンケートでは「動画のほうがわかりやすいと思う」という意見が多く，次回以降の発表を行う際の資料作りに生かしたい.

（※文責: 吉田琉夏）

5.3 今後の課題

- 現状では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を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.
- アドオンを開発する際のデザインは Web サイトと同じく HTML や CSS で UI を設計することができるが，ID ベース暗号の処理の記述に力を入れたことと，Web デザインの設計などに詳しい人がプロジェクトに居なかったため，簡易的なものになってしまった．利便性を高めるために，デザインを統一して見栄えを良くしたいと考えている.
- 今回は Chrome 系ブラウザのアドオンの開発を行ったが，Firefox 版のブラウザアドオンも開発したいと考えている.
- 開発段階にて，認証サーバがダウンすることが多くあったが，原因を突き止めて安定してサービスを提供するようにしたい.
- 今回はブラウザのアドオンとして開発を行ったが，本来目指していた 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機能の実装を行いたい．これに関する解決策としては，メールクライアントソフトが 64bit に対応しているものを探す必要がある.

  nPOP やほかの 32bit のメールクライアントソフトを利用したいという場合は，mcl の開発者と連絡を取り，32bit 版をリリースしてもらう，または他のペアリングライブラリを用いることも可能である.

  これらの方法が難しいようであるならば，開発にかかる時間は大幅に増すが，OpenSSL などの既存の暗号ライブラリを用いて自らペアリングライブラリを開発するという方法も考えられる.

（※文責: 吉田琉夏）

付録 A　新規習得技術

- Firebase
- ID ベース暗号

付録 B　活用した講義

- 講義名　アルゴリズムとデータ構造
  内容　c 言語や JavaScript でプログラミングをする際に考え方が役立った
- 講義名　ネットワークセキュリティ
  内容　共通鍵暗号や公開鍵暗号の知識を用いた

参考文献

[1] 土屋 正， 辻宏 郷， 黒谷 欣史， 亀山 友彦， 渡邉 祥樹， 大友 更紗， 吉本 賢樹， 宇梶 宏美， 田村 智和， 熊谷 悠平， 佐々木 敬幸， 佐藤 輝夫， 阿部 未歩， 情報セキュリティ 10 大脅威 2020， 局面ごとにセキュリティ対策の最善手を， IPA， 2020.

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

[3] S/MIME 用証明書 GMO グローバルサイン【公式】https://jp. globalsign. com/service/clientcert/smime. html

[4] A. Shamir, Identity-based cryptosystems and signature schemes. In: Workshop on the theory and application of cryptographic techniques. Springer, Berlin, Heidelberg, pp. 47-53, 1984.

[5] 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.

[6] CRYPTREC ID ベース暗号調査 WG， ID ベース暗号に関する調査報告書， 2008.

[7] R. A. Sahu and S. Padhye, ID-based signature schemes from bilinear pairing: A survey. Frontiers of Electrical and Electronic Engineering in China, pp. 487-500, 2011.