卒業論文　　2010年度（平成22年度）

電子メールヘッダの特徴情報を用いた標的型攻撃の検知

慶應義塾大学 環境情報学部

氏名：梅田 昂翔

担当教員

慶應義塾大学 環境情報学部

村井 純

徳田 英幸

楠本 博之

中村 修

高汐 一紀

重近 範行

Rodney D. Van Meter III

植原 啓介

三次 仁

中澤 仁

武田 圭史

平成23年2月14日

卒業論文要旨 - 2010 年度 (平成 22 年度)

電子メールヘッダの特徴情報を用いた標的型攻撃の検知

近年，電子メールを用いた攻撃が増加している．それにより様々な被害が発生しており，被害は個人だけでなく，企業や官庁にまで広がっている．電子メールを利用した攻撃の中でも，標的型攻撃は対策が困難である．標的型攻撃は電子メールを用いて特定の組織やグループを標的に悪意あるプログラムや URL を送信する攻撃である．電子メール本文などに攻撃対象が普段から利用しているようなメッセージを含むため，受信者が不正なメールと判断することが難しい．また，標的に合わせて攻撃手法が変化するため，一般的なセキュリティ対策ソフトウェアなどによる対策が困難である．そこで，本研究では標的型攻撃を判別する手法を確立し，実装する．本研究では標的型攻撃の中でも電子メールを利用し，標的の関係者になりすました攻撃を対象とする．

本研究では標的型攻撃の対策として，Mozilla Thunderbird のプラグインを用いて電子メールのヘッダ情報を取得，蓄積，表示する手法を提案する．まず，個々の電子メールのヘッダ情報の特徴を分析し，外部ファイルに保存する．同時に，過去に蓄積したヘッダ情報と，受信した電子メールのヘッダ情報を比較することで，標的型攻撃である可能性を評価する．そして，受信した電子メールが標的型攻撃であると判定した際に，ユーザに対して最終的な判断を促すための情報を提供する．これにより，標的の関係者になりすました攻撃を判別することができ，情報漏えいなどのリスクを軽減させることが期待できる．

キーワード:
1．電子メール, 2. Mozilla Thunderbird, 3. セキュリティ, 4．アドオン

慶應義塾大学 環境情報学部

梅田 昂翔

Abstract of Bachelor's Thesis - Academic Year 2010

Targeted Attack Detection by Analyzing Characteristics of Electric Mail Header.

Recently, the number of attacks using E-mail increased. Various types of damages occur and the damages extends not only to the individuals, but the enterprises and the government offices. Among the attacks using E-mail, it is especially difficult for us to take measures against Targeted Attack.

Targeted Attack is an attack that transfers a malware or URL using E-mail, to a target, which is often a certain organization or a group. It is difficult for the recipient to judge that the mail is illegal, begause the E-mail contains a sort of message that the recipient is familiar with. Moreover, because attack techniques differ with the targets, taking measures with a general security software is difficult. Therefore, a technique for distinguishing Targeted Attack is established in the following research and implementation. The research aims to distinguish attacks, impersonating acquaintance of the target and uses E-mail.

The research proposes a technique for acquisition of header information on E-mail, accumulation, and Displaying it by using a plug-in of Mozilla Thunderbird as measures against Targeted Attack in the research. First of all, the characteristics of header information on individual E-mail is analyzed by the plug-in of Mozilla Thunderbird. and it preserves the header information in a file. At the same time, possibility of Targeted Attack is estimated by comparing E-mail header information accumulated in the past against header information on the received E-mail. And, when it is judged ,that the received E-mail is likely to be a Targeted Attack, information tofor making final judgement is furnished to the user.

As a result, the risk of the intelligence leak can be expected to be reduced by distinguishing the attacks, impersonating the acqaintance of the target.

Keywords :
1. Electronic mail, 2. Mozilla Thunderbird, 3.Internet Security, 4. add-ons

Keio University, Faculty of Environment and Information Studies

Takato Umeda

目 次

第 1 章　序論 **1**
1.1　背景 1
1.2　本研究の目的 1
1.3　本論文の構成 2

第 2 章　標的型攻撃 **3**
2.1　標的型攻撃の概要 3
2.2　標的型攻撃の実例 4
2.3　電子メールを利用した攻撃の分類 4
2.4　本論文において対象とする攻撃 6

第 3 章　標的型攻撃への対策と課題 **7**
3.1　標的型攻撃への対策 7
3.1.1　サーバでの実装 7
3.1.2　クライアントでの実装 9
3.2　まとめ 10

第 4 章　関連研究 **11**
4.1　標的型攻撃の分析 11
4.2　予防接種による対策 11
4.3　送信ドメイン認証による対策 12
4.3.1　送信ドメイン認証とフィッシングメール防御 12
4.3.2　送信ドメイン認証と暗号化した電子メール 12
4.3.3　送信ドメイン認証とヘッダ情報を利用した対策 12
4.3.4　携帯電話での対策 13
4.4　まとめ 13

第 5 章　電子メールヘッダ情報の取得と蓄積による対策 **14**
5.1　対策の概要 14
5.2　前提 14
5.3　事前調査 15
5.4　提案手法 17
5.4.1　情報の収集 17
5.4.2　情報の蓄積 18

5.4.3 結果の表示 19

第 6 章 実装 **20**
6.1 収集 20
6.2 蓄積 22
6.3 表示 22

第 7 章 評価 **25**
7.1 評価項目と期間 25
7.2 評価の結果 25
7.2.1 IP アドレス 25
7.2.2 ドメイン 26
7.2.3 電子メールクライアント 28
7.2.4 タイムゾーン 29
7.3 考察 29

第 8 章 結論 **31**
8.1 まとめ 31
8.2 今後の展望 32

謝辞 **33**

図 目 次

2.1 標的型攻撃の概要 4
2.2 JPCERT/CC「標的型攻撃について」より 5
2.3 標的型攻撃の実例 5

3.1 IP アドレスによる認証 8
3.2 電子署名による認証 9

5.1 電子メールヘッダの例 18

6.1 実装したプログラムの動作概要 21
6.2 蓄積しているファイル 23
6.3 結果の表示 23

7.1 IP アドレスの調査結果 27
7.2 ドメインの調査結果 28

表 目 次

2.1 電子メールを用いた攻撃の分類 6

5.1 IP アドレスの調査結果 16
5.2 電子メールクライアントの調査結果 16

7.1 標的型攻撃への対応評価 30

第1章　序論

本章では，現在社会で起こっている電子メールによる脅威について簡単に説明した上で本論文の目的と構成について述べる．

1.1　背景

近年，企業や官庁，大学などにおいてコンピュータから情報が流出する情報セキュリティに関する問題が発生しており，多くの対策がなされている．攻撃の手法には，攻撃者がターゲットユーザにブラウザを用いて特定の場所から悪意のあるプログラムをダウンロードさせるものや，サーバやクライアントに直接アクセスして攻撃するもの，メールによって不正なプログラムを送るものや，URL によって特定のサイトにアクセスさせるものなど，非常に多くの種類がある．

本論文ではその中でも電子メールによる攻撃を対象とした．電子メールは利便性に優れているため，利用者が多く存在する．そのため，電子メールによる攻撃は上記に挙げたもの以外にも様々な種類がある．一般的に，電子メールによるセキュリティ上の脅威としてあげられるのは，SPAM メールである．SPAM メールは不要なインターネット広告を含んだ電子メール等の受信者が望んでいない電子メールのことである． 現在では SPAM メールの対策が進んだが，ほとんどが未だになくなってはいない．SPAM メールの特徴は件名の時点で，それが SPAM メールであることは容易に判断できる．また，アドレスや本文によってそれが広告や攻撃を目的としたものであると判断できる．しかし，同じ攻撃でも件名や本文，アドレスなどの情報だけでは判断できない攻撃が，標的型攻撃である．

標的型攻撃は，一律の攻撃コードが用いられず，攻撃対象のユーザに合わせて本文や件名，アドレスなどのヘッダ情報を変えている．そのため，アンチウィルスソフトやパーソナルファイアウォールを含む総合セキュリティソフトによる対策や，SPAM メールフィルターなどの対策では対応することが難しい．

1.2　本研究の目的

本研究の目的は，標的型攻撃への対策を提案し．実装することにより，標的型攻撃による被害を防ぐことである．

標的型攻撃はその特性からそのメールが攻撃であると判断することは難しい．電子メールヘッダを読むことで判断を行うことができるが，電子メールヘッダは文字情報のみで構成されるため，一般的に読みやすいとは言えない．そこで，本論文においてはその電子

メールヘッダ情報より特徴情報の抽出・分析を行ない，標的型攻撃であるか否かの判定を行う手法を提案する．同時に，一般に広く利用できるように，Mozilla Thunderbird[1] のアドオンとして実装した．ユーザは電子メールに記載された URL や添付ファイルを開く前に，その電子メールが標的型攻撃か否かをアドオンから得られる情報によって判断し，標的型攻撃を防ぐことが可能となる．

1.3 本論文の構成

本論文は全 8 章で構成される．まず，第 2 章において標的型攻撃について触れた上で，本論文で対象とした攻撃について述べる．次の第 3 章では標的型攻撃への対策の課題として，既存のセキュリティツールによる，メールを利用した攻撃への対策の実例について述べる．第 4 章では関連研究として，標的型攻撃への対策に利用できる既存研究について述べる．第 5 章では標的型攻撃の判定手法として，本研究で利用した標的型攻撃の判定手法について述べ，第 6 章でその実装方法，第 7 章において評価と考察について述べる．第 8 章では結論として，本論文のまとめと今後の展望について述べる．

第2章　標的型攻撃

標的型攻撃の概要について，実際の標的型攻撃の実例を引用しながら説明を行う．また，攻撃を目的としたメールの分類を行った上で，本論文において対象とした攻撃について述べる．

2.1　標的型攻撃の概要

標的型攻撃は，対象を限定して行う攻撃である．JPCERT/CC が 2007 年に発表した「標的型攻撃について」[2] にある定義によると「情報セキュリティ上の攻撃で，無差別に攻撃が行われるものでなく，特定の組織あるいはグループを標的としたもの．攻撃対象となる組織あるいはグループに特化した工夫が行われることもある.」とある．主に電子メールを利用して攻撃を行い，悪意のあるコードを含む Microsoft Office[3] のファイル．PDF[4] ファイルといった文書ファイルに偽装したマルウェアを添付したメールや，マルウェアなどが設置してあり，それをダウンロードさせることを目的とした URL が記載されたメールを，対象とする企業や個人に送信する．直接，プログラムが送られていない場合は，受信した企業や個人が電子メールの添付ファイルや URL を開くことによって，ブラウザによって攻撃者の意図したサーバにアクセスする．その結果，キーロガーやバックドアがダウンロードされてしまう．それらのプログラムは攻撃者の意図した情報であるパスワードなどの個人情報が盗まれるなどの被害が発生している攻撃である．

攻撃の際には，特定の企業や組織に向けてそれらに特化した文面や件名にしたり，受信者が信用する送信元アドレスに偽装するなどの手法が用いられている．そのため，一般的なセキュリティ対策では限界があり，攻撃に対応しきれない組織が多い．また，本文なども攻撃対象に合わせて送信するため，一見しただけではそれが攻撃目的の電子メールと判断することができない．

