送信ドメイン認証技術を用いた送信者レピュテーションの構築手法とフィードバックループを備えたメールシステムに関する研究

櫻庭 秀次

電気通信大学 大学院情報システム学研究科
博士（工学）の学位申請論文

2023年3月

送信ドメイン認証技術を用いた送信者レピュテーションの構築手法とフィードバックループを備えたメールシステムに関する研究

博士論文審査委員会

主査　大須賀 昭彦　教授

委員　田中 健次　教授

委員　南 泰浩　教授

委員　大坐畠 智　准教授

委員　清 雄一　准教授

Research on Sender Reputation Construction Method Using Sender Authentication Technologies and Mail System with Feedback Loop

Shuji Sakuraba

Abstruct

The mail system on the Internet has become an important means of communication, and is used as part of various systems and as a means of data transmission. On the other hand, unsolicited emails (spam) are also a means of inflicting security damage, such as being an intrusion route for malicious software and spoofed emails leading to fake web sites. Against this background, various techniques for spam countermeasures have been studied. Under these circumstances, as a method to prevent spoofing emails, a standard for sender authentication technologies were created to authenticate the domain name of the sender information. If it is possible to determine the receipt of emails using this authenticated domain name, it is expected that spam countermeasures will be implemented more efficiently. For example, it can be used to determine which emails should be received based on the sender information, and to determine whether or not to receive other emails by examining them in more detail with an email filter based on the content of the email. Sender reputation is the information that serves as a criterion for judging such mail reception. However, the criteria for judging which emails should be received and the means of collecting information such as what kind of information is used to build a sender's reputation are not clear. There are challenges in building a sender reputation. Therefore, although the sender authentication technologies are spreading, it is difficult to say that the sender reputation is being utilized.

In this paper, we describe a method to collect information of senders who should receive emails and build sender reputations. Regarding the sender information of the mail to be received, we focus on the forwarded mail and collect the legitimate mail domain name to be received by using the sender. Use the results of sender authentication to determine forwarding mail. Only include domain names that have been authenticated by sender authentication so that sender reputation does not include spoofed domain names. To build

a sender reputation, we need information on the IP address of the sender of the received email, the result of sender authentication, and the domain name. These information are generally included in the record information of received mail (mail-log) , and we propose to use this information. Since there are differences in the transmission method of forwarded mail depending on the forwarding source, we propose a determination method corresponding to each forwarding method. We applied this proposed method to about 340 million reception logs received by an actual mail service, and built a sender reputation of the sender that should be received. This sender reputation was applied to actual reception logs, and the constructed sender reputation was evaluated. As a result, the proposed method was able to obtain sufficiently effective results, and it was possible to show that the proposed method of constructing sender reputation is effective. In addition, as a result of applying the constructed sender reputation, it was found that spam emails were also sent from legitimate email senders. There is a high possibility that this is an unsolicited mail sending method that uses a legitimate mail server as a stepping stone, and it is thought that the authentication information of legitimate mail users is abused. In such a situation, there is a possibility that the authentication information is abused for purposes other than sending spam, and this is an issue that should be addressed on the sender side. We proposed the use of a feedback loop as a mechanism for correcting the use of this compromised account.

Based on these research results, we were able to demonstrate a method of constructing a sender reputation using the sender authentication technologies by using the recorded information of received emails. This method can be constructed without the need for checking the content of highly confidential emails or new mechanisms for collecting reputation information, because the organization's received email record information can be used. Furthermore, in order to effectively utilize this sender reputation, we proposed a feedback loop method using sender authentication technologies. By promoting the introduction of these methods, it is expected that the email usage environment will become more sound.

送信ドメイン認証技術を用いた送信者レピュテーションの構築手法とフィードバックループを備えたメールシステムに関する研究

櫻庭 秀次

概要

インターネットにおけるメールシステムは重要なコミュニケーション手段となっており，様々なシステムの一部として，またデータ伝達の手段などにも利用されている．その一方で迷惑メールが不正なプログラムの進入経路となったり，なりすましメールによって偽のサイトへ誘導されるなど，セキュリティ的な被害をもたらす手段にも悪用されている．こうした背景から，迷惑メール対策に関する様々な手法が研究されてきた．この中で，なりすましメールを防ぐ手法として，送信者情報のドメイン名を認証する送信ドメイン認証技術の規格がつくられた．この認証されたドメイン名を用いて，メールの受け取りを判断することができれば，迷惑メール対策をより効率良く実施することが期待できる．例えば受け取るべきメールを送信者情報で判断し，それ以外をメール内容などに基づくメールフィルタでより詳細に検査して受け取りを判断する，といった使い方である．こうしたメール受け取りの判断基準となる情報が送信者レピュテーションである．しかしながら受け取るべきメールをどのように判断するかといった基準や，どのような情報を利用して送信者レピュテーションを構築するかといった情報収集の手段は明確ではなく，送信者レピュテーションの構築には課題がある．そのため送信ドメイン認証技術は普及しつつあるものの，送信者レピュテーションが活用されているとは言い難い状態となっている．

本論文では，受け取るべきメール送信者の情報を集めて送信者レピュテーションを構築する手法について述べている．受け取るべきメールの送信者情報については，転送メールに着目し，その送信元を利用して受け取るべき正規のメールドメイン名を収集する．転送メールを判断するために送信ドメイン認証の結果を用いる．送信者レピュテーションに詐称されたドメイン名が含まないように，送信ドメイン認証で認証されたドメイン名だけを対象とする．送信者レピュテーションの構築には，受信したメールの送信元 IP アドレスと，送信ドメイン認証の結果とそのドメイン名の情報を必要とする．これらの情報は，一般的に受信メールの記録情報（ログ）に含まれており，この情報を利用すること提案する．転

送メールの送信方法にも転送元によって違いがあるため，それぞれの転送方法に対応する判定手法を提案している．この提案手法を，実際のメールサービスで受信した約 3 億 4 千万件の受信ログに適用し，受け取るべき送信元の送信者レピュテーションを構築した．この送信者レピュテーションをさらに実際の受信ログを用いて適用させ，構築した送信者レピュテーションの評価を行った．その結果，提案手法が十分に有効な結果が得られ，提案した送信者レピュテーションの構築手法が有効であることを示すことができた．また，構築した送信者レピュテーションを適用した結果，正規のメール送信元からも迷惑メールが送信されていることがわかった．これは，正規のメールサーバを踏み台のように利用する迷惑メール送信手法である可能性が高く，正規メールユーザの認証情報が悪用されていると考えられる．こうした状況は，迷惑メール送信以外にも認証情報が悪用されている可能性があり，送信側で対策すべき課題である．この踏み台利用を是正するための仕組みとしてフィードバックループの利用が提案されている．しかしながら，フィードバックされる情報の信頼性に関する課題もあり，送信側の踏み台送信対策としてはこれまであまり利用されてこなかった．このフィードバックループの信頼性を高めて踏み台送信の対策に利用するために，送信ドメイン認証技術を利用するフィードバックループのフレームワークを提案した．

これらの研究成果により，受信メールの記録情報を利用して，送信ドメイン認証技術を用いた送信者レピュテーションの構築手法を示すことができた．この手法は，自組織の受信メール記録情報が利用できることで，機密性の高いメールの内容を確認したり，レピュテーション情報収集のための新たな仕組みなどを必要とせず構築することができる．さらにこの送信者レピュテーションを効果的に活用するために，送信ドメイン認証技術を用いたフィードバックループの手法を提案した．これらの手法の導入が進むことによって，メール利用環境がより健全化していくことが期待できる．

目 次

図 目 次

表 目 次

第1章　序論

本章では，本研究の背景を述べたあと，本論文の目的と意義を説明する．その後，本論文の構成について述べる．

1.1　本研究の背景

電子メールは，インターネット上のコミュニケーション手段として広く利用されている．その一方で，広告宣伝を目的とした内容や不正なプログラム（ウイルスやマルウェア）が添付された，メール受信者が望まない迷惑メールが増え，大きな社会問題となっている．さらに，直接的な金銭搾取を目的とした迷惑メールも増加している．例えば，実在する企業をなりすましたメールを送信し，そのメールに記載されたURL[1]先のサイトにアクセスさせることで，実在するサイトの偽サイトに誘導し，ログインするための認証情報やクレジットカード番号などの情報を摂取する，フィッシングが増加しており被害も増えている[2]．さらに，不正プログラム（マルウェア）を添付ファイルとして送信したり，ウェブサイトからダウンロードさせるように誘導し感染させる行為が行われている．これらのマルウェアに感染させられたPCは，外部と通信を行うことでロボットのように操作されることからボットと呼ばれている．これらのボットは，さらに迷惑メールを送信することでより多くの感染PCを増やしてボットネットを形成し，DDoS[3]攻撃などにも利用される．さらにマルウェアの中には，PC内部からアクセスできるファイルを暗号化して身代金を要求するランサムウェアがあり，被害も増加している[4]．ランサムウェアによる被害は，ファイル復号化の鍵を得るための身代金だけに限らず，ファイルが復号化できない場合に業務継続が困難となったり，ファイルを外部に暴露するといった脅迫行為や情報を転売される場合もある．こうした被害が，迷惑メールを起点に発生しており，迷惑メール対策は引き続き重要な課題の1つとなっている．

---

[1] Uniform Resource Locator
[2] https://www.antiphishing.jp/report/monthly/
[3] Distributed Denial of Service
[4] https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf

迷惑メールを受け取らないための対策には，メール受信時に迷惑メールかどうかを判断し，迷惑メールの場合にはメール受信者に直接届けない，といった手法が用いられる．受信したメールが，迷惑メールであるかどうかを判断する手法としては，メールの送信者を判断する手法と，メールの内容が迷惑メールであるかを判断する手法がある．

メールの送信者を判断する手法は，受信メールサーバへの接続元をネットワーク的に示すIPアドレスがこれまで利用されてきた．例えば，迷惑メールの送信元や，どこからでもメールを受け取って送信できるオープンリレー設定されているメールサーバのIPアドレスを集め，ブロックリストとして利用する手法である．しかしながらIPアドレスは，メールサーバ変更時に付け変わったり，IPv4アドレスが枯渇していることからIPアドレスが移転され，管理元や用途が変わる場合がある．またクラウド型のメールサービスなど，複数の利用顧客を同時に扱うメールサーバもあり，メールの利用形態も多様化しており，送信元のIPアドレスが特定の送信者を恒久的に示す情報とは必ずしもいえなくなっている．そのため，メールの送信者を判断するための情報として，IPアドレスを利用することが適切でない場合も増えている．メールでは，送信者を示す情報としてメールアドレスを提示しなければならない．しかしこのメールアドレスが，本当に実際の送信者であるかどうかを検証する仕組みが無かったことから，信頼できる送信者情報としてこれまで利用されてこなかった．これが送信ドメイン認証技術により，メールの送信者をドメイン名単位で認証できるようになった．また，フィッシングなどのなりすましメール対策として普及も進んでいる．この認証されたドメイン名を，メールの受け取り判断に利用することが期待されている．この受け取り判断のための情報が，送信者レピュテーションである．

メール内容を判断する手法は，迷惑メールの目的が広告宣伝である場合には，伝えたい対象やそれを広告する特徴的な内容があり，キーワードや単語，それらの出現頻度や関連といった統計的な情報からある程度判断することができた．しかしフィッシングなどの詐欺的な行為を目的とした迷惑メールは，なりすまそうとする実在する対象を模倣することから，メール内容だけから判断することが非常に困難になってきている．そのため，メール内容に示された誘導先のURLの情報やその特徴，メールヘッダやメールの送信元などを利用し，総合的な判断を行うことが一般的となっている．

このように，受信側での迷惑メール対策は，特定の技術だけで対応できるわけではなく，複数の技術を組み合わせて総合的に行う必要がある．しかしながら，一般的な受信側の迷惑メール対策では，受け取ったメールが迷惑メールであるかをメール内容から判断する手法が主流となっている．メール内容によるは判断では，誤判定の問題がどうしても避けられないため，受け取るべき正規のメールが迷惑メールと誤判定され，必要なメールが受け

取れなくなる可能性がある．こうした問題をなるべく発生させないために，判定が曖昧な受信メールに対する強い判定処理等ができず，迷惑メールの見逃しなども発生する要因にもなっている．こうした課題に対しては，送信者情報を利用した送信者レピュテーションを適用させることで，受け取るべき送信元からのメールを確実に受け取れるようにすることで，こうした誤判定や見逃しの問題を軽減させることが期待できる．これをメール内容による判断の前段で行うことにより，メール内容による誤判定の問題や，判断のための処理負荷の軽減などが期待できると考える．そのためには，信頼性の高い送信者レピュテーション，特に受け取るべき送信元の情報を集めるための手法が必要である．

1.2 本研究の目的と意義

本研究では前述の背景を受けて，迷惑メール対策として，メールの送信者情報から受け取るべきかどうかの判断に利用する，送信者レピュテーションの構築手法を提案することを目的とする．送信者情報としては，送信ドメイン認証技術によって認証されたドメイン名を主に利用する．この送信者レピュテーションを構築するためには，(1) 受け取るべきメールの判断基準とその識別手法，(2) 送信者レピュテーション構築のために重要なメール情報の収集方法が明確である必要がある．

現在のメールサービスの多くは，受け取るべきかどうかの判断として，主にメール内容から迷惑メールかどうかを判定するメールフィルタを利用する．これらのメールフィルタは，迷惑メールを集めそれらの特徴から迷惑メールであるかを判定している（図 1.1）．

迷惑メールや添付されるマルウェアが巧妙化するに従い，これらを判定するための処理も高度化する必要があり，その処理負荷も高まっている．メールの送信者を示す情報は，IP アドレスや送信ドメイン認証によって認証されたドメイン名であり，それらの情報を取得するための処理は，メール内容を元にしたメールフィルタよりは格段に軽い処理で得ることができる．送信者レピュテーションが予め構築できていれば，取得した送信者情報が含まれているかを判断するだけであり，メール内容からの判断処理と比較すればその処理負荷も同様に高いものではない．また受け取るべきメールの送信元がわかれば，それらの受信メールをメールフィルタを経由せず，直接メール受信者に届けることができる（図 1.2）．このようなメールフィルタの構成により，明らかに受け取るべきメールに対する不要なメール内容による検査を省くことができ，メールフィルタ全体の処理負荷を軽減することが期待できる．メールフィルタの処理を軽減させることで，より高度な負荷の高い処理を同じ計算機資源で実現することも可能となる．これにより，メール受信者に届けるべきメール