攻撃の概要について図 2.1 に示す．まず，攻撃者が特定の組織やグループのユーザに URL を含むか，添付ファイルのある電子メールを送信する．ユーザがそれを攻撃と気がつけずに，その URL や添付ファイルを開くと特定の場所から悪意のあるプログラムがダウンロードされる．そのプログラムが働くことでユーザの ID やパスワードが盗まれるという流れである．

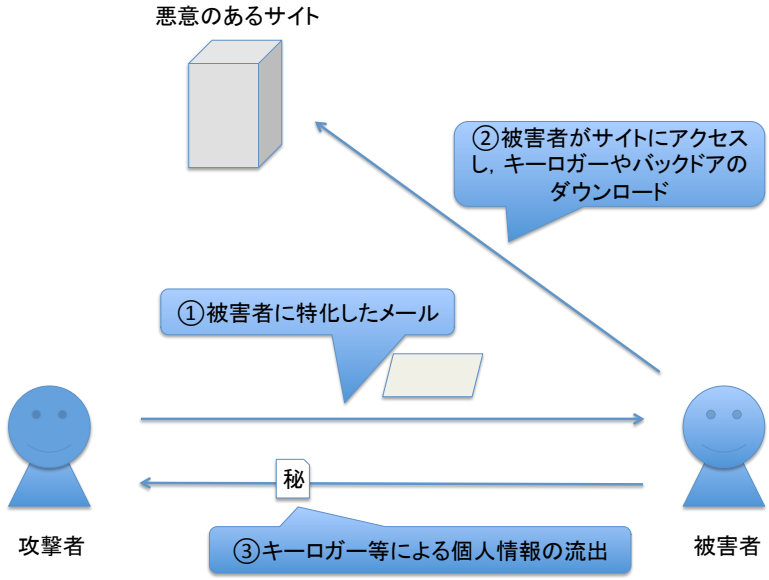

図 2.1: 標的型攻撃の概要

2.2 標的型攻撃の実例

電子メールを利用した標的型攻撃は Google[5] の他，アメリカ軍関連企業 [6] や IT 企業 [7][8] など様々な機関を対象に実際に攻撃が行われている．本説では，JPCERT/CC が 2007 年に発表した「標的型攻撃について」[2] より，実際の攻撃事例を図 2.2 に示す．

図 2.2 のように，標的型攻撃には様々な種類がある．その中の一つで，本論文で対象とした電子メールを利用した標的型攻撃の例を図 2.3 示す．図 2.3 の例では，SPAM メールと違い，件名，本文の内容が一般的な電子メールと見分けがつかない．また，添付されているファイルも本文に対応したファイル名になっている．このことから，本文の内容に関係のあるユーザが受信した場合，それを攻撃と判断することは非常に難しいと言える．

2.3 電子メールを利用した攻撃の分類

電子メールを用いた攻撃について，その形態と受信者への特化の度合いに応じた分類を表 2.1 に記す．レベル 1 はアドレス，本文ともに標的への特化を行わない攻撃でいわゆる SPAM メールがレベル 1 に分類される．内容も受信者とは関わりがなく，受信者は攻撃目的での電子メールであるとの判別は容易である．次のレベル 2 は，内容が時事的なものとなる．政治の問題，事件などをテーマとするなど，受信者が比較的興味を持ちやすいものを利用する．レベル 3 では，本文はレベル 2 と同じであるが，アドレスを実在する企業や団体，個人などのものとしている．以下，レベル 5 までいずれも同じくアドレスの偽装を行っているものと定義する．なお，本文では，レベル 4 が企業サイトなどの公開情報を利

- オフィスアプリケーションの脆弱性を狙う攻撃 Microsoft Office やジャストシステムの一太郎など

- 主に特定地域で使用されているアプリケーションの脆弱性 (もしくはユーザ) を狙う攻撃
  QQ(インスタントメッセンジャー，中国)，zeroboard(掲示板ソフト，韓国)，一太郎 (ワードプロセッサ，日本)，Winny(ファイル共有ソフト，日本)

- 特定銀行の利用者に限定して，フィッシングサイトへと誘導する CD-ROM を送付

- 「金銭を払わなければ，Web サイトに DDoS 攻撃を行う」という恐喝

- ソーシャルエンジニアリングの手法を組み合わせる
  新聞社を騙る，顧客を装う，企業/組織の役員の名前を騙る 件名・本文に大きな時事問題に便乗した内容を含める

図 2.2: JPCERT/CC「標的型攻撃について」より

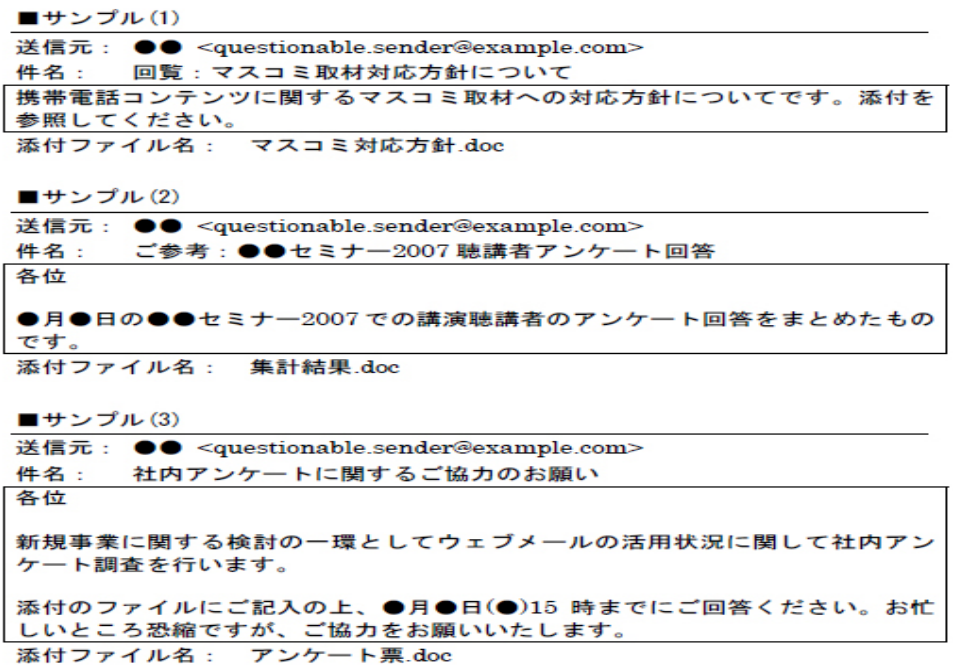

図 2.3: 標的型攻撃の実例

表 2.1: 電子メールを用いた攻撃の分類

レベル	主な特徴 (アドレス)	主な特徴 (本文・件名)
5	内部情報など	特化
4	公開情報など	特化
3	時事的なテーマ	特化
2	時事的なテーマ	特化せず
1	特化せず	特化せず

用して文章を特化させたもの，レベル 5 が公開されていない内部情報を利用して文章を受信者に特化させたものと規定した．レベルの数値が上がるほどユーザはそれを受信した際に標的型攻撃であると判定するのが難しくなる．特に，4，5 は一見しただけではなりすましではなく，本来想定している相手からの電子メールであると誤判定する可能性が極めて高い．

2.4 本論文において対象とする攻撃

本研究での対象とした攻撃は，電子メールを利用した攻撃の中で，以下の 3 つの条件に当てはまる攻撃とし，対策手法において判定を行うものとする．

- ある人物になりすまして送信された電子メール
- メールアドレスや送信者名を偽装していること
- 本文が受信者に応じた内容であること

これらを満たすのは，表 2.1 のレベル 3 〜 5 にあたる攻撃である．また，過去に一度も受信したことがないアドレスからのメールも判別できるようにすることとする．

第3章　標的型攻撃への対策と課題

電子メールを利用した攻撃は複数の種類があり，それぞれ対策が行われている．本章では，それらの対策をサーバ側での実装とクライアント側での実装に分類し，標的型攻撃への対応が可能か否かを中心に検討する．なお，サーバ側での実装として送信ドメイン認証，クライアント側での実装としてベイジアンフィルタを例として取り上げる．既存の技術を検討した上で，標的型攻撃への対策として最も妥当な実装方法を検討する．

3.1　標的型攻撃への対策

セキュリティ上の脅威に対する対策として，一般ユーザが最も対策できるものがセキュリティ対策ソフトの導入である．現在のセキュリティ対策ソフトは従来からあるアンチウイルス機能だけでなく，パーソナルファイアウォールや，ブラウザでサイトにアクセスする際のレピュテーション，保護者機能などの様々な機能を備えている．多機能化したセキュリティ対策ソフトは，複数のベンダーから販売され，誰でも購入可能になった．それらの有料セキュリティソフトウェア以外でも無料のセキュリティ対策ソフトが配布されており，ユーザの任意で選ぶことができる．また，電子メールに限れば，SPAM メール対策はそれらの対策ソフト以外の形でも提供されており，本研究で利用した Mozilla Thunderbird[1] や，web を利用した Google 社の GMail[9] にも対策が実装されている．

次に，サーバで実装されている対策について述べる．POPFile[10] や送信ドメイン認証など実装されている対策には複数の種類がある．本節では，セキュリティ対策のサーバへの実装による対策とクライアント側での対策を比較する．なお，以下電子メールを利用した攻撃への対策を前提としている．

3.1.1　サーバでの実装

電子メールを利用した攻撃対策のサーバでの実装の例として，送信ドメイン認証があげられる．

送信ドメイン認証では，メールアドレスのドメインをチェックし，その電子メールが正規のサーバから発信されているか否かを検証し，送信者のアドレスが正規のものであることを証明する．電子メールを利用した攻撃では，送信者を偽ってメールを送る「なりすまし」が行われるため，なりすまし防止のために利用される技術である．送信ドメイン認証の技術には大きく分けて，IP アドレスを利用する方式と電子署名を利用する方式の 2 つが存在する．