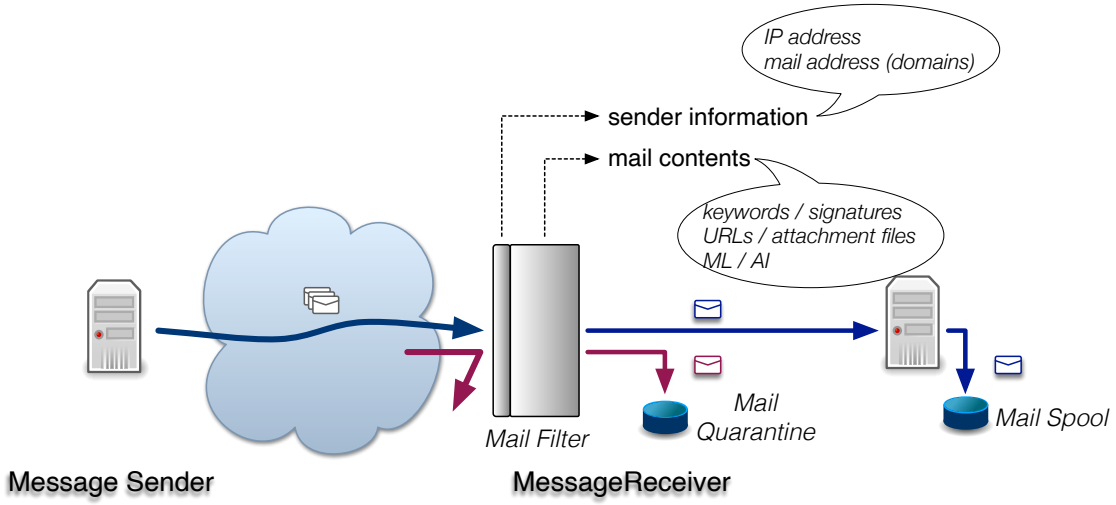

図 1.1: メール受信側の迷惑メール対策

を確実に届け，不要な迷惑メールの判断処理により計算機資源を割り当てることで，不要なメールを届けない，といったメール環境を実現することができる．

送信者レピュテーション構築のためには，受け取るべきメールの送信者情報（ドメイン名）を集める必要がある．一般に，迷惑メールの送信元に関する情報は，迷惑メールを集めることでその送信元を抽出し，ブロックリストとして構築する．迷惑メールは不要なメールであるため，メール受信側としても提供しやすい．特にブロックリスト利用者にとっては，迷惑メールを提供することで届かなくなるのであれば，積極的に提供する理由にもなる．しかしながら，受け取るべきメールについては，必要なメールであり場合によっては個人情報やビジネス上の情報を含む場合があり，提供が難しいという側面がある．メールの送信元の IP アドレスや認証ドメイン名だけの提供についても，メール受信者がそれと簡単に判断できるような形式とはなっておらず，仮に提供されたとしても，それが正しく受け取るべき送信者であるかを，メール本文無しにどのように判断すべきかも難しい．

受け取るべきメールは，受け取っているメールの中に含まれており，それらは例えばメールシステムの管理者などが参照できるメールの受信記録情報（ログ）に記録されているはずである．これらのログ情報から受け取るべきメールの送信元情報を抽出できれば，他の送信者レピュテーションの提供組織に依存することなく，自らのメールシステムに適した送信者レピュテーションを構築することができる．メールの受信ログには，メールの送信元 IP アドレスや，送信ドメイン認証を実施していれば，その認証結果や認証ドメイン名

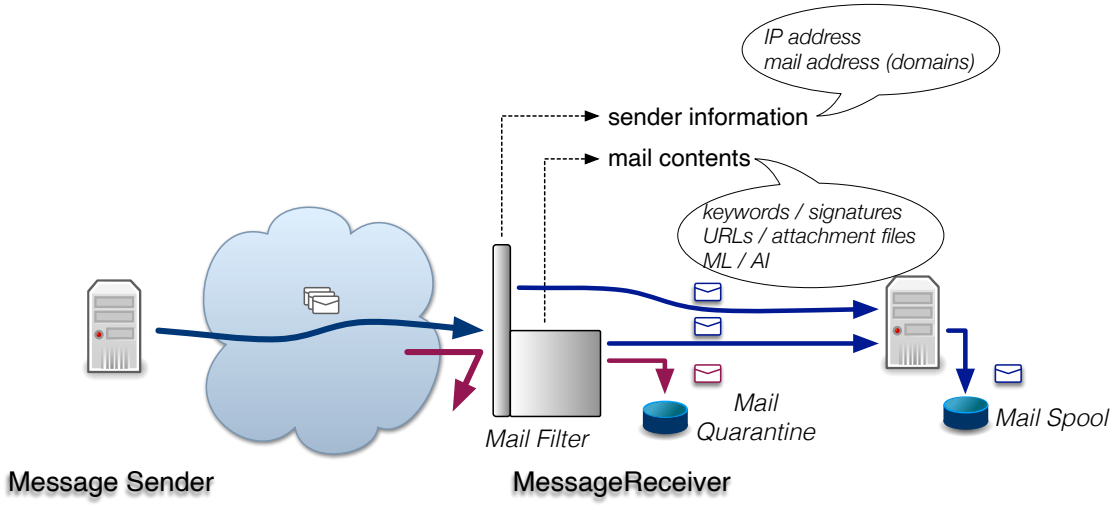

図 1.2: 送信者情報を利用したメール受信側の迷惑メール対策

などが一般的に記録されている．メールの受信ログは，メール受信毎に逐次更新されいくため，これを自動的に分析し送信者情報を抽出することができれば，新しいメール送信元にも対応していくことができる．そこで，自組織で運用しているメールシステムやメールサービスの受信記録情報（ログ）を利用して，送信者レピュテーションを構築する新しい手法を開発した．

まず，利用する送信者情報としては，詐称されない信頼性が高い情報である必要があるため，送信ドメイン認証技術によって認証されたドメイン名を利用する．送信ドメイン認証技術には，その手法の違いによって複数の技術があるが，そのうち最も普及率が高い SPF（Sender Policy Framework）を利用した．これは，ドメイン名単位でメールの送信元を区別できれば良いため，SPF 以外の送信ドメイン認証技術であっても利用できる手法と考えている．次に，送信ドメイン認証の結果を利用して受け取るべきメールの送信ドメイン名を抽出する．この手法については，第 3 章で述べる．これら送信ドメイン認証の結果や認証したドメイン名は，いずれも受信時のメールログに記載されている情報である．抽出した受け取るべきメールのドメイン名を集め，これを送信者レピュテーションとして構築する．これを実際のメールシステムで受信したログを利用して構築する．この手法で抽出した送信者レピュテーションを評価するために，受信メールに適用する．構築した送信者レピュテーションを利用し，受け取るべきメールを多く抽出し，受け取るべきではない迷惑メールの抽出が少なければ，受け取るべき送信者レピュテーションの品質が高く，本論文

で提案する送信者レピュテーションの構築手法が優れている，といえる．

送信者レピュテーションの評価基準は難しいが，受け取るべきメールを多く抽出できれば，その分負荷の高いメール内容によるフィルタに適用させるメールを減らすことができ，メール受信側の全体の処理負荷の低減につながることになる．迷惑メールを受け取るべきメールと判断してしまう場合は，通常のメールフィルタでのいわゆるすり抜け（False Negative）と同様の結果であり，実際の商用のメールフィルタでも発生していることであるが，当然ながらできる限り少ないことが望ましい．

受信したメールのログを利用して，送信者レピュテーションを構築し，構築した送信者レピュテーションを受信メールに適用する，受信側のメールシステムの概要を図 1.3 に示す．

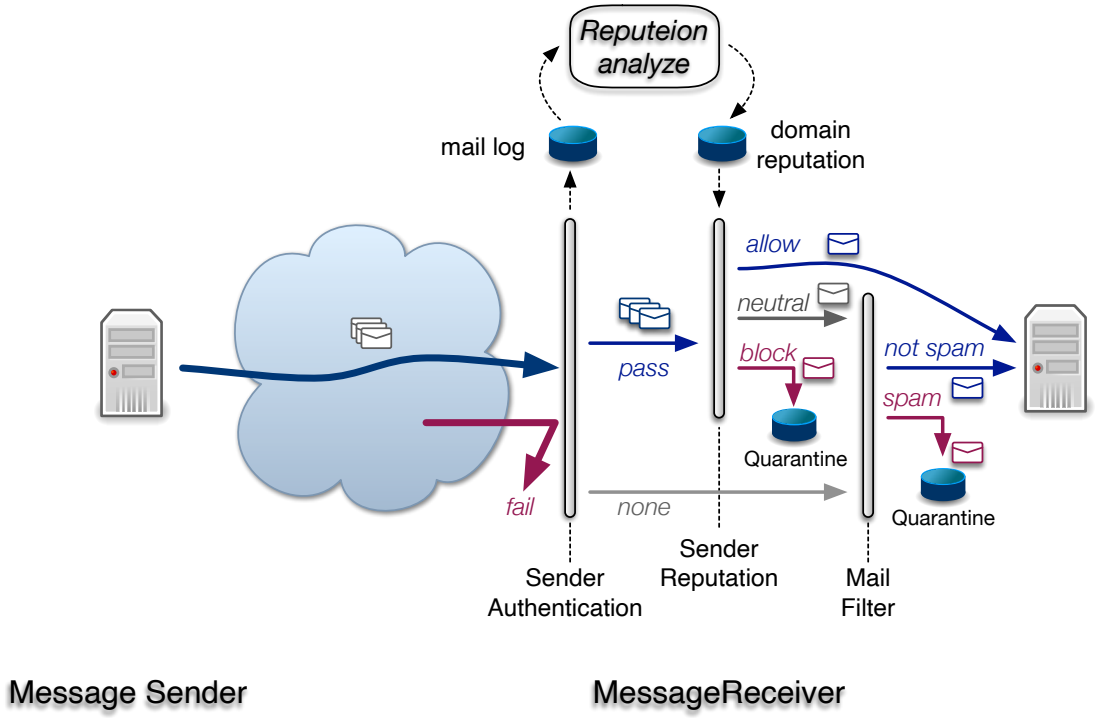

図 1.3: 送信者レピュテーションを構築し利用する受信メールシステム

受け取るべき正規のメール送信元を送信者レピュテーションとして構築できた場合でも，その送信元から迷惑メールが送信されてしまう可能性もある．例えば，メール送信時の認証情報として簡単に類推できるような脆弱なパスワードを設定していた場合や，メール利用者の PC がマルウェアに感染したことでこれら認証情報が摂取されていた場合，またマルウェア感染により外部から迷惑メール送信の指令を受けて送信する場合などである．こ

うした正規のメールサーバを踏み台利用するような迷惑メール送信に対する対策も重要であり，これはメール受信者だけの問題ではなく，メールサーバが悪用されている送信側でも対策すべき重要な課題である．こうした迷惑メール送信手法を対策しなければ，送信者レピュテーション自体の信頼性も損なわれることになる．

したがって，本研究の意義は次の通りである．

1. 送信ドメイン認証技術を利用して，認証した送信者のドメイン名からメールを受け取るための判断手法の提案

2. 送信者レピュテーションについて，メール受信ログに記録されるような情報を利用して自動的に収集し構築できるような手法の提案

3. 送信メールサーバの踏み台利用に対する対策の提案

特に，本研究における最も重要な主張点は，送信ドメイン認証の結果を利用して受け取るべきメール送信元を判断する手法の提案である．

本論文では，以降第 2 章で要素技術および関連研究について説明し，第 3 章で送信ドメイン認証技術を用いた送信者レピュテーションの構築手法について述べる．第 4 章では，フィードバックループの仕組みについて説明し，信頼性を高めるために送信ドメイン認証技術を利用する手法について述べる．第 5 章では，送信者レピュテーションとフィードバックループを備えたメールシステムの全体構成について述べる．最後に第 6 章でまとめとする．

第2章　関連研究

本章では，本論文で構築する送信者レピュテーションとフィードバックループの基盤となる技術について説明する．いずれもメールの送信者を特定するための技術をそのための基盤技術として利用する送信ドメイン認証技術について述べる．またこれまでの迷惑メール対策の概要や，送信者レピュテーションに関連する研究として，ドメイン名の評価手法や，ブロックリスト構築のための情報収集方法についても説明する．

2.1　送信ドメイン認証技術の概要

本節では，送信ドメイン認証技術 [56] の概要について説明する．送信ドメイン認証技術は，メール送信者をドメイン名単位で認証する技術であり，その認証方法の違いにより複数の技術が提案され利用されている．いずれの認証技術も，メールの送信側が認証のための設定を行い，メールの受信側がそれら設定された情報を利用してメール受信時に認証処理を行う．それぞれの認証技術について仕組みや特徴について述べる．

各送信ドメイン認証技術の普及については，有名ドメイン名などに対して設定の方法やその内容，それぞれの設定割合の違いなどの調査が示されている [47]．メールサービスで受信しているメールについて，送信ドメイン認証の調査結果も示されている [53]．

2.1.1　送信ドメイン認証技術 SPF

送信ドメイン認証技術 SPF（Sender Policy Framework）[25] は，配送上の送信者情報であるメールアドレスのドメイン名部分を認証する．配送上の送信者情報は，メール受信者が一般的に参照する送信者であるメールヘッダで示された送信者（From ヘッダ）ではなく，メールの配送手続き（SMTP:Simple Mail Transfer Protocol）[26] の中でメールの送信側から示されるメールアドレス（RFC5321.From[1]）または接続時に示される識別子を認証す

[1]RFC5321.From は，SMTP の仕様規格 RFC5321 上の From で示されるメールアドレスであることからの表記，エンベロープ From と呼ぶ場合もある

る（図 2.1）．SMTP では，メール送信側から送られる MAIL コマンドの引数として示される．メール受信側での認証の手順は，この配送上の送信者情報のドメイン名から DNS[2] 上の SPF レコードを取得し，メール受信時の送信元 IP アドレスがこの SPF レコード含まれているかどうかで判断する．

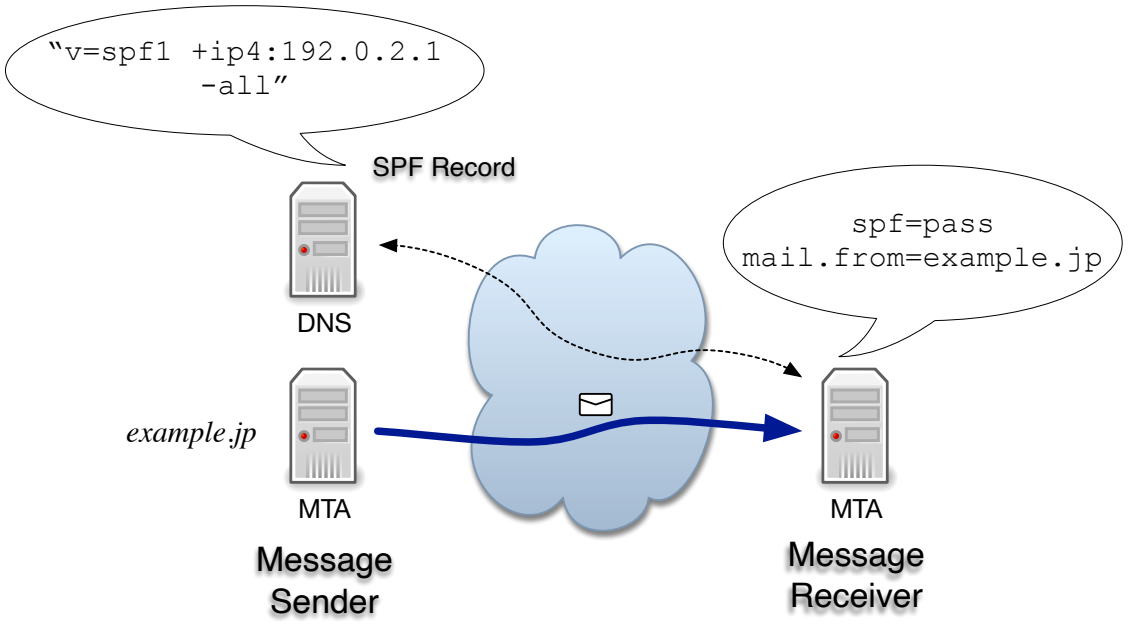

図 2.1: SPF 認証

メール送信側では，対象ドメイン名の DNS に SPF レコード（実際は TXT 資源レコード）にメールの送信出口を示す情報を設定する．つまり，送信側での SPF 導入については，既存の送信メールサーバ（MTA: Mail Transfer Agent）に対する機能追加や設定変更等が必要無いという利点がある．総務省の電気通信事業者らの統計データ [55] によれば，2022 年 3 月時点で 95.29%の受信メールで送信側が SPF に対応 しており，87.75%が SPF の認証を pass している．仕様が作られた時期が最も古いということもあるが，送信側の導入が簡単であることから最も普及が進んでいる送信ドメイン認証技術といえる．メール受信側では，メール受信時に SPF 認証のための追加機能が一般に受信メールサーバに対して必要となる．

SPF では，メールの送信元をネットワーク情報である IP アドレスを用いて認証を行うため，ネットワーク方式あるいはパス方式の送信ドメイン認証技術ともいわれる．ネットワー

[2]Domain Name System.

ク方式では，受信時の送信元メールサーバが最初のメール送信者と異なるような配送経路で届いてしまう場合，正しく認証できないという問題がある．具体的には，一旦届いたメールが設定により他のメールアドレスに自動的に転送された場合が該当する．メール転送によって届けられた転送先では，通常 SPF の認証ドメイン名である RFC5321.From が変更されずに届くが，転送先からみた転送元メールサーバの IP アドレスは，最初のメール送信者とは無関係であるため，RFC5321.From のドメイン名の SPF レコードに転送元メールサーバの IP アドレスが含まれていないことにより，SPF の認証が失敗する．図 2.2 に示した例では，

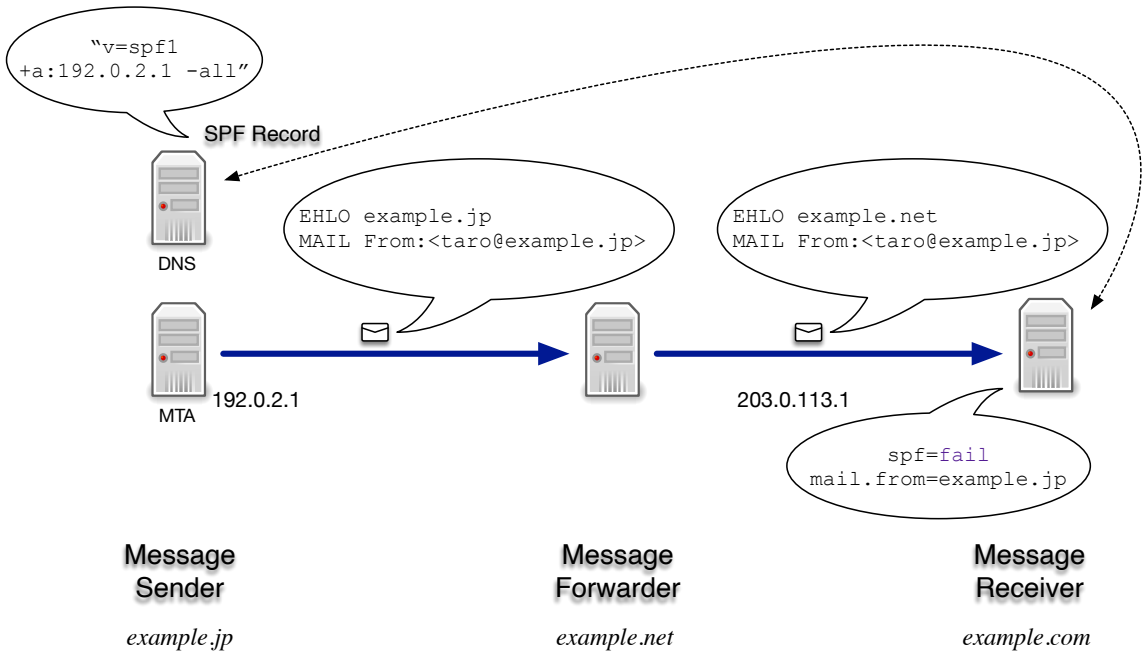

図 2.2: 転送メールの SPF 認証

example.jp から送信されたメールが宛先の example.net 宛に一旦届き，メール転送設定されているために example.com にメール転送されている．example.net では，メール転送の際に最初の送信者の RFC5321.From をそのまま引き継ぎ転送先の example.com に送信している．転送メールの受信元である example.com では，SPF の認証ドメインである example.jp に対して SPF レコードを取得するが，転送メール元の IP アドレス 203.0.113.1 が含まれていないため，SPF 認証は失敗する．

SPF 認証が，メール転送された場合に転送先で正しく認証できない問題は，SPF の仕様が作られた時点で既に明らかになっていた．そのため，SPF の仕様書 [25] にもメール転送時の RFC5321.From を書き換える手法が述べられており，これは改訂前の最初の仕様書

（RFC4408）でも示されていた手法である．さらに，業界団体の送信ドメイン認証技術の導入に関する提言書 [19] でも，メール転送時に転送先で SPF 認証が失敗する問題の対策として，転送時に RFC5321.From を書き換える手法が紹介されている．図 2.3 にメール転送時に RFC5321.From を書き換えるメール転送の例を示す．この例では，exampl.net が受け取ったメールを example.com に転送しているが，その際の SPF の認証ドメイン名である RFC5321.From は，転送元のドメイン名 example.net に書き換えている．そのため，転送先の example.com では，SPF 認証のための SPF レコードを example.net から取得し，受信時の IP アドレスが取得した SPF レコードに含まれているため，SPF 認証は pass する．

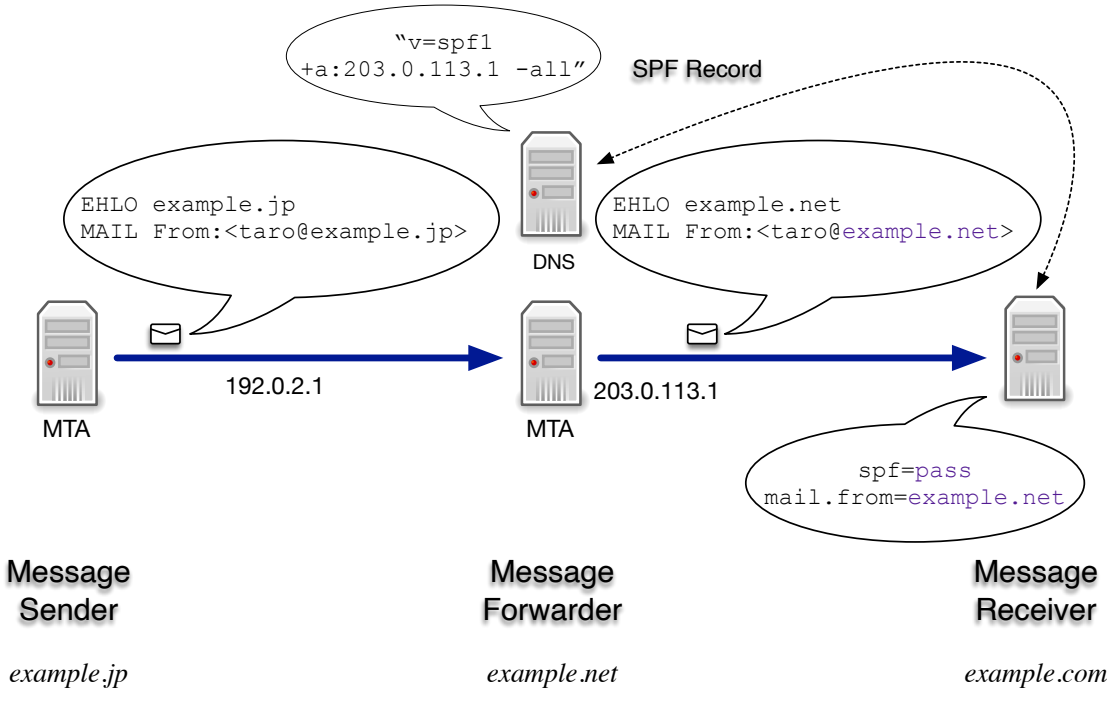

図 2.3: 送信ドメインを書き換える転送メールの SPF 認証

しかしながら SPF の認証結果を利用する送信ドメイン認証技術 DMARC（2.1.3 節）は，メール転送時に SPF の認証ドメイン名である RFC5321.From を書き換えてしまうと，DMARC の認証ドメイン名（ヘッダ From）と異なってしまうため，DMARC 認証には失敗してしまうという課題もある．

2.1.2 送信ドメイン認証技術 DKIM

送信ドメイン認証技術 DKIM（DomainKeys Identified Mail）[31] は，メール送信側がメール内容から電子署名を作成し，関連情報を含めてメールヘッダを追加し記載する．メール受信側は，メールヘッダに記載された電子署名の関連情報から，ドメイン名およびセレクタ名を抽出し，DKIM 鍵レコード（TXT 資源レコード）の場所（ドメイン名）を構築する．DKIM 鍵レコードを DNS から取得し，電子署名の検証に必要な公開鍵を取得し，受け取ったメールの内容から電子署名を検証する．電子署名が検証できれば，DKIM が認証されたことになる（図 2.4）．つまり DKIM は，電子署名の検証に必要な公開鍵を含む DKIM 鍵レコードが設定されているドメイン名（SDID[3]）を，その公開鍵と対になる秘密鍵で作成された電子署名が付加されたメールに対して認証する技術といえる．

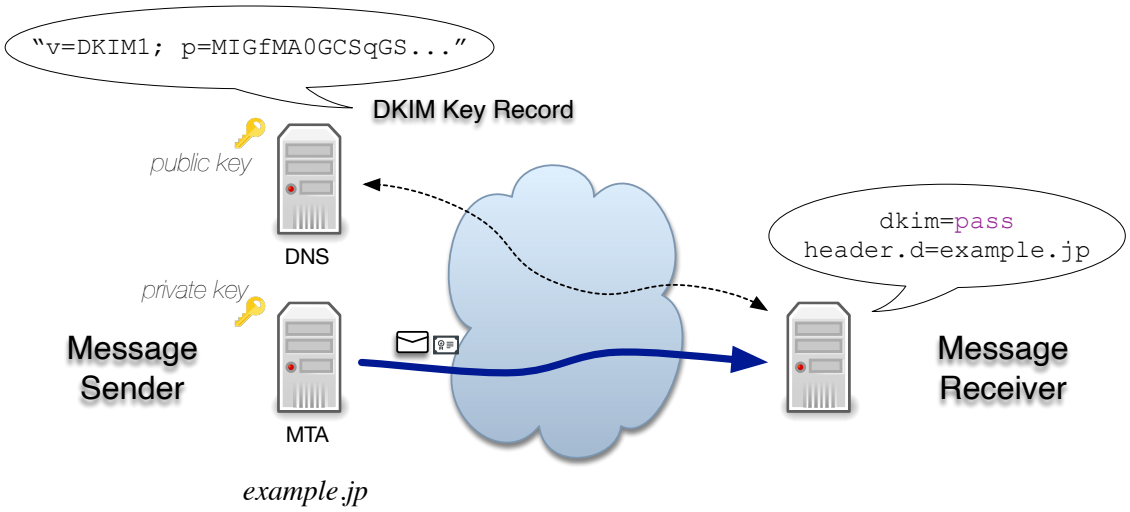

図 2.4: DKIM 認証

DKIM では，メールの配送経路によらない電子署名を利用して認証を行うため，転送されたメールであっても認証することができる．正しく DKIM の電子署名が付加されたメールが，認証できなくなるようなメールの利用形態としては，電子署名の作成時に対象としたメールヘッダや本文が変更されるような場合である．現在のメールの利用形態で，これら DKIM 認証ができなくなるメール内容が変更される事例には，メーリングリストがある．

メール送信側での DKIM 導入は，DNS への DKIM レコードの設定とともに，送信メー

[3]Signing Domain Identifier

ルサーバ上で電子署名の作成とメールへの追加処理が新たに必要となる．そのため SPF に比べて送信側の普及率は一般に低く，総務省の電気通信事業者らの統計データ [55] によれば，2022 年 3 月時点で 70.78%の受信メールで送信側が DKIM に対応しており，69.11%が DKIM の認証を pass している．メール受信側では，メール受信時に DKIM 認証のための機能追加が一般に必要となる．

2.1.3　送信ドメイン認証技術 DMARC

送信ドメイン認証技術 DMARC（Domain-based Message Authentication, Reporting and Conformance）[33] は，新たな認証の仕組みを導入するものではなく，SPF あるいは DKIM の認証結果を利用することで，それぞれの課題の緩和や導入効果をより得られるための仕組みである．DMARC で認証する送信者情報は，メール受信者が一般的に送信者と判断する，メールヘッダ上の送信者情報（RFC5322.From[4]）である．SPF あるいは DKIM で認証したドメイン名が，RFC5322.From のドメイン名と同じか，組織ドメイン名が同じ場合に，DMARC では認証が pass する（図 2.5）．