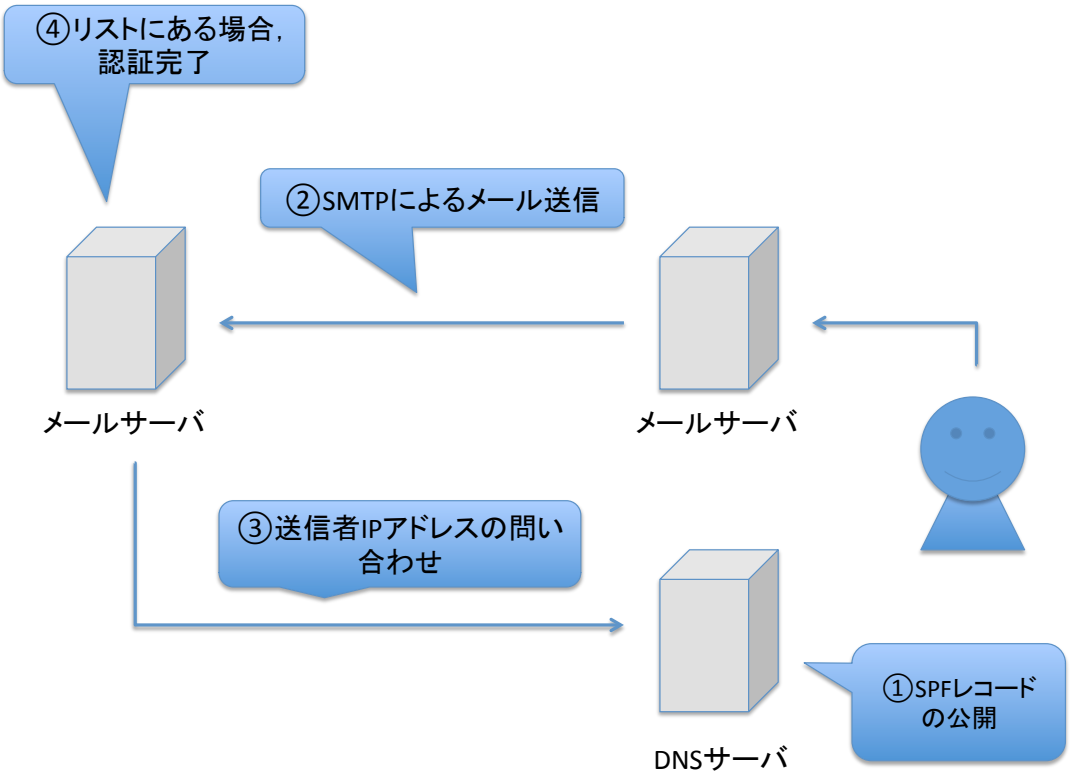

図 3.1: IP アドレスによる認証

一つ目の IP アドレスによる認証を行う方式では，エンベロープの送信者（SMTP プロトコルにおいて，MAIL FROM:の引数として与えられるアドレス）かメールヘッダ上の送信者（RFC で規定されている電子メールヘッダに記録された送信者）のいずれかのアドレスを利用する．メールを送信する側では，DNS に自身のドメインからメールを送信する可能性のあるホストのリストを公開する．そして，メールを受信する側では，メールの受信中にメールの送信者のドメイン部分を取り出し，そのドメインの DNS から公開されたレコードを読み出して，メールの送信者の IP アドレスがそのリストに含まれているかをチェックする．そして，それが含まれている場合に，認証される．IP アドレスによる認証の流れを図 3.1 に示す．

次の電子署名による認証を行う方式には，DomainKeys と DKIM の 2 つがある．どちらもあらかじめ電子署名の照合に利用する公開鍵を DNS サーバーに設置し，電子メールにそのデータをもとにした電子署名を付与して送信する．受け取った電子メールサーバは，その電子署名の引数からドメインを取り出し，DNS に公開鍵を問い合わせ，取得した公開鍵を使って電子署名を検証する．電子署名による認証の流れを図 3.2 に示す．

送信ドメインの認証は概要において「なりすまし」を防ぐ手段としてあげた通り，標的型攻撃へも応用することができる対策手法であると考えられる．しかし，標的型攻撃はアドレスも偽装されているため，たとえ正規のサーバを利用して送られたものであっても，

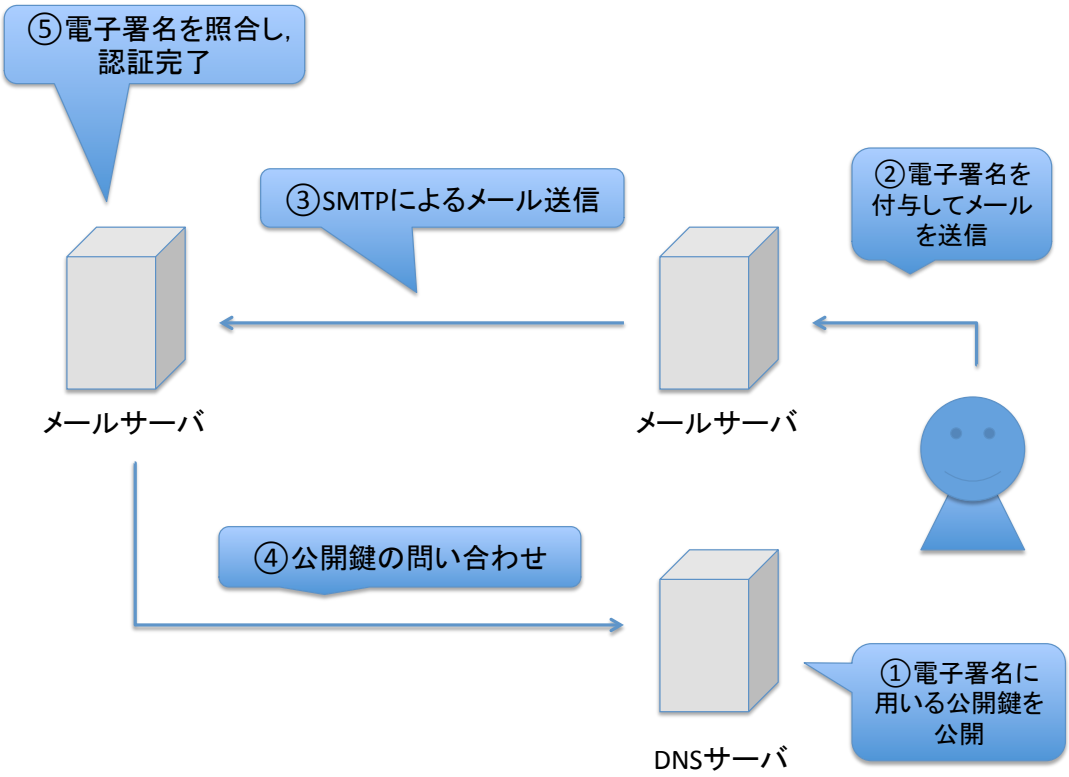

図 3.2: 電子署名による認証

それが本人かどうかについての保証されたとはいえない．例えば，取引先の A 氏とのやりとりにおいて，攻撃者が，A 氏が普段利用していないサーバを利用しながら，A 氏のアドレスから送られたものであると偽装して攻撃してきた場合には送信ドメイン認証によってそれがなりすましであると判断することができる．しかし，攻撃者が取引先のサーバを利用して電子メールを送った場合にはドメインは正規のものを利用することができると考えられるため，ドメイン認証による対策は難しい．

3.1.2 クライアントでの実装

電子メールユーザが普段利用しているコンピュータ上で攻撃への対策を行う方式である．クライアント側の実装の例として，ベイジアンフィルタが挙げられる．

ベイジアンフィルタは，ベイズの定理を応用し，データを解析・学習・分類するためのフィルタである．現在の振り分け対象となるデータの学習量が増えると振り分ける精度が高くなるという特徴を持っている．個々の判定を間違えた場合にはユーザが判定し直すことで再学習を行う必要があるが，振り分け精度の向上にともなって，再学習の頻度は少なくなる．主に，SPAM フィルターとして，SPAM の判定に用いられている．

従来型のキーワード指定によるフィルタとは異なり，対象データの内容をフィルタが学

習して自動的に分類するため，ユーザーがキーワード指定を行う必要が無い．そのため適切なキーワード指定ができない初心者に向いていると言われている．また，電子メールの内容に関わらず，統計的に解析するため，大量の迷惑メールを受信する場合などにも向いている．補足用機能として，特定のキーワードやアドレスのメールはフィルタに優先して受け付けるなどの機能を有するものもある．

ベイジアンフィルタにおいては，実装により異なるが，電子メールの件名，本文を対象にしてデータの抽出を行なっている．取得するデータは文字情報であり，SPAM メールなどの攻撃を目的としたメールに高頻度で出現する文字を抽出することで，受信した電子メールを SPAM メールであると判断している．しかし，それらを応用して作られている現在のベイジアンフィルタは主に SPAM メールを対象としており，一般的な電子メールと同じ文字列を利用している標的型攻撃に応用することは難しい．

3.2 まとめ

本章では，電子メールを利用した攻撃への対策手法の実装方法を，サーバ側での実装とクライアント側での実装の二つに分け，それぞれの実例も交えながら標的型攻撃への利用可能性などを検討した．しかし，これらの一般的手法では，標的型攻撃を防ぐことはできない．送信元ドメイン認証であれば，電子メールをやり取りする人とあわせて対策を導入する必要があるし，ベイジアンフィルタでは，一般に電子メールで用いられる文面を攻撃と判定することはできない．そのため，標的型攻撃対策を行うため，本研究では，対策の導入が比較的容易であること，件名や本文以外の要素であるヘッダ情報を利用することを対策の要件とすることで解決することとした．

第4章　関連研究

本章では関連研究として標的型攻撃への対策に関する研究および，電子メールヘッダを利用した研究について述べる．

4.1　標的型攻撃の分析

日本国内においては，JPCERT/CC や IPA から標的型攻撃の調査研究に関する文書が公開されている．それらは標的型攻撃の一例を紹介し，対策方法をまとめている．JPCERT/CC の,「標的型攻撃対策手法に関する調査報告書」[11] では標的型攻撃の実態を公開文献と国内組織へのヒアリングによって調査し，その内容に即した効果的な対策手法 を報告書としてまとめている．IPA では,「脆弱性を利用した新たなる脅威の監視・分析による調査」[12] と「脆弱性を狙った脅威の分析と対策について Vol .3」[13] があげられる．標的型攻撃を含む新たな脅威に向けた対策方法を検討たり，実例をあげた上で，標的型攻撃違和感に気づくポイントと違和感に気づいた後の対策を公表している．この他，IPA では「情報セキュリティ安心相談窓口」[14] を設置し情報を収集し，対策を提案している．

4.2　予防接種による対策

標的型攻撃への対策として，情報セキュリティ教育手法のひとつである予防接種を利用した研究 [15] である．予防接種の有効性を検証し， 有効な実施手法等について考察，提案している．予防接種は，標的型攻撃を模した「疑似攻撃メール」を送付して行っている．疑似攻撃メールは，添付ファイル付きの電子メールで，添付ファイルには，メール自体が疑似攻撃であり無害であることや，連絡先，対策や注意点などが記載される．論文内において,「メールを出す」という行為のみで実施できるため，コストが低く，組織状況に関係なく実施しやすい，費用対効果が高い方法であると述べられている．

特定の組織に対して，ある一定の効果を挙げることは論文からも明らかではあるが，より多くの人に対して標的型攻撃の対策を実施するためには，時間や費用などのコストが多く掛かってしまうと考えられる．また，内部の人が作成した標的型攻撃は，内部の人のみが知り得る情報を含むことができるため，それを判別することは難しい．

4.3 送信ドメイン認証による対策

送信ドメイン認証を用いた対策では，DNS と連携したり，ヘッダに情報を追加することで対策している．送信ドメイン認証を利用した研究や実装について本節で例を挙げる．

4.3.1 送信ドメイン認証とフィッシングメール防御

フィッシングメールの特性についてメールヘッダを基に解析し，フィッシングメールに対するフィルタリング手法を提案した研究 [16] である．

こちらの論文では，メールフィルタリング手法の中でも特にフィッシングメールに着目し，新たに定義された DNS 問い合わせベースの送信者信頼コストとコンテンツコストによるフィッシングメールを定量的に評価する手法を提案している．具体的には，ヘッダ情報を調査し，送信者の電子メールアドレスのドメインが存在しない場合，送信者の電子メールアドレスのドメインとその電子メールの送信元となる SMTP サーバのドメインが異なる場合，送信者がメールを送信する際に経由した SMTP サーバアドレスの FQDN を DNS に問い合わせて存在しない場合，あるいは，その IP アドレスとホスト名に関して正引き，および逆引きとマッピングしない場合などを評価し，パラメータを設定した上で，それらを組み合わせて送信者の信頼度を測定している．