組織ドメイン名とは，TLDs（Top Level Domains）や，jp ドメイン名のように TLDs に属性ラベル（ac，co など）が付加された上位ドメイン配下の，通常登録可能なドメイン名のことである．つまり，example.co.jp ドメイン名を管理しており，そこに DMARC レコードを設定した場合，メールに利用しているドメイン名が mail.example.co.jp であり，このドメイン名には DMARC レコードを設定していなくても，example.co.jp ドメイン名の設定内容が mail.example.co.jp に対して設定したと同じ意味を持つ．つまり，DMARC では組織ドメイン名に設定した DMARC レコードの内容が，そのサブドメイン以下に対してデフォルト値のような効果が得られる仕組みとなっている．

さらに DMARC では，メールの受信側からドメイン管理側（メール送信者）に対して，受信したメールの認証結果をレポート送信する機能がある．このレポートを参照することで，メールの送信側が SPF や DKIM を含めて設定の不備や漏れ等がないかを確認することができる．

DMARC は認証の仕組みの基盤として SPF と DKIM を利用しており，それぞれの送信ドメイン認証技術の仕様がつくられたあと 2015 年に仕様が作られた．メールシステムにおける新しい技術や仕様は，既存の配送の仕組みが阻害されることの無いように，オプション的に作られる場合が多い．そのため，効果の高い新しい技術であっても，普及は急速に

[4]RFC5322.From は，電子メールのヘッダを含めた本文の構造を規定した仕様 RFC5322 上の From: ヘッダに示されるメールアドレスであることからの表記．

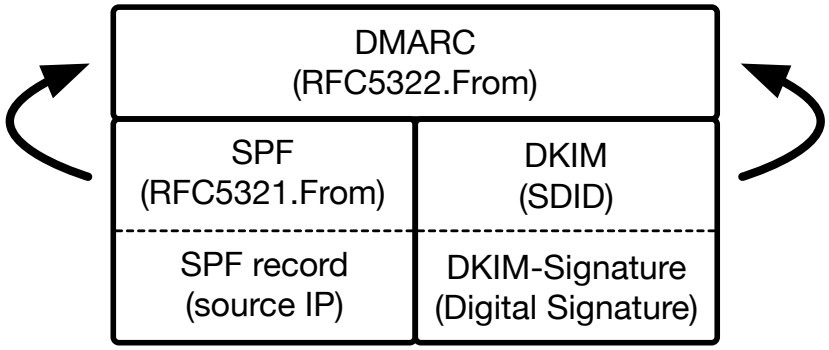

図 2.5: DMARC 認証の構造

は進まないという特徴がある．図 2.6 に国内のメールサービスでの受信メールの DMARC 認証の結果の推移を示す [54]．2016 年 1 月から 2020 年 4 月まで 1ヶ月間の DMARC 認証の結果の平均値の推移を示している．2020 年 4 月での DMARC 認証の結果では，none の割合が 75.4%あり，受信メールの 24.6%しか DMARC に対応していなかった．総務省の電気通信事業者らの統計データ [55] では，2022 年 3 月時点で 59.7%の受信メールが DMARC に対応していた．これら調査の対象となっているメールサービスはそれぞれ異なっており，単純に比較することはできないが，DMARC の普及は急速には進まないことがわかる．

2.1.4 送信ドメイン認証による認証結果

‘送信ドメイン認証技術，SPF, DKIM, DMARC のそれぞれの認証の仕組みや特徴，普及状況について述べた．表 2.1 に概要を示す．

表 2.1: 送信ドメイン認証技術の概要

送信ドメイン認証技術	認証ドメイン名	認証方法
SPF	RFC5321.From (envelope from)	送信元 IP アドレス
DKIM	署名ドメイン (SDID)	電子署名
DMARC	RFC5322.From (ヘッダ From)	SPF and/or DKIM

送信ドメイン認証では，認証した結果をメールヘッダに示すことになっている．この結果を示すメールヘッダは，`Autehntication-Results:` ヘッダとして形式が規格として決め

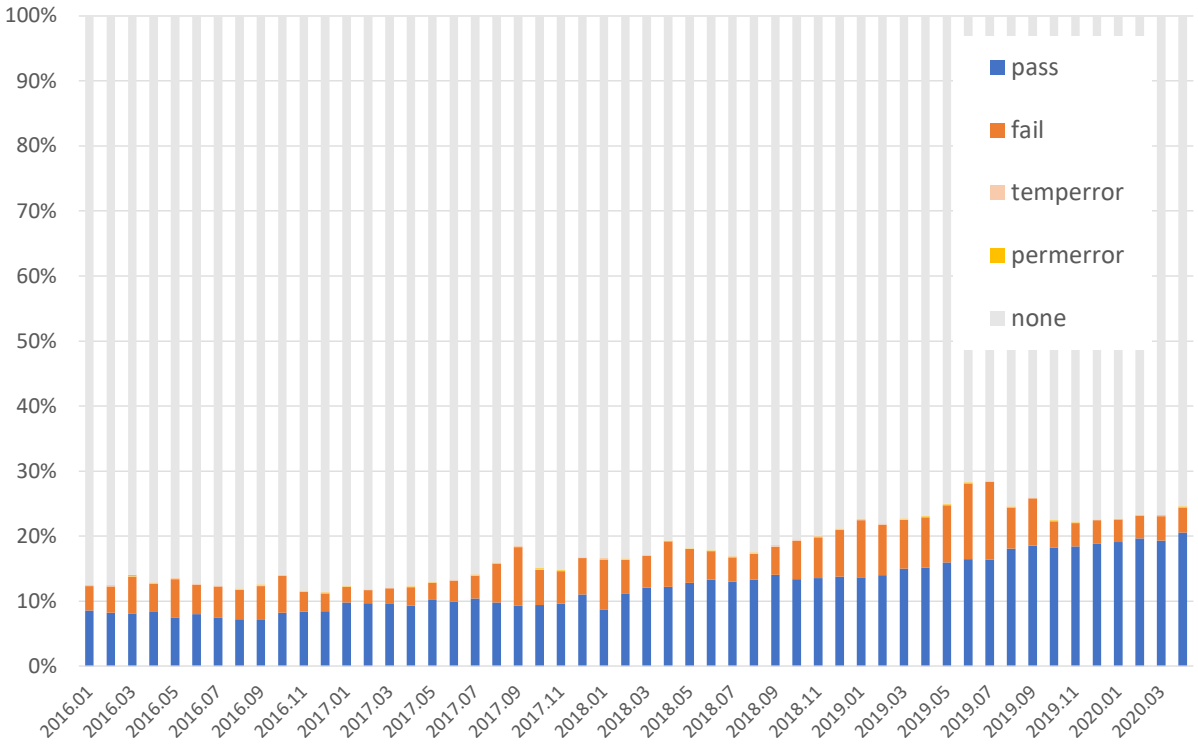

図 2.6: 国内における DMARC 認証結果の推移

られている [29]．以下に Autehntication-Results: ヘッダの例を示す．

```
Authentication-Results: example.com;
      spf=pass smtp.mailfrom=example.net;
      dkim=pass (good signature) header.i=@example.net;
      dmarc=pass header.from=bob@example.net
```

ヘッダ名（Autehntication-Results:）に続くホスト名（example.com）は，認証を行ったホスト情報である．各送信ドメイン認証などの結果は，認証の仕組みとその結果と認証ドメイン名を “;” で区切ることにより，複数記載することができる．認証を行うホストは，認証結果のなりすましが行われないように，既に同じホスト名で認証情報が付加されていないかを確認の上，ヘッダ情報を付加する．メール受信者や MUA などのメールソフトウェアは，このヘッダ情報を参照し，受信したメールの送信ドメイン認証の結果を確認することができる．

最近では，DMARC の認証結果が pass だった送信ドメイン名に対して，ロゴ（Brand

Indicator）を表示する BIMI[5][3] の規格の議論が行われており，メール受信者に対してよりわかりやすい認証結果の提示方法についても検討が行われている．

2.2 迷惑メールと送信者レピュテーション

迷惑メールは，様々なセキュリティに関する問題の発端にもなっており，その対策手法はこれまで様々なものが研究されてきた [24][5]．メール内容から判断する手法としては，メール本文中の単語やそれらを統計的に判断するベイジアンフィルタ [41][17] が注目を集めたが，その後も機械学習などを含め様々な試みが行われてきた [20][8][16]．また多くの商用メールサービスで利用されている迷惑メールフィルタでは，送信されている迷惑メールの特有の特徴を集めることで迷惑メールであるかを判定する手法が利用されている [37]．

受信したメールの送信者の情報を利用して，受け取りの判断を行うことは，迷惑メール対策の手法としてこれまで広く行われてきた．メール受信時に得られるメール送信元の IP アドレスは，送信者を識別する信頼できる情報であり，迷惑メールかどうかの判断に利用されてきた [39][43]．DNS の仕組みを利用して，ブロックすべき IP アドレスかを問い合わせることができる DNSBL(DNS Block List) は，リアルタイムに最新の情報にアクセスできること，簡単にメールサーバに組み込めることから古くから利用されており，提供する組織も複数存在している．さらに送信元の IP アドレスの履歴などから，メールの受け取りを遅らせるなどの手法 [49] や，IP アドレスがブロックリストに含まれている場合に受け取りを拒否したり，受け取りの判断ができない送信元 IP アドレスについて，通常のメールサーバであれば再送することを期待して一時的な受け取り拒否をおこなう Greylisting[6][30] などの手法も提案されてきた．

ここでは，迷惑メール対策としてメールの送信者情報を評価する送信者レピュテーションについて，これまでの手法や元になる情報の収集方法について説明する．

2.2.1 IP レピュテーションと収集方法

DNSBL を運営している Spamhaus[38] では，“spam” の定義を UBE (Unsolicited Bulk Email，未承諾大量メール) としており，メールの内容については評価していないとしている．しかしながら，Spamhaus による SBL[6]の Policy としては，自組織のメンバによって判

[5]Brand Indicators for Message Identification
[6]Spamhaus Block List

断された IP アドレスあるいは IP アドレス範囲を対象としており，その判断基準や情報の収集方法については明らかにされていない．また別の DNSBL を提供する SpamCop[46] でも，同様に IP アドレスのブロックリスト SCBL（SpamCop Block List）を提供しているが，利用者からの報告や自動的な報告，ハニーポットなどを利用してにリストを構築し，それらの頻度によって重み付けを行なって IP アドレスの評価を行っている．SpamCop では，ブロクリストの誤認識による受信拒否を防ぐために，許可リスト（Allow List）の利用を推奨しているが，その具体的な対象や収集方法については述べられていない．

IP アドレスに対する評価方法は様々提案されており，Esquivel[12] らは，メール利用者への spam の配送量を軽減するための仕組みとして，軽量な pre-acceptance アプローチに注目し，IP レピュテーションの効果と構築の可能性について報告した．メールの送信者を (1) 正規のメールサーバ（legitimate servers）(2) エンドユーザが利用するホスト（end-hosts），(3) 不正利用者 (spam gangs) の 3 種類に分類する．正規のメールサーバは，大手のメールサービスプロバイダなどのドメイン名や，商用のメールフィルタを用いてこれまでの送信履歴などからドメイン名を収集し，それらの SPF レコードから IP アドレスを収集する．end-hosts と spam gangs をブロックすべき送信元とした．なおエンドユーザが利用する動的ネットワークアドレスに対して，ネットワークを管理する ISPs[7]が，フィルタを設定してインターネット側へ直接メール送信させない対策（OP25B[8][18]）が，これまで日本では送信側の対策として普及してきている．

IP アドレスの評価エンジンである SNARE[22] は，メールの送受信のタイミングや地理的な距離などから IP アドレスの評価を行う．既存の DNSBL などのブロックリストに対して，ローカルな配信を利用して動的に閾値を求める手法と，過去の迷惑メール送信元からネットワーク範囲を広げることで，改善する手法の提案もある [44]．ボットネットからの迷惑メール送信など，IP アドレスは異なっても特定の送信パターンがある送信元をその特徴から検知する手法もある [40]．

メール送信元の IP アドレスの評価については，受け取らないブロックリスト以外にも，受け取るべき正規のメール送信元（White List, 許可リスト）を集める手法も考えられる．DNSBL と同様に DNS の仕組みを利用して IP アドレスを問い合わせる DNSWL が運営されており [10]，DNSBL の場合も含めて問い合わせのための仕様も作られている [34][51]．DNSBL では IP アドレスを分類する手法として，IP アドレスの管理元を WHOIS などから調べることでヒューリスティック分類している．

[7] Internet Service Providers.
[8] Outbound Port 25 Blocking.

送信者レピュテーションの構築にあたって，DNSBL などの IP アドレスの判断を行う組織では，収集するデータ（迷惑メール）が基準の元となる．判断基準の信頼性を高めるためには，データの収集方法をある程度制限する必要があり，組織内だけでデータを集めるという運営方針がある．その一方で，より多くのデータを集めるために，信頼性をある程度の犠牲にし，その代わりに誤判定の回避手段を提示するといった運営方針もある．いずれも明確な判断手法や機械的に処理できるような手法では無く，また情報の集め方にもその信頼性を維持には課題が多いことがわかった．メールの送信元 IP アドレスを分類する手法では，受け取るべき正規のメールサーバの判定方法として，大手のメールサービスプロバイダのドメイン名とするなど対象範囲の基準は曖昧である．また，受け取るべき正規の IP アドレスは，SPF レコードに記述されている送信元 IP アドレスを収集するが，メールシステムは設備の更新等により送信元 IP アドレスが変更される場合があり，その変更のタイミングはそれぞれドメイン名毎に不定である．この手法では，正規のメールサーバの IP アドレスを最新に保つためには，定期的な SPF レコードの確認とアップデートが必要となるはずである．

2.2.2 ドメインレピュテーション

ドメイン名を評価することによって，メールの受け取り判断やウェブサイトへのアクセス制限に利用することができる．DNS の仕組みを利用して，不正なドメイン名を検出する研究は多く行われてきた [2][1][21].

送信ドメイン認証技術が普及してきたことにより，ドメイン名の評価への利用の検討も進んできている．特に SPF では，メールの送信元を示す IP アドレスを，ドメイン名に対する SPF レコードに記述するため，この記述内容を利用して不正なドメイン名を検知しようとする手法がある [45][15]．迷惑メールに利用されるドメイン名について，DNS へのアクセス数とメール受信ログから得られる情報から機械学習によって分類し推定する手法も提案されている [9].

受け取るべきメールの送信元のドメイン名について，メールの利用者から集める手法が提案されている [11]．メール利用者が利用する MUA[9]へのプラグインを開発することで，受け取るべきドメイン名のリストを集約し，メール受信の判断に利用する手法である．ドメイン名の評価基準として，アクセス数が多い人気の高いドメイン名を利用しようとする手法がある [36]．さらにメールを受け取るべきドメイン名を判断するために，これら外部の

[9]Mail User Agent.

人気ランキングと DNS での実際のアクセス，逆に不正なドメイン名やそれと関連するドメイン名などの情報を元に閾値を動的に求める手法もある [4].

メールの受け取り判断に送信ドメイン認証の結果を利用する場合，正規のメールが配送経路によって正しく認証されない課題への対応が必要となる．Konno[27][28] らは，送信ドメイン認証の誤検知に対応する手法として，メール受信側がメール送信側に送信する DMARC レポートを利用する手法を提案した．DMARC レポートには，メール送信元の IP アドレス毎に，メール受信時の SPF，DKIM，DMARC の送信ドメイン認証結果や受信処理に関する統計情報が含まれている．これらの情報を用い，送信ドメイン認証の結果と RFC5322.From（ヘッダ From）との一致しているかなどの情報から，X-means によって送信元をクラスタリングする．既知の転送メール元が含まれるクラスタを転送メールと判断する．転送メールの送信元 IP アドレスがわかれば，SPF で認証が失敗したメールがその転送メールの送信元から送信されていれば，なりすましメールと誤判断することを抑止できる．

ドメイン名については，IP アドレスと異なりネットワーク構成の変化に影響を受けないという利点はあるが，その取得は容易であり，日々新しいドメイン名が作成される現状で，その評価を予め決めておくことは簡単ではない．特に迷惑メール送信時に利用されるドメイン名は，送信ドメイン認証技術によってなりすましが難しくなってきていることもあり，類似ドメイン名や関連するようなドメイン名 [23] を取得し利用するようになってきた．こうした背景から，迷惑メール送信に利用されるドメイン名を何らかの手法で集めるようなアプローチではなく，受け取るべきメールのドメイン名を集める手法が，メール運用の観点からは有益であると考えている．受け取るべきメールを送信者情報から迅速に判断し，遅延なくメール受信者に届ける．受け取るべきと判断できないメールについては，従来手法通りメールフィルタ等を利用し，場合によっては時間をかけて判断することで，メール受信者にとってのセキュリティリスクを軽減するといったアプローチである．本研究では，送信者レピュテーションの受け取るべきメール送信元の判断基準となるデータについて，機械的に判断可能であり，できる限り一般的に得られるような情報を利用して構築できる手法を目指している．

第3章　送信者レピュテーションの構築手法

本章では，送信者レピュテーションの構築手法として，2つのアプローチについて述べる．いずれも送信者を示す情報として，メール送信元のIPアドレス，あるいは送信ドメイン認証技術で認証されたドメイン名を利用する．

1つは，メールフィルタの判定結果を利用する方法である．もう1つは，既存の迷惑メールの判定手法などを利用しない新しい手法として，送信ドメイン認証技術の結果だけを利用し，受け取るべきメールの送信元をその特性から判断し，送信者レピュテーションとして利用する手法である．具体的には受信したメールが転送メールであるかを判定し，その送信元の情報を利用する．以下，それぞれの手法での送信者レピュテーションの構築手法と，その評価手法および評価結果について述べる．

3.1　メールフィルタを利用した送信者レピュテーションの構築

DNSBLなどのブロックリストでは，迷惑メールの情報を収集してIPブロックリスト（IPレピュテーション）を構築している．これらのブロックリストでは，メール受信者の判断で迷惑メールと判定したメールを収集する．本節では，メールフィルタの構築手法として，できる限り人を介さず自動的に収集する手法を目指し，メールフィルタの判定結果を利用する手法を提案する．受信したメールに対して，迷惑メールフィルタやアンチウイルスフィルタなどのメールフィルタを適用し，その判定結果を利用して，迷惑メールと迷惑メールでないメールに分類し，それぞれの送信者情報を抽出し，送信者レピュテーションを構築する手法である．つまり，受信した全てのメールについて，メール受信者から迷惑メールあるいは迷惑メールではないと申告を受ける代わりに，メール受信者ではなくメールフィルタの判定を利用する手法である．

受信側のメールシステムにおいては，メール受信毎にメールフィルタを利用して，受け取るべきメール（ham）と，受け取るべきではない迷惑メール（spam）を判定し，それぞ

れのメールの送信元の情報を抽出し，送信者レピュテーションとする．抽出した送信者レピュテーションを，次に受信するメールに適用することで，明らかに ham あるいは spam であるメールをメールフィルタを適用せずにそれぞれの処理を行うことで，メールフィルタに適用させるメールを減らし，受信メールシステム全体の処理負荷を軽減させる．送信者レピュテーションで判定ができなかった受信メールについては，メールフィルタに適用させることで，判定結果に応じた受信処理を行い，また送信者レピュテーションの情報の更新を行う．これらの処理の流れを図 3.1 に示す．

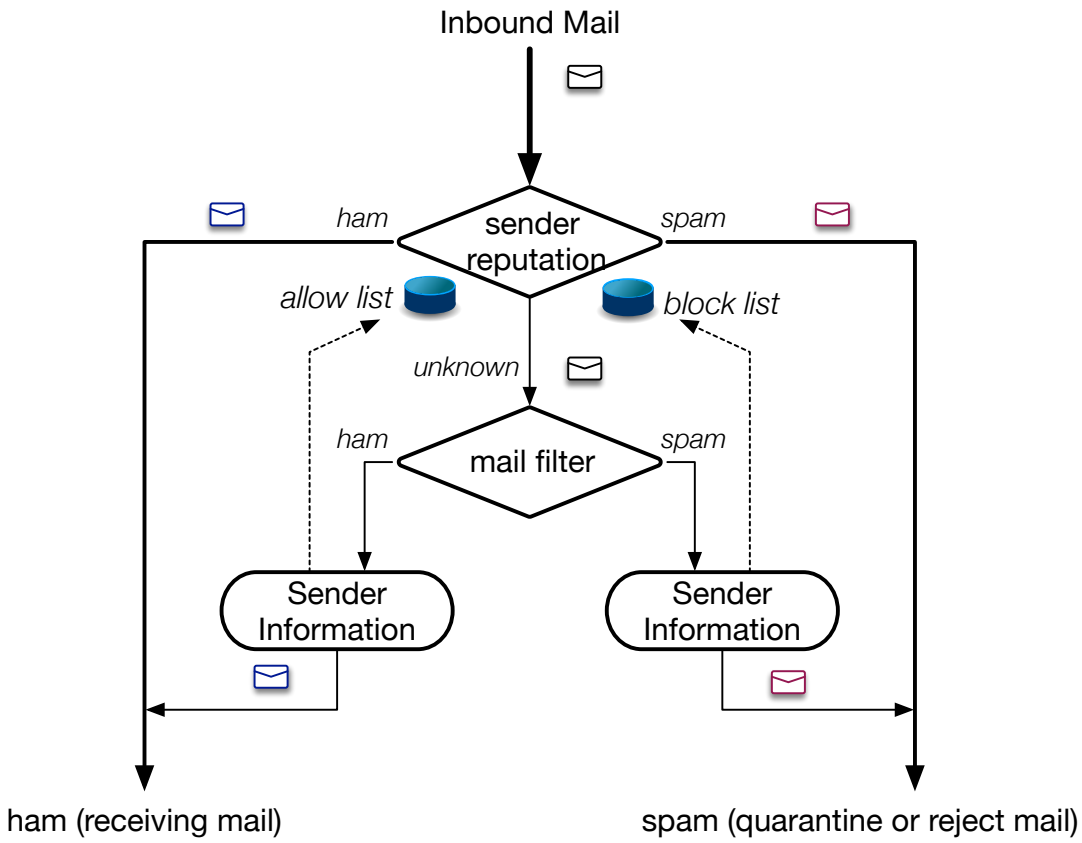

図 3.1: メールフィルタを利用した送信者レピュテーションのによる受信メールシステム

本手法によるメールフィルタの判定結果を利用した送信者レピュテーションの構築手法を評価するために，メールフィルタを備えたメールサービスで受信したメールの情報を利用し，送信者レピュテーションを実際に構築する．構築する送信者レピュテーションは，迷惑メールと判定されなかったメール（ham）と，迷惑メールと判定されたメール（spam）

それぞれを構築する．これを構築期間以降に受信したメールフィルタを適用したメールそれぞれに対して適用する．迷惑メールと判定されなかったhamに対して，hamの送信者レピュテーションがどの程度の割合が含まれれるか，同様にspam判定されたメールに，spamの送信者レピュテーションがどの程度の割合が含まれるかを調査する．より多く送信者レピュテーションが含まれれば，メールフィルタを適用しなくて済むメールが多くなるということになり，送信者レピュテーションが有効に機能する割合が高いということになる．送信者レピュテーション構築のための受信メール量による有効性を評価するために，送信者レピュテーションの構築期間を1週間と4週間に分けて調査する．また，これらの構築した送信者レピュテーションが，収集期間以降にどの程度継続して利用可能かを把握するため，それぞれの受信メール期間毎に含まれる割合についても調査した．

送信者レピュテーションの誤判定は，できる限り少ないことが求められる．そのため，送信者レピュテーションの構築においては，収集期間内において全て受け取るべきメール（ham）と判定された送信元と，全て迷惑メール（spam）と判定されたメール，それぞれの送信元情報だけを集めることとした．つまり，同じ送信元から，迷惑メールおよび迷惑メールではないとそれぞれ判定されたメールがあった場合，その送信元情報は，いずれの送信者レピュテーションにも含まれないことになる．

送信者レピュテーションは，2019年9月にそれぞれ1週間と4週間に受信したメールを対象とした．2019年9月の1ヶ月間で受信したメールは，約3億4千万通であった．構築した送信者レピュテーションの適用は，構築期間以降，1週間単位の受信メールに対してどの程度含まれていたかを調査した．1週間に受信したメール量は，約8千万通から約9千万通であった．

収集する送信者情報としては，送信元のIPアドレス，送信ドメイン認証技術SPFで認証されたドメイン名，送信ドメイン認証技術DKIMで認証されたドメイン名とした．以下，それぞれの調査結果を示す．

3.1.1 IPレピュテーション

メールの送信元を示すIPアドレスは，これまでも迷惑メール対策の手法として，ブロックリストとして利用したり，グレーリストの手法などに利用されてきた．このIPアドレスを，送信者レピュテーションとしてメールの受け取りの判断にどの程度利用できるかを調査した．本研究では，IPアドレスは送信側のメールシステムによって変わる可能性がある情報であるため，送信者レピュテーションとしては，送信ドメイン認証技術によって認証

されたドメイン名を利用することとしているが，本調査は既存の手法（IP ブラックリストなど）との比較を目的として行う．調査結果を図 3.2 に示す．

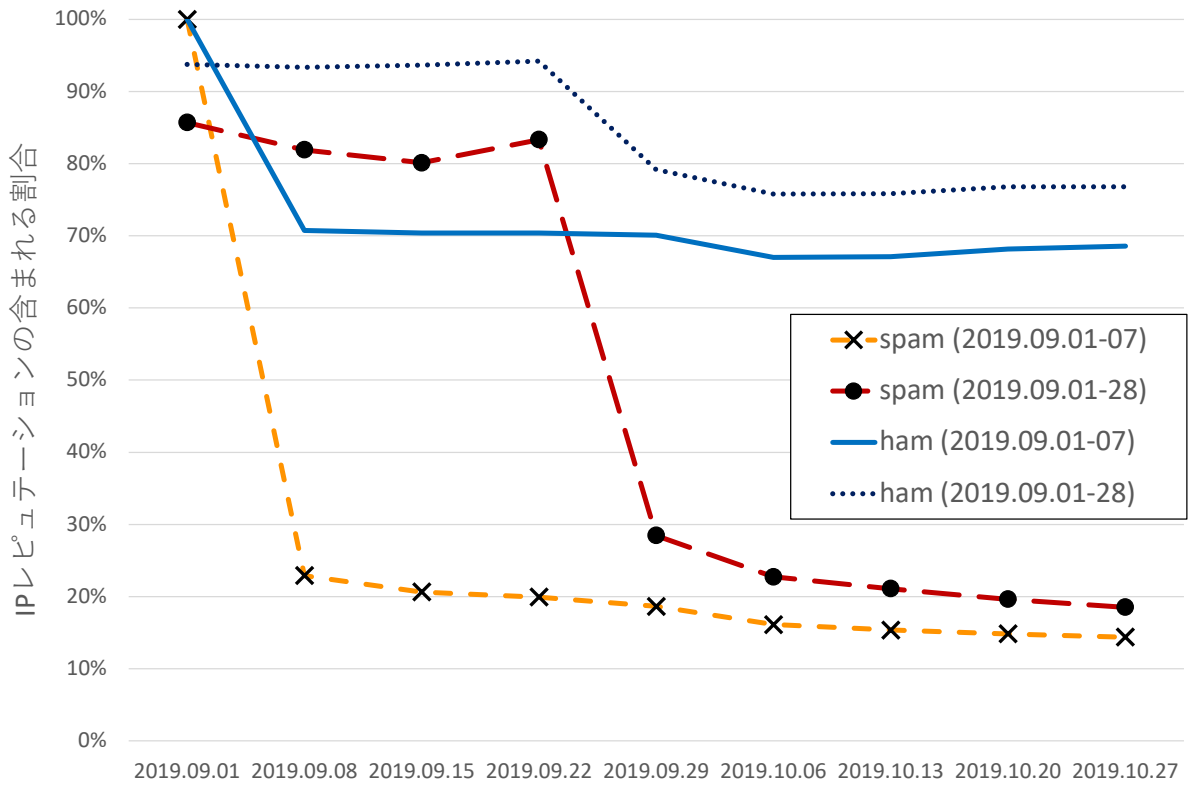

図 3.2: IP レピュテーションの継続割合

それぞれの調査は，送信元の IP アドレスがどの程度含まれるかに対する割合であり，実際に受信したメール量の割合とは異なっている．つまり，送信者レピュテーションとしての IP アドレスが含まれる割合が高い場合でも，メール送信量が多い送信元が含まれていなければ，メール受信量としての割合としては低くなる場合もある．実際に，迷惑メールでないメールに含まれる ham の IP レピュテーションの含まれる割合は，収集期間以降で約 80%弱で推移しているが，メール受信料割合としては約 60%弱であった．

IP アドレスによる送信者レピュテーションでは，迷惑メールではない ham に対して含まれる割合が高く，逆に迷惑メールの spam に対する割合が低い結果となり，さらに収集期間以降に極端に低下するという結果が得られた．またいずれも，収集期間が長い方がそれ以降に含まれる割は高いが，spam の方が含まれる割合が減少していく傾向がより強いことがわかった．これは，迷惑メール（spam）の実際の送信元が広範囲にわたり，同じ送信元からの spam 送信がそれほど多くないことが理由と考えられる．