4.3.2 送信ドメイン認証と暗号化した電子メール

電子メールの送信元サーバを認証することにより，送信元の詐称を削減することを目的とした研究 [17] である．同時に，ユーザ間で暗号化電子メールをやり取りするための仕組みも併せて提案している. 提案されている手法の主な特徴は，ID-based 暗号を用いた送信ドメイン認証であること，SMTP 自体には手を加えずに，実装していることが挙げられる．以上に加えて，機能として，正当なサーバを経由しているかの確認を署名により行っている．また，これらは既存のサーバの機能を拡張する形で実装が行われている．

論文内で提案されている手法は，送信ドメイン認証の一つの形態である．そのため，第 3 章においてあげた送信ドメイン認証の長所欠点がそのまま当てはまるとも考えることができる．しかし，既存のサーバの機能拡張であるという点から，普及することで大きな効果が期待できると考えられる．

4.3.3 送信ドメイン認証とヘッダ情報を利用した対策

前項と同じく送信ドメイン認証を利用した手法 [18] である．この手法においては，送信サーバが，ユーザから受け取った電子メールに対してユニークな ID を生成し，それをデータベースに保存，電子メールのヘッダ内に埋め込んで送信する．受信サーバではそのヘッダが付いていた時に, 送信元アドレスのドメインに対し，その ID の付いたメールを送信したことを問い合わせてから受信する，という形態で実装を行なっている．なお，前

項の手法と同じように，どちらか一方のサーバが対応していない場合は従来通りの電子メー ルとして受信される．

こちらの手法も，サーバを利用した送信ドメイン認証の一種であることから，送信側と受信側のサーバが共に動作を行う必要がある．そのため，前項と同様に送信ドメイン認証の長所短所が適用されると考えられる．

4.3.4 携帯電話での対策

携帯電話各社 [19][20][21][22][23] では，Sender ID ／ SPF による送信ドメイン認証を行っている．迷惑メールを防止するため，送信元 IP アドレスと，DNS サーバに公開された送信用メールサーバの IP アドレスとを比較し，それらが合致した場合にのみメール受信している．なお，不一致の場合や，送信元 IP アドレスが DNS サーバに存在しない場合には受信しないという機能がある．なお，ユーザはそれぞれに用意された設定画面から，送信ドメイン認証を利用するか否かを選択することが可能である．

4.4 まとめ

本研究に関連する研究として，標的型攻撃に関するものと送信ドメイン認証に関するものを挙げた．前章でも述べているが，既存の対策では標的型攻撃への適応は難しい．また，送信ドメイン認証に関連した研究はサーバ側での実装であることから，広く一般に普及するまでは対策として十分な機能が果たせることを期待できない．そこで，広く一般の人が対策を導入しやすい形態は何か，サーバとサーバなど２つ以上のコンピュータを連携させることなく対策することができないか検討を行う必要があるだろう．それらの比較については第 3 章で述べた．次章では，具体的な対策として本論文で提案する手法について述べる．

第5章　電子メールヘッダ情報の取得と蓄積による対策

本章では，電子メールを利用した攻撃，その中でも，第2章で述べた標的型攻撃への対策手法を提案する．

5.1　対策の概要

クライアント単体による標的型攻撃への対策として，電子メールから取得したヘッダ情報を蓄積し，それを元に検知する手法を提案する．電子メールを受信した際に，過去に同じアドレスからきた電子メールがどのような環境からきたものであったか調査を行い，過去に利用されたことのない環境から送られたヘッダ情報が含まれる電子メールを受信した際に，標的型攻撃の可能性があるとして，ユーザに注意を促す．

5.2　前提

本手法では，標的型攻撃の判別にヘッダ情報を利用した．第2章で述べた通り，クライアント単体で動作する対策であるため，利用できる情報が限られる．利用できる情報は，電子メールの本文，件名，ヘッダ情報の３つである．標的型攻撃では，本文や件名には特徴はほとんどなく，通常送られてくるメールと相違がないため，ヘッダ情報を利用する．

ヘッダ情報はいくつかの情報からなる．詳細な内容は5.4.1節で述べるが，ヘッダ情報には，電子メールの送信元から受信者に到達するまでに経由したサーバ，送信者のタイムゾーン，送信者の利用した電子メールクライアントなどの情報がある．もちろん，それらの情報は送信者ごと，送信する場所などにより異なる．また，同じ場所で送信した時であっても，利用する送信サーバが異なる場合があり，常に同一のヘッダ情報になる保証はない．そこで，送信元が利用しているIPアドレスをある一定の範囲について同様のものとみなし，電子メールクライアント情報を大まかなバージョンごとにまとめることで情報に傾向が出るのではないかと考えた．本手法で想定するユーザが電子メールを送る主な利用箇所は以下のとおりである

1. 自宅
   自宅での通信．デスクトップ型・ラップトップ型のパーソナルコンピュータ，無線LAN機器を利用した携帯端末などによる通信．

2. 職場 (学校)
利用者が自宅外で利用する中で，職場や学校などで自身の所有するパーソナルコンピュータや，備え付けのパーソナルコンピュータを利用する場合の通信．

3. 携帯端末 (スマートフォンなど)
近年，急速に普及しているスマートフォンを利用した通信．一部，従来の携帯電話による通信も含む，携帯端末単体での利用によるもの．

4. モバイルブロードバンド
携帯電話と同じ通信網を利用したものや，WiMAX による通信．端末はその他のパーソナルコンピュータに接続して利用する通信．

5. その他 (出張先のホテルなど)
上記以外の通信．外出先の Wi-Fi スポットや，出張先のホテルなどでの通信．

その中でも 5 は比較的特殊な場所での利用であると考えられるため，ユーザが電子メールを送信する環境は 1 〜 4 に集約されるものと考えられる．そして，4 つ程度に集約するのであれば，過去に同じ送信者がどの環境（送信元 IP アドレス，電子メールクライアント，タイムゾーンなど）にいたかの情報を蓄積し，受信した電子メールのヘッダ情報と比較することで，普段は送信していない環境からの送信を判定できると考えた．ユーザが普段送信しない環境から送られた電子メールであるならば，本来のアドレスの所有者が送った電子メールではない可能性が考えられる．5 の場合で，いつもと違う出先から電子メールを送信した場合など，本人が通常と違う環境から送った可能性も考えられる．しかし，ヘッダ情報から得られる情報でそれを完全に推測することは難しいため，普段利用していると考えられる環境以外からの送信を異常と検知することで，標的型攻撃の判別に利用することとした．

本手法では，電子メールヘッダ情報の異常検知を行っている．通常の環境と違う場合に標的型攻撃の可能性があると判定を行っているため，初めて受信する電子メールアドレスからのメールである場合や，いつもは国内にいる人が急に海外から送った場合などにも警告を発することが可能である．

5.3 事前調査

前節で設定した前提は推測であるため，ヘッダ情報を蓄積し比較することで異常を検知することが可能か否か，そしてそれらの情報が標的型攻撃の判定に有効であるかを調査して，どの程度情報が収束するのか，どのヘッダ情報であれば判定に有効であるかを検証する必要がある．そこで，本研究で主に利用している IP アドレスと電子メールクライアントの 2 つの情報について調査した．調査は，あるユーザの特定期間の電子メールからの情報を抽出した上で，それらのデータがどの程度まとまるのか，一定の傾向はあるのかの 2 点の検証をした．検証には，実際に筆者が受信した電子メールを利用した．調査対象は 2 名とし，一方に異常な数値が出た場合に対応できることとした．本研究の提案手法では，

表 5.1: IP アドレスの調査結果

出現順位	ユーザ A	ユーザ B
1 位	121.2.xxx.yyy(33)	222.228.xxx.yy(108)
2 位	120.75.xx.yy(14)	131.11.xxx.yy(57)
3 位	120.75.xxx.yy(12)	133.27.xx.yyy(15)
4 位	219.98.xxx.yyy(11)	133.27.xx.yyy(11)
5 位	218.41.xx.yy(6)	133.27.xxx.yyy(9)
5 位までの数/母数	76/123	200/269

表 5.2: 電子メールクライアントの調査結果

出現順位	ユーザ A	ユーザ B
1 位	Thunderbird2.0.0.23(59)	Thunderbird2.0.0.23(104)
2 位	Thunderbird3.0.6(13)	Thunderbird2.0.0.21(66)
3 位	Thunderbird2.0.0.21(11)	Thunderbird2.0.0.22(33)
4 位	Thunderbird3.0.5(11)	Thunderbird2.0.0.21(33)
5 位	Thunderbird2.0.0.22(10)	Thunderbird3.0.4(14)
5 位までの数/母数	104/123	250/269

取得する情報が年月を経るごとに変化することが考えられる．電子メールクライアントであれば，長期的にみればバージョンアップが行われ，利用する送信元サーバも変化する可能性がある．そこで，本手法が長期間の利用であっても有用であるかについても調査を行うため，2009 年 4 月〜2010 年 8 月の 1 年 4ヶ月間と長期間の電子メールを調査の対象とした．IP アドレスでの調査結果を表 5.1 に，電子メールクライアントでの調査結果を表 5.2 に示す．

IP アドレスでは，ユーザ A で約 62 %，ユーザ B で約 74 % のデータが 1 〜 5 位までのデータに収束した．なお，表 5.1 に示した IP アドレスは，前述の加工を行わず，完全一致のみを用いている．第 3 オクテットまでに加工した場合は，多くのデータが上位 5 つに収束した．そのため，完全一致では，攻撃の判定に利用できないが，第 3 オクテットまでに加工するなどすれば，判定に利用可能である判断した．

次の電子メールクライアントは，調査したユーザ A，B ともに利用しているクライアントが同じであったが，バージョンの違いも含めた完全一致を行った．細かいバージョンの違いまで含めたが，ユーザ A で約 85 %，ユーザ B で約 93 % に収束した．今回結果に出た Thunderbird は，定期的にバージョンアップが行われていることを考慮し，判定に利用可能であると判断した．

以上の結果より，ヘッダ情報を蓄積することで，ユーザが普段利用しない環境からの電

子メールを判別することは可能である．しかし，ひとつの情報だけでは誤判定を起こす可能性があるため，これらの情報に加えてタイムゾーンなど複数の情報を組み合わせて，実装することとした．

5.4 提案手法

第 3 章に述べた特徴と，5.2 節で述べた特徴を持つものとして電子メールヘッダの特徴情報を利用して標的型攻撃の検知を行う手法の概要を説明する．なお，クライアント側に実装を行うため，実装には電子メールクライアントに機能を拡張した．