この調査結果から，送信元の IP アドレスについては，迷惑メールでない ham に対しては，送信者レピュテーションとしてある程度有効に機能する可能性が高いことがわかった．

3.1.2 SPF レピュテーション

送信ドメイン認証技術 SPF で認証されたドメイン名についても，IP アドレスと同様に調査を行った．まず，送信者レピュテーションの構築期間である，2019 年 9 月に受信したメールの SPF による送信ドメイン認証の結果の割合について図 3.3 に示す．

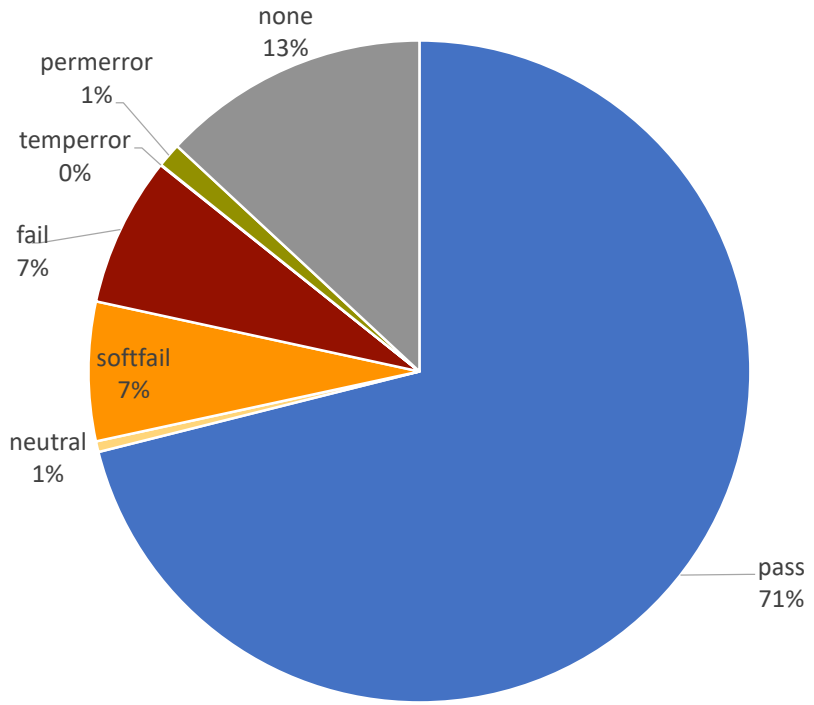

図 3.3: 受信メールの SPF 認証結果割合

メール送信側の SPF の導入割合は高く，受信したメール全体の 87%が SPF に対応したドメイン名を利用していた．そのうち，正しく認証できたメールの割合は 71%であり，これも比較的高い割合であった．このことから，送信ドメイン認証技術 SPF で認証されたドメイン名を利用した送信者レピュテーションは，ある程度有効に機能することが期待できる．SPF で認証が失敗した割合は，失敗の種類はそれぞれ異なるが[1]，合計では 15%と比

[1]SPF の認証失敗の種類は，送信ドメイン名側で設定した SPF レコードの強度による．

較的高い割合であった．これは，詐称されたメールが多かった可能性もあるが，既に述べた通り，転送されたメールにより SPF 認証が失敗した可能性もあると考えられる．

次に IP アドレスのレピュテーションと同様に，SPF 認証されたドメイン名について，メールフィルタの結果から ham と spam のドメイン名に分類し，それぞれ受信メールにどの程度含まれたかを調査した．これも受信メール量に対する割合ではなく，SPF 認証されたドメイン名の種類全体に対する割合である．結果を図 3.4 に示す．

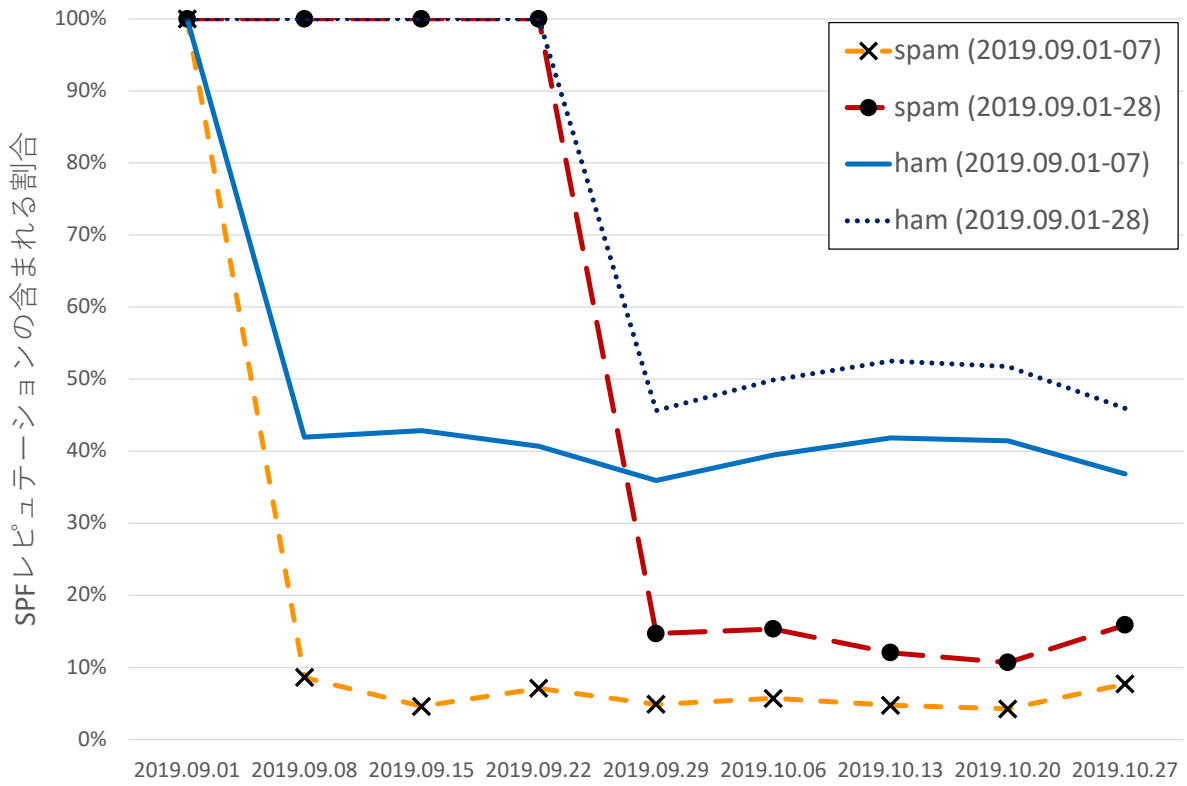

図 3.4: SPF レピュテーションの継続割合

SPF 認証されたドメイン名による送信者レピュテーションでは，迷惑メールでない ham に対して含まれている割合が高かったが，IP アドレスに比べてその割合は低い結果となった．ドメイン名の収集期間の長さでは，1 週間では約 40%前後，4 週間でも約 50%前後という結果となり，IP アドレスと比較して 30%程度低い結果となった．spam に対しても同様に，IP アドレスと比較しても含まれる割合はより低い結果となった．

受信メールの受け取るべきメールと判定された ham に対して，SPF の送信者レピュテーションが含まれる割合がそれほど高くない理由としては，SPF 認証に対応したドメインの数が多くかつ広範囲であることが考えられる．これに対して，送信者レピュテーションで

より多くの送信者情報（SPF 認証ドメイン名）を適合させるためには，より長い収集期間で受け取るべき SPF 認証ドメイン名を収集する方法が考えられる．またより多くのメールを送信する SPF 認証ドメイン名を，受け取るべき送信者レピュテーションに含めることができれば，受信メール量に対してより多くの割合のメールをメールフィルタを経由せずメール受信者に届けることができる．そこで，メールフィルタの判定結果による分類毎に，抽出した SPF 認証ドメイン名の数と，それらの送信元からどの程度メールが送信されているかを把握するために，メール受信数割合とドメインあたりの平均メール送信数を調べた．結果を表 3.1 に示す．

表 3.1: SPF ドメインレピュテーションの抽出

判定分類	ドメイン数	受信割合 (%)	平均送信数
ham only	1,473,326	68.9	115.1
spam only	155,088	0.3	4.4
both	14,804	30.8	5,125.4

判定分類の ham only は，調査期間のなかで迷惑メールと 1 度も判定されなかった SPF 認証ドメインを示している．ドメイン数も多く，SPF 認証できたドメイン名全体の約 90%であった．判定分類の spam only は，調査期間のなかで全て迷惑メールと判定された SPF 認証ドメインを示している．判定分類の both は，迷惑メールと判定された場合と，迷惑メールでないと判定された場合の両方であった SPF 認証ドメインを示している．この調査結果から，both はドメイン数自体は多くは無いが，ドメイン名あたりの送信メール数が他の分類に比べて極端に多く，その結果受信メールに対しても約 30%と高い割合となっていることがわかった．この送信元のドメイン名は，メール送信数からもメールマガジンなどを送信する，いわゆる大量送信メール（bulk mail）の送信元であることが推測できる．メールマガジンは，その内容として Web サイトの URL 情報などを多く含む場合が多く，その手法が迷惑メールと類似しているために迷惑メールと判定されてしまった可能性がある．またメールマガジンの購読を登録したメール受信者が，購読したことを忘れたか購読解除の方法が見当たらないことから受け取らないようにするため，迷惑メール申告してしまう場合もあり，これによりメールフィルタによって迷惑メール判定されている可能性もある．よって，受け取るべきメールを送信者レピュテーションを利用して判断する割合を増やすためには，この both の送信元の中から，なるべく受け取るべきメールが多い送信者を抽出する必要がある．

また参考までに，spam only の送信元からのドメインあたりの平均送信メール数が 4.4 通

と極端に低いこともわかった．これは，なるべく同一の送信元から spam を大量に送信しないことで，受信側に検知され対策されることを防ぐことを目的としていると考えられる．こうした spam 送信の手法は，一定の制限以下で迷惑メールを送信する snowshoe spam[50] とも呼ばれる．さらに，この spam only の SPF 認証ドメイン名は，迷惑メールを送信するために，あえて SPF の設定をして送信していることになる．メール受信側で送信ドメイン認証技術を導入する初期の頃は，認証に失敗したメールはなりすましメールであるため，受け取る必要が無いメール，と判断することがあった．しかしながらこの結果らも，迷惑メール送信者の中には．SPF 認証が成功するような設定をして迷惑メールを送信する場合があることがわかった．これらのことからも，送信ドメイン認証の結果（pass した）だけではなく，正しく受け取るべきメールを判断するためには，認証したドメイン名を評価することも必要であることがわかる．つまり，認証したドメイン名に対すて送信者レピュテーションを適用することが必要ということである．

3.1.3　DKIM レピュテーション

送信ドメイン認証技術 DKIM で認証されたドメイン名についても，同様に調査を行った．DKIM についても，送信者レピュテーションの構築期間である 2019 年 9 月に受信したメールの DKIM による認証結果の割合について図 3.5 に示す．

メール送信側の DKIM 導入割合は，SPF に比べて低く，受信メールの 40%程度の割合であった．その一方で，認証が失敗する割合は低く，約 1%という結果であった．これは，SPF とは異なり DKIM はメール転送でも認証が失敗しないことが理由として考えられる．DKIM 認証が失敗する理由は幾つか考えられるが，認証が失敗（fail）したということは，DKIM 認証のための情報である `DKIM-Signature` ヘッダをあえて付加し，その電子署名が合わなかったということになる．通常の認証失敗では，署名対象となる本文やヘッダが署名時から変更された場合ということになる．また DKIM 署名に設定間違いがあった場合も考えられる．SPF と異なり，認証失敗の原因は電子署名を計算等して確認する必要があるため，一般的なメール受信者では理由がわからない場合が多い．迷惑メール送信者が，とりあえず DKIM 認証のためのヘッダがあれば，たとえ DKIM 認証が失敗したとしても，なんらかの配送経路上の事情によるもので正規のメールと判断してもらえると考えた可能性も考えられる．

次に IP アドレスや SPF 認証ドメイン名の送信者レピュテーションの構築と同様に，DKIM 認証されたドメイン名について，メールフィルタの結果から ham と spam のドメイン名に

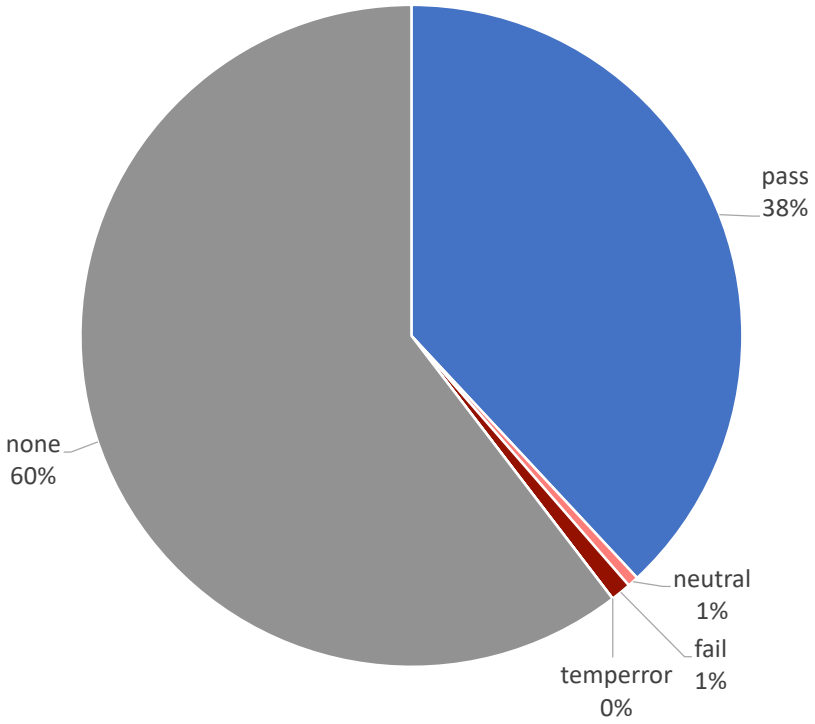

図 3.5: 受信メールの DKIM 認証結果割合

分類し，それぞれ受信メールにどの程度含まれたかを調査した．結果を図 3.6 に示す．

DKIM 認証ドメイン名を利用した送信者レピュテーションの中で，受け取るべきドメイン名については，SPF 認証ドメイン名に比べて比較的高い割合となった．しかしながら，SPF に比べて DKIM 認証できたメールの割合が少ないことから，そうした傾向が DKIM への対応が増えた場合でも継続するかは別途確認が必要と考える．