本手法の動作は大きく 3 つに分けられる．その流れに従って概要を述べる．

5.4.1 情報の収集

本研究において収集する情報は電子メールヘッダ情報である．電子メールヘッダ情報は，クライアント環境で取得する場合，一般的に利用されている電子メールクライアントで閲覧，収集が可能である．今回研究で利用した Mozilla Thunderbird3 であれば，電子メール画面の宛先などが表示されている画面の「その他の操作」→「ソースの表示」で閲覧できる．しかし，ソースの表示によって提示される情報は，電子メールのヘッダ，件名，本文が一覧で記入されており，情報に応じて分類するなどの整理は行われていない．

電子メールヘッダにある情報は，送信元，送信先の電子メールアドレス，送信・受信時刻，電子メールの送信経路， 送信元が使用した電子メールクライアントなどが挙げられる．以下で，ヘッダ情報のうち主要な項目に関して簡単に述べる．

- From
  送信元の電子メールアドレス

- Date
  送信元が電子メールを送信した日時

- Received
  電子メールの経路を表す.「Received from A by B」のような形で記述され，A から B 宛に電子メールが配送されたことを表している．複数のサーバを経由することが多いため，複数行にわたって記述されることが多く，下の行ほど送信元に，上の行ほど送信先に近いことを示す．

- Message-ID
  電子メールにつけられる ID.「ID @ ドメイン名」の形で記述され，各サーバごとにユニークであることが求められるため，同じ ID を付されたメールは基本的に存在しない．

Return-Path: ⟨*test@aaa.keio.ac.jp*⟩
Received: from example.aaa.wide.ad.jp (example.aaa.wide.ad.jp [aaa.bbb.xxx.yyy])
by ex.aaa.wide.ad.jp (Postfix) with ESMTPS id 45F3E2340AF;
Tue, 14 Dec 2010 10:40:34 +0900 (JST)
Received: from ex.aaa.keio.ac.jp ([aaa.bb.x.yyy])
by ex.aaa.wide.ad.jp with ESMTP; 21 Dec 2010 21:28:36 +0900
Received: from sample.aaa.keio.ac.jp ([aaa.bb.x.yyy])
by sample.sfc.keio.ac.jp with ESMTP; 14 Dec 2010 10:40:34 +0900
Message-ID: ⟨4*D*109*D*71.3049604@*aaa.keio.ac.jp*⟩
Date: Tue, 14 Dec 2010 10:40:34 +0900
From: test name ⟨*test@aaa.keio.ac.jp*⟩
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; ja; rv:1.9.2.13) Gecko/20101207 Thunderbird/3.1.7
MIME-Version: 1.0

図 5.1: 電子メールヘッダの例

- Reply-To
  電子メールの返送先を表す．通常，指定がない場合には From と同じアドレスが記入されている．

- X-Mailer
  送信元が使用している電子メールクライアントを表す．

上で挙げている情報以外にも経由したサーバや送信元の電子メールクライアントによって付加されるヘッダがある．今回は，一般的にどの電子メールにもある項目について列挙した．また，これらの項目は，本研究において標的型攻撃への対策に利用できるものとして実装においても取得している情報である．電子メールヘッダの例を図 5.4.1 に挙げる．

本研究においては，電子メールクライアントを利用して，受信した電子メールより情報を取得し，整理して表示した．この機能は電子メールクライアントに標準で実装されているものではないため，機能拡張を行うことで対応した．

5.4.2 情報の蓄積

本対策の手法において，従来の対策と異なる点が，蓄積を採用していることである．従来の電子メールヘッダを利用した対策では，受信したメールのヘッダ情報を取得し，それをもとにサーバにアクセスして情報を確認する形態をとっている対策が多い．サーバ側で情報を保管する手法は，各ユーザがやりとりするアドレスは人によって様々である上に，勝手に情報を収集するのでは，個人情報保護の観点から問題がある．そこで，本研究にお

いて提案する手法では，取得した電子メールヘッダ情報をユーザ所有の環境 (クライアント環境) に随時保管する手法を採用した．

本研究においては，前項で取得した情報を汎用的なファイル形式に変換して保存している．保存により，蓄積された過去の情報との照合を行い判定を行う機能をサポートしている．情報は，送信元アドレスおよび Message-ID によって管理され，重複なく情報を蓄積することを可能にした．また，汎用的なファイル形式として，txt ファイルを採用している．汎用的なファイル形式を採用し，必要な情報のみを csv と同じカンマ区切りで情報を蓄積することでアドオン以外のテキストエディタなどからの情報の編集を可能にした．

5.4.3 結果の表示

一般的な攻撃への対策手法において，攻撃を識別するための結果表示画面には多種多様な種類がある．そこで，誤判定の処理を検討する必要がある．なぜなら，受信した電子メールを攻撃であると誤検知したにも関わらず，自動的に電子メールをゴミ箱に移動する隔離を行った場合，ユーザに不利益を与えてしまうからだ．電子メールを利用した攻撃を完全に識別することが可能であれば，隔離などの措置を自動的に行うことができるが，現状では電子メールを利用した攻撃では処理をユーザの判断に任せていく必要がある．そのため，標的型攻撃を判定した場合は，電子メールを隔離せずに，ユーザに警告を発する．ユーザが識別しやすい位置に警告用の画像を表示することで，ユーザに電子メールヘッダに異常があったことを示す．画像は数段階の色を用いて標的型攻撃の可能性を示す．

第6章　実装

本手法を実装するために，機能拡張に対応している電子メールクライアントとしてMozilla Thunderbird を利用した．Mozilla Thunderbird は，OS に依存せず利用することができ，Microsoft 社の Windows だけでなく，Apple 社の Mac OS X といった一般に販売され利用されている OS や，Linux や BSD 系の Unix などの OS に対応している．また，機能の追加が容易に可能である，アドオンと呼ばれるプラグイン機能がサポートされており，規格にあったプログラムを作成すれば，許諾を待つことなく，誰でも Thunderbird の機能を拡張することが可能である．以下，本章において，実装するプログラムをアドオンと称することとする．実装したプログラムの動作概要を図 6.1 に示す．

本研究では，Thunderbird の最新版である Mozilla Thunderbird 3[1] を利用した．Mozilla のプラグインは xpi というファイルで表される．xpi ファイルは ZIP 形式でまとめられた複数のファイルで構成され．中には以下のようなファイルが含まれている．

- install.rdf
  アドオンのタイトルや，作成者，対応する Thunderbird のバージョンが記載される
- chrome.manifest
  アドオンのインターフェイスを Thunderbird に組み込む際に利用する
- *.xul
  アドオンのインターフェイスを定義する
- *.js
  アドオンの動作を定義する

プラグインによっては以上の他に言語ファイルや画像ファイルなどを含んでいるが，本研究で実装したアドオンでは，以上の 4 種類のファイルで構成した．

アドオンは Thunderbird にインストールされた時点から自動で情報の収集を行なっている他，必要に応じて過去に受信した電子メールから一括してヘッダ情報を取得することも可能である．以下では 5.4 節で利用した収集，蓄積，表示の 3 つに分けて詳しい実装方法を述べる．

6.1　収集

アドオンは，新たに電子メールを開いた際にその電子メールヘッダより送信元電子メールアドレス，送信元 IP アドレスおよび送信元ドメイン，電子メールクライアント，Message-

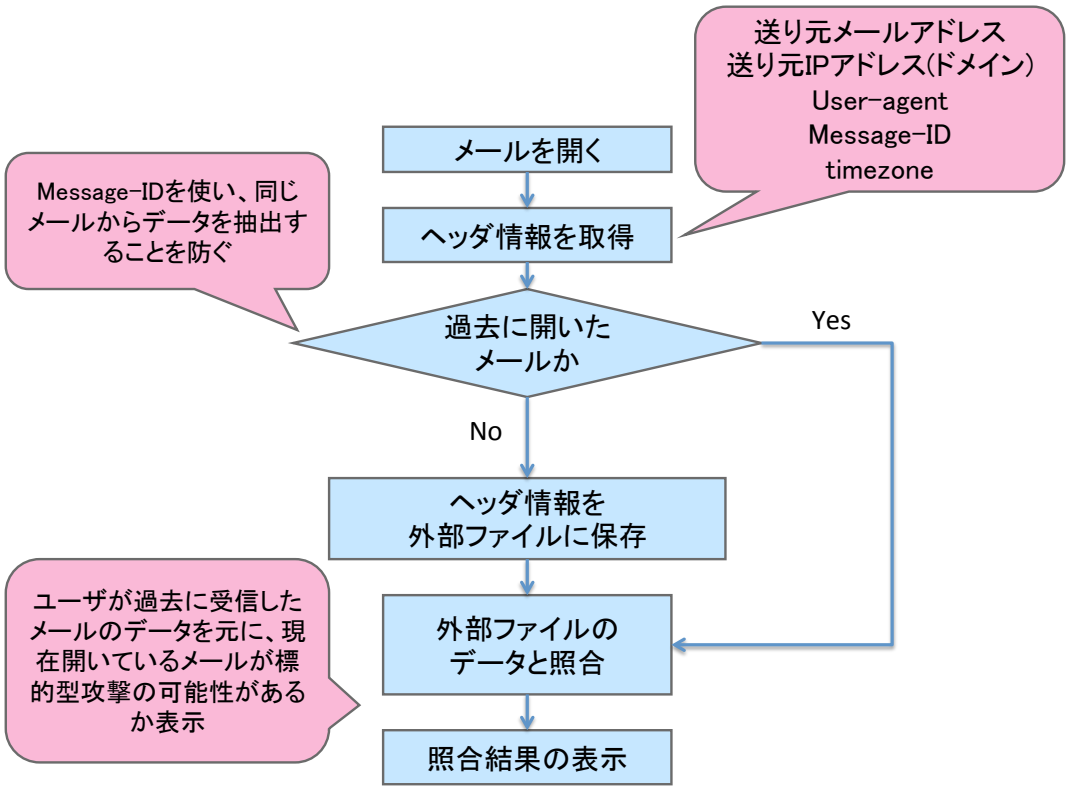

図 6.1: 実装したプログラムの動作概要

ID，Time-zone を取得する．情報を取得している箇所は以下のとおりである．

- 送信元 IP アドレス
  「Received： from」から始まる複数の行の中から，一番送信者に近い情報である，ヘッダ情報の中で最後に記入されているものを利用した．なお，Received:from には，中継するサーバが IP アドレスよりドメイン名を逆引きして載せているため，ドメインも同時に取得している．送信元 IP アドレスは偽装される可能性があるが，今回の実装では，他の情報を併用することにより検知できなくなることを防いでいる．また，IP アドレスは IPv4 のみを対象とし，IPv6 については対象外とした．

- 電子メールクライアント
  「User-agent」若しくは「X-Mailer」より取得．なお，本研究で利用している Mozilla Thunderbird は，ヘッダ情報が「Mozilla/5.0 (Windows; U; Windows NT 6.1; ja; rv:1.9.2.13) Gecko/20101207 Thunderbird/3.1.7」などのように長くなっているため，「Thunderbird 3.1」のように短い情報に加工している．加工の際，バージョン情報を「3.1.7」から「3.1」にすることで細かなバージョンの違いを異常と検知しないようにした．

- Message-ID

「Message-ID」より取得．5.4.1 節に述べたとおり，各ドメインごとにユニークであることから，各メッセージの識別子として利用し，情報の蓄積の際に，同じアドレスから情報を取得していないかチェックしている．

- Time-zone
  クライアントのデータを利用するため,「Date」より取得．末尾に保管されているタイムゾーン情報を取得．日本国内の場合，末尾に「+0900」とある．

これらの情報は，蓄積する情報としている他，各電子メールが標的型攻撃であるかの判定を行う際に利用している．

6.2 蓄積

蓄積したファイルの例を図 6.2 に示す．
情報の蓄積では，6.1 節で取得したデータをアドオン専用のディレクトリに保存している．本手法では，Thunderbird の各個人の設定ファイルなどが保存されている Profile ディレクトリを利用した．ファイルはアドレスごとに用意し，同じ送信元アドレスの場合は同じファイルに保存される．また，前節に述べたとおり，重複したデータを取得することを避けるため，各データは Message-ID を用いて管理した．情報の取得の際に取得した Message-ID を蓄積したデータと比較し，同じ Message-ID が存在する場合には，同じ電子メールから過去にデータを取得していると判断し，外部ファイルへの保存は行わない．外部ファイルに保存しているデータは，情報の取得の段階で取得したデータをすべて蓄積している．

6.3 表示

抽出した情報をもとに標的型攻撃の可能性を判定し，結果をユーザが注目しやすいように視覚的に表示する．判定は標的型攻撃であるか否かではなく，複数の情報を組み合わせて，怪しさの度合いを表示する．判定した結果を段階的に色やマークを使ってユーザがその危険性を判別しやすいように表示する．メッセージソースを読むことなく，標的型攻撃であるかどうかの判断を支援する機能を実装した．本研究では，電子メールヘッダ情報を読むことができないユーザが標的型攻撃であるかの判断を可能にすることを目的とするため，ユーザに対して，標的型攻撃の可能性かどうか情報のみを提供することでも十分に効果がある．そのため，標的型攻撃の可能性があるとアドオンが判断した場合やユーザが怪しいと判断した場合など，ユーザの任意のタイミングで受信したメールに関する情報を閲覧する機能も有している．

- 判定
  IP アドレスは第 3 オクテットまでで比較を行ない，第 3 オクテットまでの一致をもって，過去に同じ IP アドレスから送られてきていると判断している．5.2 節でも述べたとおり，送信元 IP アドレスは利用するサーバによって異なり，ISP サービス

⟨4A9ED4A3.3054349@sfc.wide.ad.jp⟩ , 211.10.aa.bb, d0d4a32.tokyte00.ap.so-net.ne.jp, Thunderbird 2.0.0.23 (Windows/20090812), Thunderbird 2.0, +0900, 03 Sep 2009

⟨4A88DBAF.3949503@sfc.wide.ad.jp⟩ , 211.10.aa.bb, d0d4a32.tokyte00.ap.so-net.ne.jp, Thunderbird 2.0.0.22 (Windows/20090605), Thunderbird 2.0, +0900, 17 Aug 2009

⟨4A55B38A.0032345@sfc.wide.ad.jp⟩ , 211.10.aa.bb, d0d4a32.tokyte00.ap.so-net.ne.jp, Thunderbird 2.0.0.22 (Windows/20090605), Thunderbird 2.0, +0900, 09 Jul 2009

⟨4A4C76C7.2235954@sfc.wide.ad.jp⟩ , 133.27.aa.ccc, aa-a.sfc.keio.ac.jp, Thunderbird 2.0.0.22 (Windows/20090605), Thunderbird 2.0, +0900, 02 Jul 2009

⟨4A434060.3302033@sfc.wide.ad.jp⟩ , 133.27.aa.ccc, aa-a.sfc.keio.ac.jp, Thunderbird 2.0.0.22 (Windows/20090605), Thunderbird 2.0, +0900, 25 Jun 2009

⟨4A3A058E.2294853@sfc.wide.ad.jp⟩ , 133.27.aa.ccc, aa-a.sfc.keio.ac.jp, Thunderbird 2.0.0.21 (Windows/20090302), Thunderbird 2.0, +0900, 18 Jun 2009

図 6.2: 蓄積しているファイル

図 6.3: 結果の表示

の電子メールであれば特に大きくなることが予想される．しかし，利用するサービスにより IP アドレスの範囲は異なることから，IP アドレスのクラス分類において一番範囲が狭いクラス C を参考に，第 3 オクテットまでの一致をもって，同様の IP アドレスからの送信であるとした．電子メールクライアントは，Thunderbird についてのみ，加工した情報を利用している．その他のクライアントおよび Time-zone その他の情報は，完全一致を用いて比較を行なっている．

- 表示
  アドオンの警告表示の例を図 6.3 に示す．警告は，メッセージの送信者や件名などを表示している場所に画像によって表示している．ユーザがアドオンを導入したことによる煩わしさを軽減するため，アラートによる表示は行わない．しかし，ユーザに対して確実に情報を提示する必要があるため，電子メールを開いた際に，注目しやすい場所に警告用の画像を表示する．５節でも述べたが，表示は段階的なものを利用する．

第7章　評価

7.1　評価項目と期間

本研究の評価では，第6章で実装したアドオンがなりすましによる標的型攻撃の判別に有用であるかどうかの評価を行う．本研究の評価では，利用しているヘッダ情報の収束を見ることで，ユーザのヘッダ情報に特徴があるかを評価している．なお，各情報の収束を見ることで標的型攻撃の可能性判定のアルゴリズムを考察することとした．

評価は，アドオンで取得している情報を対象に行う．評価項目は以下のとおりとした．

- 評価内容
  電子メールの送信元IPアドレス，ドメイン，電子メールクライアント，タイムゾーンを送信者ごとに集計した上で，送信者を属性で分類し，各項目の傾向を調査する．提案手法が標的型攻撃の判別に有効であるかを評価するために，取得している情報の収束がどの程度あるかを評価する．また，同時に送信者の属性ごとに情報の傾向に違いが出るのかを評価する．

- 調査期間
  20010年1月1日〜2010年12月31日

- 評価データの取得元
  筆者のsfc.wide.ad.jpドメインのアドレスに届いた電子メールおよび，企業からの電子メールが送られてくるアドレスより取得

7.2　評価の結果

評価は47の個人および企業のアドレスを対象とした．それらは筆者が受信した電子メールをアドレスをもとにして，学部生，大学院生，教職員，および企業の4つに分類した．内訳は学部生16人，大学院生7人，教職員7人，企業17社である．以下では，送信元IPアドレス，送信元ドメイン，電子メールクライアント，タイムゾーンの4つの項目に分けて傾向を述べた上で，結果について考察する．

7.2.1　IPアドレス

IPアドレスの判断には，第6.3節で述べたアルゴリズムにおいて採用している第3オクテットまでを判断基準として利用した．蓄積した情報の中で，送信元IPアドレスが第3

オクテットまで一致するものを同じ場所からの送信であると仮定し，過去にどの程度同じ場所から送信されているのかを調査した．第 6 章で述べたとおり，IPv4 のみを対象としている．一般利用者の多くは固定 IP アドレスを利用してないため，IP アドレスが変動する環境にある．そのため，環境によって，IP アドレスが分散した場合を考慮した．

IP アドレスの評価結果を図 7.1 に述べる．図 7.1 には，学生の中から送信元 IP アドレスの分散に特徴のあったユーザ A およびユーザ B を例として挙げている．なお，それぞれの回数はユーザの IP アドレスが同じ IP アドレスとして判定された電子メールの数を示している．同じ IP アドレスからの電子メールをまとめ，まとめられた回数に応じて分類した．結果を見ると，ユーザ A が送信された電子メールの約 98%が過去に 2 度以上同じ IP アドレスから送信されており，ユーザ B は約 89%が過去に 2 度以上同じ IP アドレスから送信されていた．なお，ユーザ A は送信した電子メールの約 79%が自宅と推測される場所から送信されたものであり，ユーザ B はその全てが大学キャンパス内から送信された電子メールであった．

IP アドレスが，第 3 オクテットまでで一致するのかは送信者が所属するネットワークに依存しているため，サブネットマスクが/24 の場合は第 3 オクテットまでの一致を見ることで同じネットワークからの送信であると推測することができるが，/16 を利用するネットワークの場合は，第 2 オクテットまでの一致をみなければ，誤検知が多発する．そのため，IP アドレス単体で送信元を区別する場合には，送信元が所属しているネットワークのサブネットマスクを事前に知っておくことが前提となることが判明した．

そこで，誤検知に対応するため，IP アドレスをある一定のグループにまとめることが可能な情報を併用することとした．そこで，ドメイン名を利用し，IP アドレスをグループに分類した．

7.2.2 ドメイン

ドメインの評価には，第 5.2 節で述べた 5 つの分類を利用した．分類の結果を 7.2 に述べる．慶應義塾湘南藤沢キャンパスや，慶應義塾大学の他のキャンパスからの送信されたものを学校および職場に分類し，湘南藤沢キャンパス以外から送信された電子メールの中で家庭で一般的に利用される ISP であると判断されるもので数の多いものを自宅とした．また，携帯，モバイル，その他の 3 項目もドメインを元に独自に判定した．本評価では，１〜４のいずれかに分類されたものをユーザが通常送るドメインの範囲とし，５に収まったものについては，旅行や出張などによる通常送る範囲外のドメインとした．分類別の評価結果を図 7.2 に示す．

学部生では，人によってばらつきはあるものの全体では約 96%が大学か自宅から送信されたものであった．また，その中でも大学内から送信されたものが多く，約 66%が大学内から送信されたものであった．

次に，大学院生について述べる．学部生と同様に全体では約 94%が学校および自宅で送信されたものであった．しかし，各個人での差はほぼ現れず，半数以上の大学院生の送信元はすべて学校および自宅からの送信であった．