SPF 認証ドメイン名と同様に，DKIM 認証されたドメイン名について，受信メールに対してメールフィルタの判定結果を元に spam only と ham only，両方の送信元である both に分類し，それぞれのドメイン名数と，メール受信の割合，ドメイン名あたりの平均送信数について調査した．結果を表 3.2 に示す．概ね SPF の場合と同様であり，メールマガジンなどの大量送信するメールの送信元が both に含まれているなど，同じような傾向がみられた．

SPF 認証ドメイン名に比べて，全体的に DKIM 認証ドメイン名の数は少ないが，これは送信側の DKIM 導入のためのコストに違いがあるためと考えられる．2.1 節で述べた通り，SPF 認証は，DNS 上の TXT 資源レコードに，SPF レコードの形式で送信メールサー

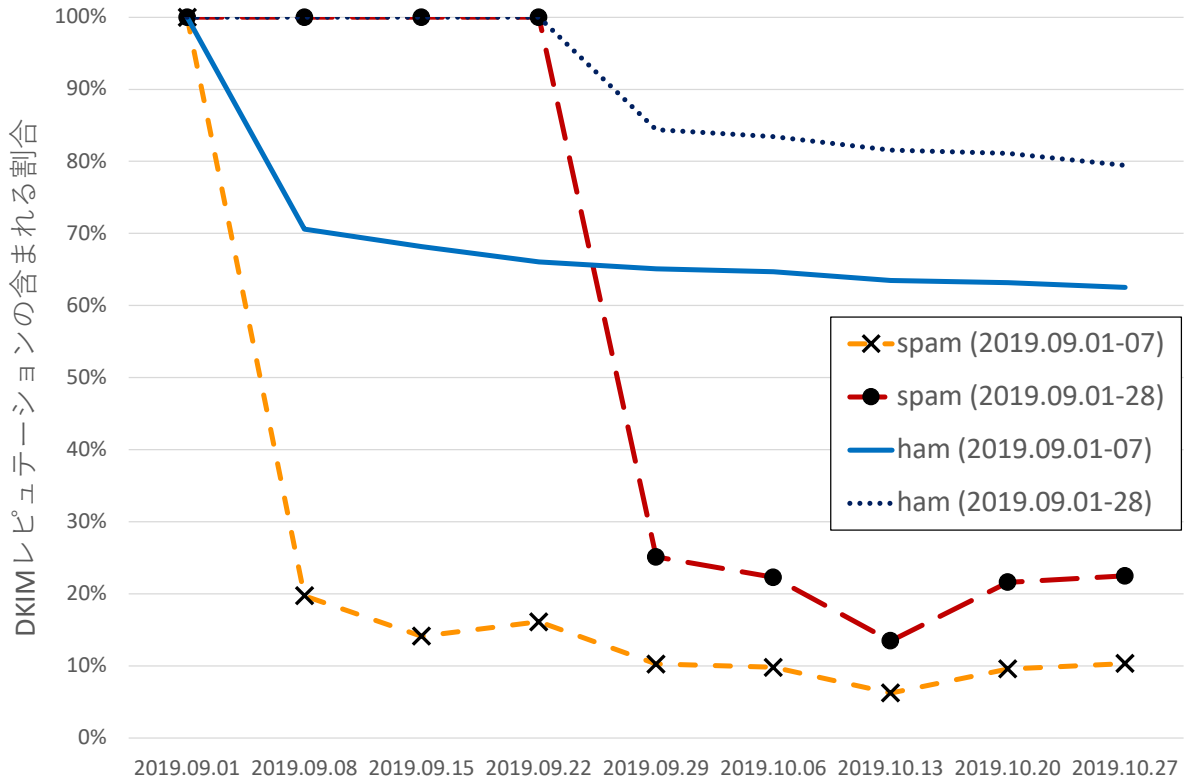

図 3.6: DKIM レピュテーションの継続割合

表 3.2: DKIM ドメインレピュテーションの抽出

判定分類	ドメイン数	受信割合 (%)	平均送信数
ham only	201,369	61.8	404.1
spam only	21,703	0.2	10.5
both	8,946	38.0	5,603.7

バの情報を記載するだけで導入することができる．それに対して DKIM 認証は，DNS 上の TXT 資源レコードに，電子署名の公開鍵情報を DKIM 鍵レコードとして記載し，送信メールサーバ上に，送信メールに対応した電子署名を作成し，メールヘッダとして記載する処理を機能追加する必要がある．こうした導入コストの差が，受信メールに対する送信ドメイン認証できたドメイン数の差になっていると考えられる．

3.1.4 メールフィルタを用いた送信者レピュテーションの考察

メールフィルタの判定結果を利用し，受信したメールを迷惑メール（spam）と迷惑メールと判定されなかったメール（ham）に分類し，それぞれのメールから送信者情報を抽出し，送信者レピュテーションを構築した．対象とした送信者情報は，送信元の IP アドレス，SPF 認証ドメイン名，DKIM 認証ドメイン名であった．また，送信者レピュテーションを抽出する期間を，1 週間の場合と 4 週間の場合それぞれで変えることで，適用できる受信メールに対する割合についても調べた．これらの送信者レピュテーションを利用し，受信したメールに適用した．実際には，受信したメールのログと，メールフィルタの判定結果のログを利用して検証した．

いずれの送信者情報による送信者レピュテーションでも，迷惑メール（spam）に対しては，適用できたメールの割合は低く，20%前後の割合であった．迷惑メールではないメール（ham）に対しては，送信者情報によって差があり，IP アドレスや DKIM の場合は 80%近くと比較的適用割合が高い結果となった．しかしながら，DKIM 認証ドメイン名は，メールの送信側で対応している割合が半分以下と低い状態であったため，SPF と同等の普及率となった場合に同じような傾向が得られるかは確認が必要と考えている．SPF 認証ドメイン名の ham については，受信メールに対して 50%程度あり，ある程度の利用できると考えている．

また，いずれの送信者情報についても，抽出期間が長い方が受信メールにより多く適用できたことから，継続して送信者情報を抽出するなどの仕組みがあれば，今回の調査結果よりはより多くの受信メールに適用できる可能性があると考えている．今回は，全て迷惑メールと判定されたメールと，全て迷惑メールでは無いと判定されたメールの送信者情報だけを抽出したが，メールフィルタの判定自体も全て正しいわけではなく，また迷惑メールの踏み台送信なども場合も考えられるため，ある程度の閾値を持った割合によって迷惑メール（spam）か受け取るべきメール（ham）かに振り分ける方法もある．または，レピュテーション自体を受け取るべきかどうかの 2 値ではなく，受け取るべき度合いを数値で示すなどの方法もある [48]．

今回の調査および送信者レピュテーションの検討では，調査結果からは，SPF の認証ドメイン名の ham については送信者レピュテーションとしてある程度利用できる結果が得られたと考えている．DKIM の認証ドメイン名については，まだ普及率が半分以下という状況であり，今後より普及した段階で別途調査および検討が必要と考えている．また，ネットワーク構成の変化によって変わる可能性がある IP アドレスは，今回の調査では参考情報としている．

3.2　送信ドメイン認証技術を用いた送信者レピュテーションの構築

本節では，送信ドメイン認証技術を用いて，受け取るべきメールの送信者レピュテーションを構築する手法について述べる．これまでの送信者レピュテーションは，既存のIPアドレスのブロックリストを含め，メール受信者によって，あるいは前節で示したように迷惑メールかどうかの判断に計算機を利用するメールフィルタなどによって，メールをまず分類することが前提であった．この分類された受け取るべきではないメールや，受け取るべきメールからそれぞれ送信者情報を抽出することで，ブロックリストや許可リストといった送信者レピュテーションを構築していく．こうした手法は，メールが迷惑メールかどうかの判断部分が全ての性能の鍵を握ることになる．

本研究では，こうしたアプローチとは異なる，メール送信元の素性についての特徴を捉えることで，受け取るべきメールかどうかを判断する，新しい手法を提案する．これらメール送信元を判断するために，複数の送信ドメイン認証技術を利用する．

まず，メールの送信元として，転送メールの利用する目的を明らかにし，転送メールの送信元が受け取るべきメール送信元であることを示す．この転送メールの送信元を，送信ドメイン認証技術の認証結果の違いを利用して判定する手法を示す．送信者レピュテーションとして，認証されたドメイン名を利用するために，メール転送の送信元のIPアドレスを利用し，受け取るべきドメイン名を抽出する手法を示す．抽出した受け取るべきメールの送信者レピュテーションを評価するために，実際に受信したメールの記録情報（ログ）から，提案する手順に従い送信者レピュテーションを構築する．この送信者レピュテーションを，さらに実際に受信したメールの記録情報（ログ）を利用して評価を行う．

3.2.1　転送メールの目的と性質

転送メールとは，メールの受信者がMUA[2]等を利用して，受信したメールをMUAを操作して別の宛先に手動で送信するメールではなく，あらかじめ転送設定された宛先にメール受信時に自動的に転送するメールである．具体的には，メールサーバ（MTA[3]）が備える，エイリアス機能やメール受信者毎に記述する`.forward`ファイルなどによって設定され，受信したメールが自動的に再配送されるメールである．こうした自動送信では，受信

[2]Mail User Agent．メール送受信ソフトウェア
[3]Mail Transfer Agent

したメールの内容は通常変更されず，受け取ったままのメールデータがそのまま転送先に送信される．

転送メールを利用する目的としては，複数のメールアドレスを利用しており，元のメールアドレスを継続して利用したい場合や，それぞれ届いたメールを 1 箇所のメールシステムで参照したい場合などが考えられる．また，転送メールとはいえ，それぞれ独立したメールアドレスであり，それぞれのメールサービスで提供する機能があるため，特定のメールサービスの機能（メールフィルタなど）を経由させるためにメール転送を利用することも考えられる．いずれにしても，転送メールの設定者は，その転送メールを受け取るメール受信者と同一であるか，強い関係を持ったメール利用者であると考えることができる（図 3.7）．

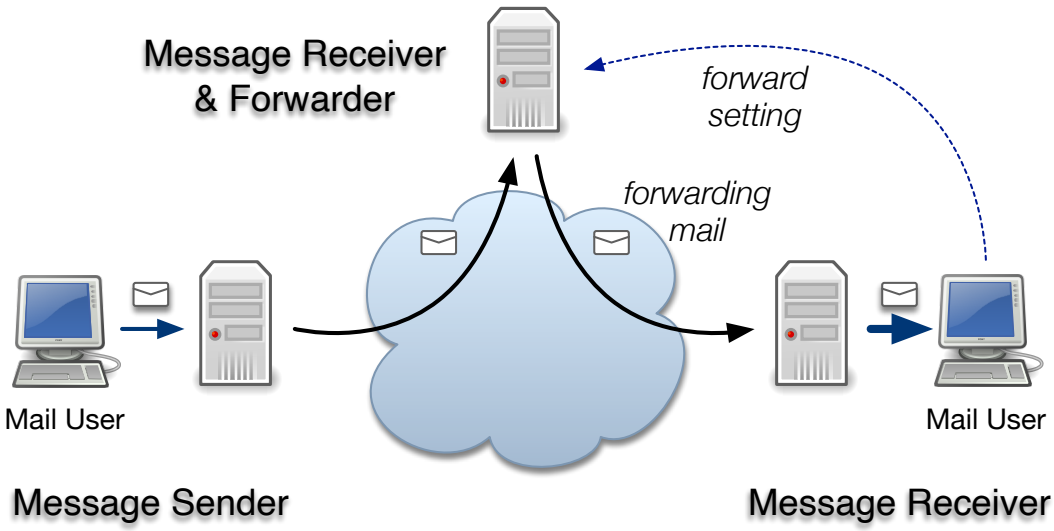

図 3.7: メール転送設定

そのため，転送メールの受信者からみれば，転送メールを送信するメールサーバは受け取るべきメール送信元であり，転送メールサーバは正規のメールサーバと捉えることができる．つまりこの転送メールの送信元メールサーバは，受け取るべきメールの送信元として，送信者レピュテーションに加えるべきである．

しかし，転送メール全てが受け取るべき正規のメールとは限らない．最初に迷惑メールが送信され，その迷惑メールがメールフィルタ等を介さずに転送された場合，転送先にも迷惑メールが送信されることになる．こうしたケースでは，転送メールサーバは送信者レ

ピュテーションにより正規のメールサーバと判断されるため，迷惑メールがメール受信者に届いてしまうことになる．そのため，こうした転送される迷惑メールの対策も必要と考える．

3.2.2　転送メール送信元の抽出

転送メールが，メール受信者からみれば受け取るべきメールであることを示した．この転送メールの送信元を送信ドメイン認証技術の認証結果を利用して，抽出する手法について述べる．

一般的なメール転送

2.1.1 節で述べたように，一般的な転送メールは転送先で SPF の認証が失敗する．また，DKIM は最初のメール送信者が DKIM に対応していれば，DKIM 認証は成功（pass）する．このメール転送の SPF と DKIM のそれぞれの認証結果を図 3.8 に示す．