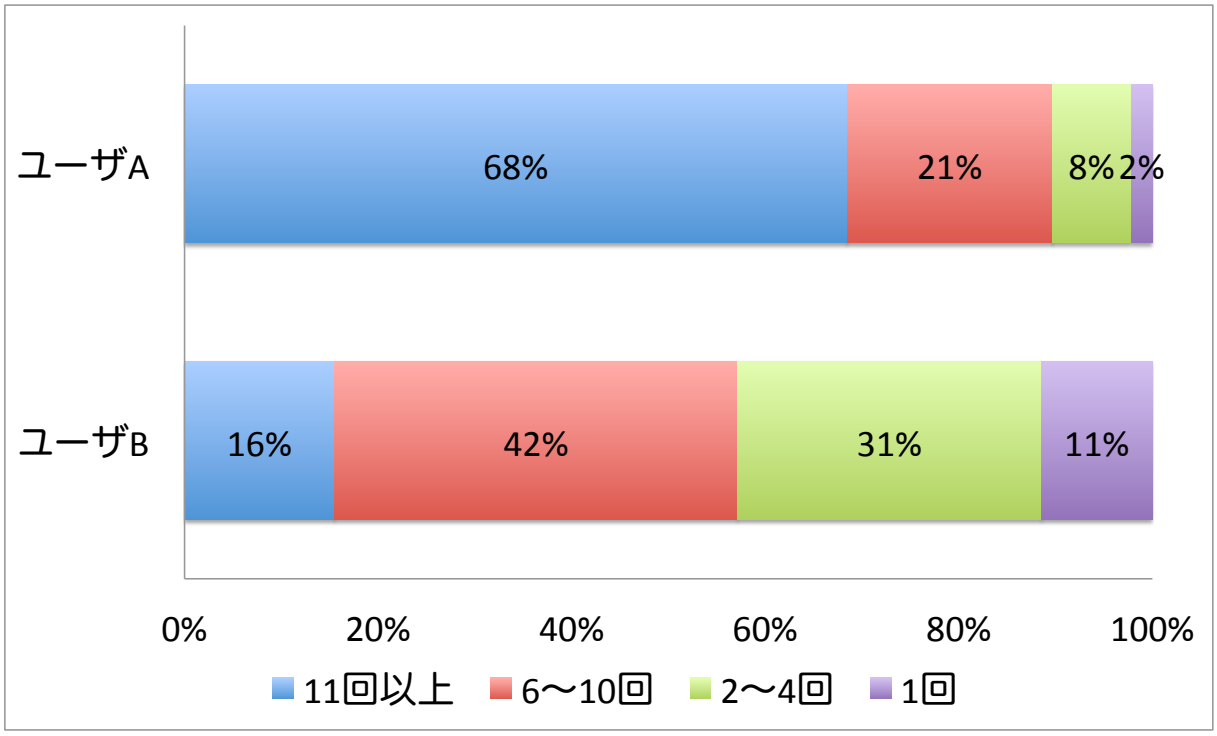

図 7.1: IP アドレスの調査結果

教職員でも，以上の 2 つの属性と同様に自宅および職場からの送信であると判断されるものが多かったが，モバイルから多くの電子メールを送る教職員もおり，全体では自宅および職場からの送信と思われる電子メールは 56%という結果になった．

最後に企業からの電子メールである．すべての電子メールにおいて，ある特定のドメインからの送信であった．また，他の属性には見られない傾向として，すべての電子メールの送信元が第 3 オクテットまで同一であることが多く，17 の企業のうち，4 つの企業ではすべての電子メールが同一 IP アドレスから送られていた．

以上の結果から，学部生および大学院生に分類された本研究室の学生は，電子メールの多くを大学内か自宅と推測される場所から送信している一方で，本研究室の教職員はそのモバイルインターネットを利用する機会も多いということがわかった．また，企業については，99%が職場から送信されていることからもわかるとおり，出先から一般個人に対して電子メールを送ることが稀であることがわかる．いずれの結果においても約 97%以上が 1 〜 4 の分類に収まることとなり，普段利用する環境以外から電子メールを送信することはほとんどないことがわかる．このことから，ユーザの送信元ドメインを蓄積して．受信した電子メールの送信元ドメインと比較することで，普段利用しない環境からの電子メールの送信を識別することが可能であり，なりすましを識別することが可能である．また，各ユーザの分類ごとの特徴と電子メールヘッダを比較することでもなりすましを判別することが可能である．

なお，旅行や出張，友人宅にいる場合や，新たに回線を契約した場合など，ユーザが普

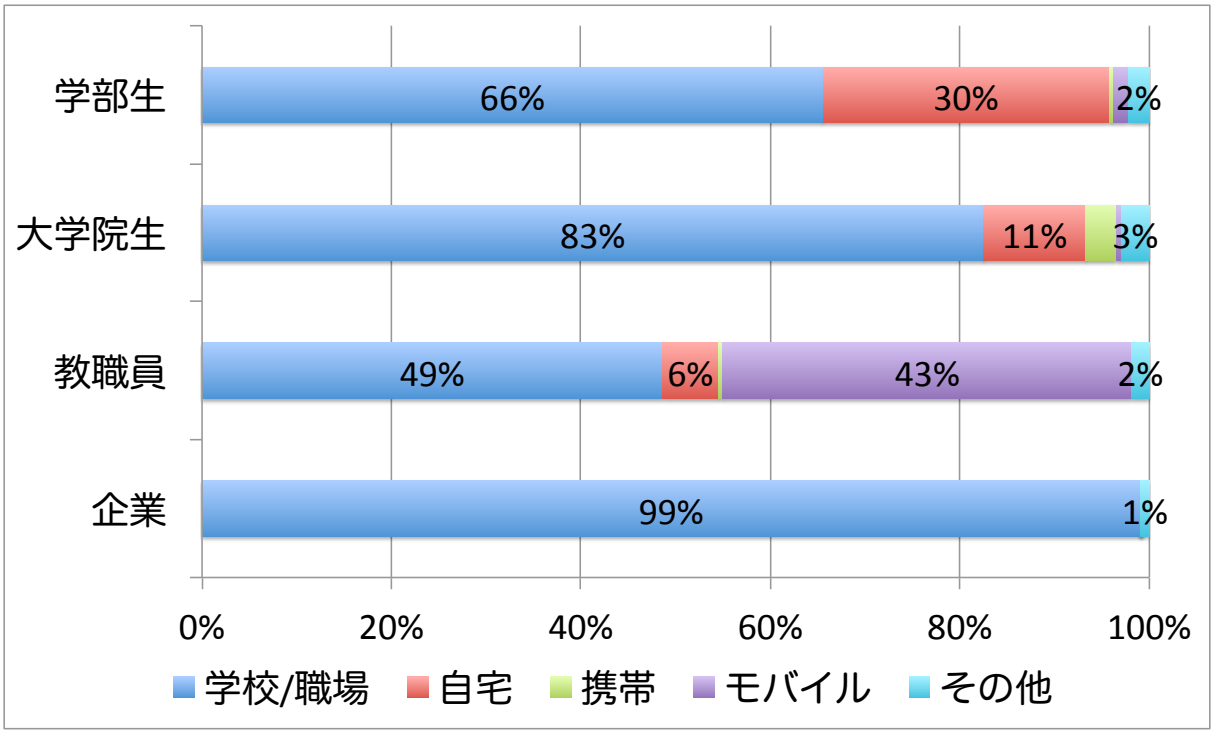

図 7.2: ドメインの調査結果

段利用する環境以外から電子メールが送信されることある．このような場合には，提案手法では誤検知してしまう可能性がある．

7.2.3 電子メールクライアント

評価の結果，電子メールクライアントでは，各属性ごとに違った傾向はなく，大学関係者 (学部生，大学院生，教職員) と企業で結果に差があらわれた．以下では，大学関係者と企業の 2 つの分類で結果を述べる．

学部生，大学院生，教職員の全体では，約 88%が Mozilla Thunderbird，約 5%が Apple 社の Mail であった．細かなバージョンの違いはあったが，全体の 93%が 2 つの電子メールクライアントの関連製品からの電子メールであった．学部生，大学院生，教職員の合計 30 人を個別に見ていくと，送信している電子メールを全てひとつの電子メールクライアントで送信している人は，13 人であった．なお，範囲を広げて，送信した電子メールの 90%以上を同じ電子メールクライアントから送信している人は 30 人中 26 人であった．

次に，企業からの電子メールでは，ClickM@iler[24] および Cuenote[25] から送られてきたものが多く約 86%がそれら二つから送信されたものであった．このふたつはいずれも電子メールの配信を行うサービスであり，企業が多くの対象に一斉に電子メールを送る際に利用されているものと考えられる．

全体では，個人で利用する電子メールクライアントが変化したのは，30 人中 16 人であっ

た．個人別で見ても，約 9 割の人が送る電子メールの 90%が同じ電子メールクライアントから送られていることがわかった．このことから，電子メールを利用した判定では，バージョンの違いを考慮に入れないことで，なりすましによる標的型攻撃を防ぐことができると判断できる．しかし，完全にバージョンの違いを取り除くと誤判定をするおそれがあるため，第 6.1 節に述べた本研究でも採用している程度のバージョンの違いによる判定が好ましいと考えられる．

本評価の結果により，ユーザは利用する電子メールクライアントを頻繁に変更することは少なく，バージョンアップが行われることによる変更を考えなければ，電子メールクライアントの変更を検知することでなりすましを判断することは可能である．また，今回の評価対象にもあったが，ユーザの中には，普段利用しているコンピュータ以外に，iPhone や Android などの携帯型デバイスに搭載されている電子メールクライアントを利用することがあり，その場合は，誤検知が発生することがある．しかし，普段から Thunderbird などのコンピュータ向けの電子メールクライアントのみを利用する人が急に iPhone[26] や Android[27] などから電子メールを送信してきた場合に，異常と検知することが必要となるため，例外とすることはできない．そこで，すべての種類の電子メールクライアントに関する情報を蓄積し，受信した電子メールの電子メールクライアントと比較することで判定をすることが可能となる．

7.2.4 タイムゾーン

評価は日本国内で行っている．そのため，受信した電子メールも 99%以上が+0900 を示し，日本国内からの送信であることがわかった．なお，本評価の期間外であったが，日本国外から電子メールを送信したと思われる電子メールがあり,「+0100」を示していた．このように，ユーザが送信する環境が変化し，タイムゾーンが変化する程度に移動した場合には，検知することが可能である．

今回の結果より，大学関係者や企業からの電子メールであれば，タイムゾーンが大きく変化することが考えられず，送信者が普段利用している送信元タイムゾーンと違う結果が出た場合には，送信者が海外へ移動している事実がなければなりすましによる第 3 者からの電子メールの可能性を考える必要がある．

7.3 考察

評価では，各項目ともいくつかの値に収束することが確認できた．本研究では，標的型攻撃の対策手法として利用したこれらの情報がいくつかの値に収束することを前提としている．そのため，いずれの情報も判定に有用であると言える．しかし，いずれの情報にしても単体で標的型攻撃の判断に利用することはできない．なりすましを行う際に，それらのデータを書き変えられてしまう可能性がある．

そこで，上記の 3 つの情報を組み合わせた上で判断を行うことが必要である．3 つを組み合わせて判定を行うことで，既存のツールでは対応できなかった攻撃を検知することが

表 7.1: 標的型攻撃への対応評価

対策の種類	初めて受信する電子メール	過去に受信したことのある電子メール	備考
ベイジアンフィルタ	×	×	通常の電子メールと同じものは判別できず
送信ドメイン認証	△	△	送信者および受信者の利用サーバがともに対応している必要がある
本研究で提案する手法	○	△	正規のユーザを誤検知する可能性がある

可能である．既存研究と本研究で提案した手法について，初めて受信するアドレスからの電子メールである場合と，以前受信したことのあるアドレスからの電子メールの二つの場合についてなりすまし判定の可否を評価した．評価の結果を表 7.1 に述べる．本研究の提案手法では，以前に受信したことのない電子メールでも過去に受信した電子メールでも対応することが出来ることがわかる．ベイジアンフィルタでは，どちらの場合でも判定することはできないし，送信ドメイン認証を利用した場合では，双方が利用するサーバがともに対策を導入している必要がある．一方で本研究で提案する手法では，初めて受信する電子メールはすべてに警告を発するため，本文で受信者の知人の名前が騙られる方式のなりすましであっても対応することができる．また，複数回受信した場合でも過去の情報と照合することで対応するため，攻撃の検知をすることが可能である．

しかし，本研究で提案している手法では，複数回受信した電子メールを評価する際に 3 つの項目のいずれかに変化が生じた場合に警告を発するため，急に電子メールクライアントを変えたり，普段利用しない場所から送信された場合など，正規のユーザからの送信を誤検知してしまう可能性がある．また，すべての情報が偽装され，正規のユーザと同じようなヘッダを利用された場合には対応することができない点を考慮する必要がある．

第8章　結論

本章では，本論文の目的を再確認し，本論文で行った対策手法についてまとめる．また，今後の展望として，本研究の今後について述べる．

8.1　まとめ

本論文の目的は，標的型攻撃を判別する手法を確立し，標的型攻撃による被害を防ぐことである．そのために，Thnderbird のアドオンとして対策ツールを実装した．

標的型攻撃は，電子メールを利用した攻撃としてSPAM メールのように認知度もなく，現状ではあまり一般的によく知られた攻撃とは言えない．また，攻撃自体が判別しづらく，被害が大きい．また，既存のセキュリティ対策ソフトでは標的型攻撃に対応することはできない．そこで，本研究において，電子メールを受信した際にそれが標的型攻撃である可能性を判定することで，ユーザが必要な対策を取れるようにする手法を提案した．提案手法は，クライアントで動作する手法とし，受信した電子メールからヘッダ情報を取得し，受信の都度その情報を蓄積していくことで過去の情報との照合を可能にした．ユーザが電子メールを送信する環境に傾向があるとの仮定のもと，普段と異なる環境から送信された電子メールを判別することで，本来意図した相手ではない相手からのメール，なりすましによるメールの判別を可能にした．

本研究では，標的型攻撃に利用している情報が判断に有用な情報であるかを評価するために，筆者が受信した電子メールを利用して 4 項目のデータを調査した．調査の結果，送信元 IP アドレスは送信者の所属するネットワークによっては広く分散してしまうことが判明した．そこで，ドメイン情報を利用し，IP アドレスを分類することで IP アドレスをユーザが送信する環境ごとにわけ，判定に利用した．判定に利用するにあたり，ドメイン情報がなりすましによる標的型攻撃の判別に利用することができるか評価を行うため，ユーザがどのような環境から電子メールを送る傾向にあるのか調査した．この傾向を利用することで，電子メールが普段ユーザが利用しない環境から送信されたことを識別できることが判明した．電子メールクライアントは，ユーザごとに特徴が見られ一人のユーザが利用する電子メールクライアントは基本的に変化しないことがわかった．なお，タイムゾーンは，ユーザが同じ地域にいる限りは変化せず，出張や旅行などにより普段と違う地域に移動した時に変化が生じることがわかった．これらの情報を利用した本研究で提案する手法は，既存の迷惑メールを防止する手段とは違い，標的型攻撃を判別することが可能であると判断した．

本研究で提案した手法により，ユーザが普段目にすることのできない情報であるヘッダ

情報による対策が可能となり，標的型攻撃の検知に役立つものになった．なお，認知度向上の観点から，本論文の第 2 章において標的型攻撃の概要を説明し，その後の第 3 章において，その対策の難しさを述べた．

8.2 今後の展望

本論文で提案した手法では，過去に情報を蓄積したアドレスからの電子メールであっても，普段利用しない環境から送信された場合などに誤検知する場合がある．また，対策を導入したユーザが過去に受信した電子メールのみから情報を取得するため，蓄積できる情報が限られてしまい，友人や知人ではなく，企業からくる電子メールなど頻繁に来ることが少ないアドレスからの標的型攻撃を判別することは難しい．それ以外にも，すべての情報を偽装された場合には検知できないという欠点もある．

そこで，電子メールヘッダ情報を収集，比較することで，より正確な判定手法を構築する．また，企業や行政からの電子メールヘッダ情報をサーバに蓄積することで複数のユーザで情報共有を行い，他のユーザが受信しているアドレスの蓄積情報を用いて判定することで精度を挙げることができる．また，ユーザを属性ごとに分類し,「学生」や「教員」,「会社員」などのグループ毎に傾向をまとめることで，蓄積している情報が少ない場合でも分類されたグループの傾向から判別することで精度を上げることが可能となるなど，受信した電子メールの数が少ない場合にも対応することが出来るように改良することも可能である．偽装への対策としては，ヘッダ情報の中で偽装することのできない情報で変化が少ない項目を再調査し，判定に組み入れることが挙げられる．いずれの対策においても，今後情報の取得範囲を拡大し，サンプルデータを増やすことで，より精度の高い検知につなげることが期待できる．

本研究では，標的型攻撃の中でもなりすましメールへの対策に主眼をおいた．電子メールを利用した攻撃は幅広く多様な攻撃が想定される．本研究を元に，電子メールを利用した企業，行政，そして個人に対する攻撃を防ぐことができるよう機能拡張を行う必要がある．

謝辞

本論文の作成にあたり，ご指導頂いた慶應義塾大学環境情報学部学部長 村井 純博士，同学部教授 徳田 英幸博士，同学部教授 中村 修博士，同学部准教授 楠本 博之博士，同学部准教授 高汐 一紀博士，同学部准教授 三次 仁博士，同学部准教授 植原 啓介博士，同学部専任講師 重近 範行博士，同学部専任講師 中澤 仁博士，同学部専任講師 Rodney D.Van Meter III 博士，同学部教授 武田 圭史博士に感謝致します．特に武田圭史博士は，セキュリティに限らない幅広い知識を教えていただき，研究の道筋やその手法を決めるに当たっても多くの助言をいただきました．

そして，研究室に入り，ネットワークやそのセキュリティの知識が全くない私が，研究を始め，現在の研究内容を決めるまでに特に助言を頂いた慶應義塾大学大学院 SFC 研究所上席所員 (訪問) 水谷 正慶博士に感謝いたします．標的型攻撃にテーマを絞り，研究を現在のようにすることができたことは氏の指導のおかげだったと思います．

政策メディア研究科修士課程 上原雄貴氏は卒論執筆の期間，特に相談に乗っていただきました．時に厳しく時に優しく指導をしていただきました．学会に共に行くなど，研究室生活において深く関わり卒論執筆を行う上で非常にお世話になりました．本当にありがとうございました．

また，福岡 英哲氏や Doan Viet Tung 氏といった共に卒論を書いた仲間をはじめ，藤原 龍氏，碓井 利宣氏，山本 知典氏を始めとした ISC のメンバー全員に感謝いたします．デルタ棟に訪れる機会も少ない私ながら，2 年間の研究室生活を有意義なものとして過ごすことができたのは，ISC の各メンバーのおかげであったと思っています．

卒論の文章構成を行ってくれた根本祐滋氏に感謝いたします．高校時代から非常にお世話になっている氏は今回の卒論執筆にあたっても私を助けてくれました．

最後に，研究室や大学で過ごした 4 年間，私を支えてくれた母と私の家族に感謝いたします．

参考文献

[1] Mozilla Japan. 無料メールソフト thunderbird. http://mozilla.jp/thunderbird/, 12 2010.

[2] JPCERT コーディネーションセンター. 「標的型攻撃について」. http://www.jpcert.or.jp/research/2007/targeted_attack.pdf, 6 2007.

[3] Microsoft Corporation. Microsoft office. http://office.microsoft.com/ja-jp/, 12 2010.

[4] Adobe Systems Incorporated. Pdf ファイル. http://www.adobe.com/jp/products/acrobat/adobepdf.html, 12 2010.

[5] エフセキュア株式会社. Google に対する標的型攻撃. http://blog.f-secure.jp/archives/50334905.html, 1 2010.

[6] エフセキュア株式会社. 米軍事契約企業に対する標的型攻撃が継続中. http://blog.f-secure.jp/archives/50338053.html, 1 2010.

[7] エフセキュア株式会社.「operation aurora」をエサにした標的型攻撃. http://blog.f-secure.jp/archives/50339288.html, 1 2010.

[8] エフセキュア株式会社. 標的型攻撃に狙われた情報産業. http://blog.f-secure.jp/archives/50339286.html, 1 2010.

[9] Google. Gmail: Google メール. http://mail.google.com/mail/, 12 2010.

[10] POPFile Documentation Project. Popfile - automatic email classification. http://getpopfile.org/docs/jp, 12 2010.

[11] JPCERT コーディネーションセンター. 標的型攻撃対策手法に関する調査報告書. http://www.jpcert.or.jp/research/2008/inoculation_200808.pdf, 8 2008.

[12] 独立行政法人 情報処理推進機構. 脆弱性を利用した新たなる脅威の監視・分析による調査. http://www.ipa.go.jp/security/vuln/report/documents/newthreat_report_2009.pdf, 7 2009.

[13] 独立行政法人 情報処理推進機構. 脆弱性を狙った脅威の分析と対策について vol .3. http://www.ipa.go.jp/security/vuln/report/documents/newthreat201006.pdf, 6 2010.

[14] 独立行政法人 情報処理推進機構. 情報セキュリティ安心相談窓口. http://www.ipa.go.jp/security/vuln/report/documents/newthreat201006.pdf, 6 2010.

[15] 山口 健太郎, 小宮山 功一朗, and 内田 勝也. ユーザへの予防接種というアプローチによる標的型攻撃対策-2. **情報処理学会第 *71* 回全国大会**, 2009.

[16] 猪俣 敦夫, ラーマン ミザヌール, 岡本 健, and 岡本 栄司. フィッシングメール防御のためのメールフィルタリング手法の提案. *Symposium on Cryptography and Information Security*, 2005.

[17] 春名光一. Id-based 暗号を用いたメール送信元サーバ認証に関する研究. Master's thesis, 筑波大学大学院システム情報工学研究科, 2006.

[18] 光田智史. メールヘッダへの id 挿入による電子メールの高機能化に関する研究. Master's thesis, 東京大学大学院新領域創成科学研究科, 2005.

[19] NTT DOCOMO INC. 送信ドメイン認証（sender id／spf）について. http://www.nttdocomo.co.jp/service/communication/imode_mail/notice/sender_id/, 1 2011.

[20] KDDI CORPORATION. 送信ドメイン認証 spf レコードについて ezweb へメール送信する際の注意事項 au by kddi. http://www.au.kddi.com/service/email/support/chui/spf_record.html, 1 2011.

[21] SOFTBANK MOBILE Corp. メール 送信のご注意. http://creation.mb.softbank.jp/mail/mail_attention.html, 1 2011.

[22] WILLCOM INC. 送信ドメイン認証サービスの開始について. http://www.willcom-inc.com/ja/corporate/press/2006/03/14/index.html, 1 2011.

[23] EMOBILE Ltd. メール設定〔携帯電話〕 イー・モバイル. http://emobile.jp/service/mailsettei.html, 1 2011.

[24] トランスコスモス株式会社. E メールマーケティングをトータルに支援するメールサービス—clickm@iler. http://www.clickmailer.jp/, 1 2011.

[25] YMIRLINK.Inc. メール配信システムなら cuenote シリーズ. http://www.cuenote.jp/, 1 2011.

[26] Apple Inc. アップル - iphone - 携帯電話、ipod、インターネットデバイスがひとつに。http://www.apple.com/jp/iphone/, 1 2011.

[27] Google. Android.com. http://www.android.com/, 1 2011.