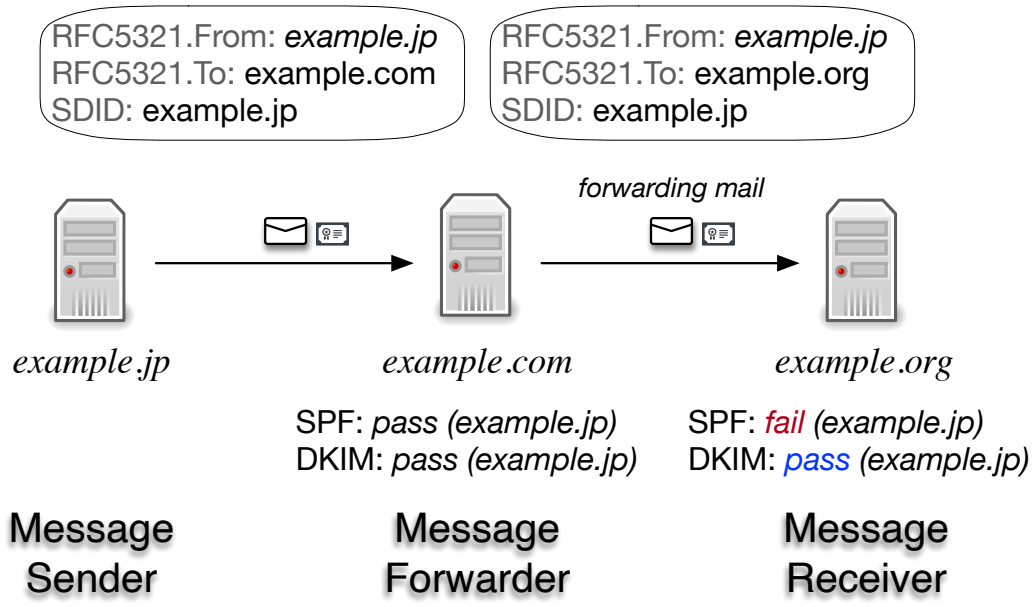

図 3.8: 転送メールの SPF と DKIM 認証

example.jp のメールサーバは，宛先 example.com へメールを送信する．example.com は，受信したメールをあらかじめ設定されたメール転送先である example.org 宛に送信する．example.com のメールサーバは，SPF の認証ドメイン名が含まれる RFC5321.From を書き換えずに，最初の example.jp のまま転送先にメールを転送する．この .forward ファイルに転送設定を行うことでメール転送し，メール転送時に RFC5321.From を書き換えずに受け取った情報のまま転送する仕組みは，オープンソースの Sendmail[7] など古くから利用されてきたメールサーバ（MTA）で利用されてきた．メール転送先の example.org では，受信したメールの SPF 認証の際に，RFC5321.From に示された example.jp の SPF レコードを取得し，受信メールの送信元 IP アドレスがその SPF レコードに含まれているかを確認する．直接のメール送信元である example.com のメールサーバは，RFC5321.From のドメイン名 example.jp とは無関係であるため，受信した転送メールの SPF 認証は失敗することになる．最初のメール送信元の example.jp が，メール送信時に DKIM 認証のための DKIM 署名を付加していたとすれば，メール転送先の example.org の DKIM 認証でも認証される（pass）ことになる．

この転送メールの SPF と DKIM の認証結果を用いれば，以下のような条件で転送メールを判断することができる．

- SPF の認証が失敗
- DKIM の認証が成功（pass）

一般にネットワーク方式の SPF の認証が失敗したということは，直近のメール送信元が本来のメール送信元でなかった，ということである．しかしながら，DKIM が認証できている（pass）ということは，メールそのものは認証されたドメイン名から送信されたメールであることを示している．転送メールそのもの自体を判断するためには，この条件を必ず満たす必要があるが，転送メールの送信元（IP アドレス）を判断するためには，この条件のメールが 1 通でも届けば転送メールの送信元の判断には十分となる．そのため，メール送信側の普及率がそれほど高くはない DKIM を本手法では利用しているが，実用上はこの手法でメールの転送元を十分に判断できると考える．

送信者情報を書き換えるメール転送

メール転送の送信元を抽出していた過程で，メール転送元が十分に抽出できていないことに気がついた．具体的には，大手のフリーメールサービスのドメイン名が含まれていな

かった．これらのメールサービスのメール転送の方法を調べたところ，メール転送時に SPF の認証ドメイン名である RFC5321.From を，自身のメールサービスのドメイン名に書き換えて転送していることがわかった．これらのメール転送サーバでは，2.1.1 節で述べたように，メール転送先で SPF 認証が失敗しないように，メール転送時に SPF の認証ドメイン名が含まれる RFC5321.From を書き換えて転送している（図 3.9）．

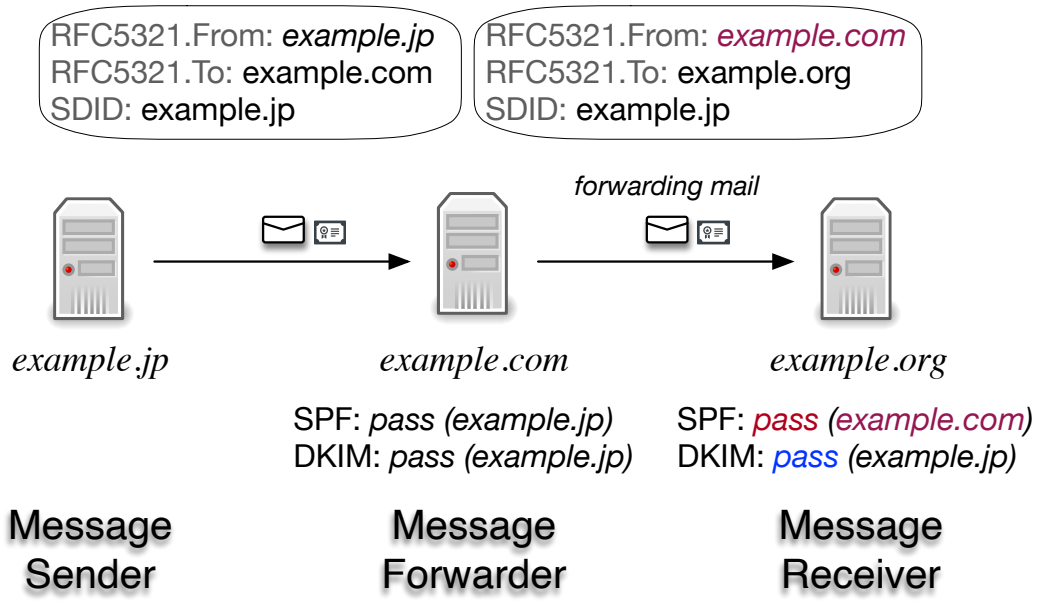

図 3.9: 送信者情報を書き換える転送メールの SPF と DKIM 認証

メール転送時に送信者情報を書き換える転送メールサーバは，メール転送時に受信時の RFC5321.From をそのまま利用せず，自身のドメイン名に RFC5321.From を書き換えてメール転送先に送信する．図 3.9 では，メール転送を行う `example.com` のメールサーバが，受信したときの RFC5321.From の `example.jp` ドメイン名を使わず，自身のドメイン名 `example.com` に書き換えてメール転送している．こうした処理により，メール転送先の `example.org` では，SPF 認証が pass することになる．

このようなメール転送時の RFC5321.From の書き換え処理により，メール転送先でも SPF 認証を pass することができ，SPF 認証が失敗したメールをなりすましメールと判断して受け取らないメール受信側にも届けることができるようになる．しかしながら，メール転送先では SPF と DKIM のいずれの送信ドメイン認証結果も同じ pass であるため，本研究で示した手法では，メールの転送元として認識することができない．

送信者情報を書き換えるメール転送元の抽出

フィッシングなどのなりすましメールが増加しており，SPF 認証や DKIM 認証の結果を積極的に利用し，なりすましメールは受け取らないとするメール受信側が増えている．こうしたメール受信側に対応するために，メール転送時に送信者情報の RFC5321.From を書き換える処理を行うメールサーバも増えてきている．さらには，メール転送そのものを止めてしまうという方法も考えられるが，普及してしまった便利なメールの利用形態は，なかなか変更することも難しい．そのため，こうしたメール転送時に送信者情報を書き換えるメール転送元についても判断できる手法が必要である．

そこで，送信ドメイン認証の認証結果だけではなく，認証されたドメイン名にも着目する．図 3.9 では，最初の送信メールが転送メールサーバの `example.com` に届いた時は，SPF と DKIM の両方の認証結果が pass であり，認証されたドメイン名も `example.jp` と同じドメイン名となっている．これは，同じメール送信元の `example.jp` から送信された通常のメール配送である．しかしながら転送メール先 `example.org` にメールが届いた時には，認証結果はいずれも pass であるが，認証されたドメイン名が `example.com` と `example.jp` となっており，異なったドメイン名となっている．これは，メール転送時に SPF の認証ドメイン名である RFC5321.From を書き換えたためであり，これをメール転送元が一致させようとすれば，メールに DKIM の再署名を行い DKIM の認証ドメイン名を SPF と同じドメイン名 `example.com` に書き換える必要がある．しかしながら，DMARC 認証までを考えれば，SPF と DKIM のいずれの認証ドメイン名も DMARC の認証ドメイン名である RFC5322.From（ヘッダ From）と異なってしまうため，メール転送時に DKIM の再署名だけを行う意味は薄い．また，DKIM の署名情報はメールヘッダとして複数存在可能なので，元の DKIM 署名をそのまま残しておくことも可能である．これらのことから，転送メールサーバでは，最初の DKIM 認証に関わる情報については変更せず，最初のメール送信時に付加した DKIM 署名もそのまま付加され転送さると考えられる．この結果から，これら SPF と DKIM の認証結果と認証されたドメイン名の違いを利用すれば，メール転送時に RFC5321.From を書き換える転送メールに対しても，その送信元を判断することが可能となる．

つまり，以下の条件でメール転送時に RFC5321.From を書き換える転送メールを判断することができる．

- SPF と DKIM の両方の認証が pass している
- その送信元からのメールで，DKIM で認証されたドメイン名が複数種類得られる

この手法も通常のメール転送の検知と同様に，全てのメールがこの条件を満たす必要はなく，それぞれDKIMに対応した転送メールが複数通届くことで，RFC5321.Fromを書き換える転送メールの送信元を抽出することができる．

3.2.3 正規メール送信元の抽出

転送メールの送信元は，受け取るべき正規のメール送信元であることを示し，送信ドメイン認証技術SPFとDKIMの認証結果および認証ドメイン名を利用して，これら転送メールの送信元を抽出する手法を示した．ここで得られる転送メールの送信元は，転送メールサーバのIPアドレスであるため，このIPアドレスから送信ドメイン認証の認証ドメイン名を取得する必要がある．本節では，受け取るべきメールの範囲をさらに広げ，認証されたドメイン名を送信者レピュテーションとして利用するために，転送メールの送信元を利用して送信者レピュテーションを収集し構築するための手法について述べる．また，実際に収集するためのアルゴリズムを示す.

転送メールの送信元は，単に転送メールだけを送信するメールサーバということはなく，そのメールサーバを利用するメールサービスの利用者のメール送信にも利用されることが一般的である．つまり，転送メールサーバが受け取るべきメール送信元であるとすれば，そのメールサーバから送信される通常のメールについても，正しく管理された受け取るべき正規のメールと考えることができる．これら正規のメールについては，転送メールの送信元から送信されたメールで，SPFの認証結果がpassであったメールとして判断することができる．送信者レピュテーションとして利用する情報は，このSPF認証がpassしたドメイン名で十分となる．つまり，メール送信元が転送メールの送信元IPアドレスでなくても，そのドメイン名がpassしていれば，同じ管理元の送信元からのメールであると判断することができる．送信者レピュテーションとして，SPFの認証ドメイン名を利用することで，そのドメイン名がどの送信元IPアドレスから送信されるかを事前に収集することなく，SPF認証がpassしたことをもって正規のメール送信元として判断することができる．

次に，この正規のメール送信元情報の収集方法について述べる．受信メールサーバで，メール受信の都度送信ドメイン認証の結果やその送信元IPアドレス，認証されたドメイン名などを収集することは可能である．しかしながら，メール受信の都度得られる情報だけでは送信者レピュテーション構築のための情報は不十分であり，得られた情報を保持しながら複数の受信メールの情報を利用しなければならない場合もある．具体的には，前節で述べたようなメール転送時にRFC5331.Fromを書き換える転送元を判断する場合や，転送

メールの送信元から受け取るべき SPF 認証ドメイン名を抽出する手順などである．

3.2.4 送信者レピュテーション構築の手順

そこで本手法の送信者レピュテーションの構築手法を検証するために，受信メールサーバのメール受信記録情報（ログ）を利用する．一般的に，メールの受信ログには，メール送信元の IP アドレスや送信ドメイン認証の結果なども記録されている．メールの受信後に，これらのメール受信ログを集めて送信者レピュテーションを構築する．

Algorithm 1 に，送信ドメイン認証の結果と認証ドメイン名，送信元 IP アドレスの情報が含まれる受信メールのログから，送信者レピュテーションを構築する手順について述べる．

Algorithm 1 Collect Legitimate Email Domains

Require: M: received mail information data
Ensure: L: Legitimate Domains

$FW \leftarrow \emptyset, SPF \leftarrow \emptyset, SPFDK \leftarrow \emptyset, L \leftarrow \emptyset$
for all $m_i \in M$ **do**
  if $spf(m_i)$ is fail **and** $dkim(m_i)$ is pass **then**
    $FW \leftarrow FW \cup \{srcip(m_i)\}$
  else if $spf(m_i)$ is pass **then**
    if $dkim(m_i)$ is pass **then**
      $SPFDK \leftarrow SPFDK \cup \{(spfdom(m_i), dkdom(m_i)\}$
    end if
    $SPF \leftarrow SPF \cup \{(spfdom(m_i), srcip(m_i))\}$
  end if
end for
for all $(dom_i, ip_i) \in SPF$ **do**
  if $ip_i \in FW$ **then**
    $L \leftarrow L \cup \{dom_i\}$
  end if
end for
for all $(spfdom_i, dkdom_i) \in SPFDK$ **do**
  $DK \leftarrow \{dom | (spfdom_i, dom) \in SPFDK\}$
  if $|DK| \geq 2$ **then**
    $L \leftarrow L \cup \{spfdom_i\}$
  end if
end for

受信したメールに関する情報の集合を M とし，個々の受信メールを $m_i(1 \leq i \leq |M|)$ とする．この受信メール情報から，正規のメール送信元（SPF 認証ドメイン名）の集合 L を抽出する．ここで，$spf(m_i)$ と $dkim(m_i)$ は，それぞれメール m_i の SPF と DKIM の認証結果を返す関数とする．SPF 認証が失敗した場合の結果には，fail（hardfail），softfail，neutral の 3 種類があるが，$spf(m_i)$ では全て fail を返すものとする．$srcip(m_i)$ 関数は，受信メール m_i のメール送信元 IP アドレスを返す関数である．$spfdom(m_i)$ 関数は，SPF 認証されたドメイン名を返す関数であり，$dkdom(m_i)$ 関数は，DKIM 認証されたドメイン名を返す関数とする．

最初の for ループ（2 行目から 11 行目）で，受信したメール全てに対して，SPF および DKIM の認証結果を利用して，転送メールの送信元 IP アドレスの集合 FW を集める．これらは，メール転送時に RFC5321.From を書き換えないメール転送の送信元の IP アドレスを集めている．さらに，SPF と DKIM の両方の認証結果が pass だったメールの，SPF と DKIM の認証ドメイン名の対の集合を求める．これは，メール転送時に SPF 認証ドメイン名（RFC5321.From）を書き換える転送メールの認証ドメイン名を集めるために利用する．また，SPF 認証が pass したメールの送信元 IP アドレスと SPF 認証ドメインの対の集合を求める．これは，転送メールの送信元 IP アドレスから，受け取るべき SPF 認証ドメイン名を求めるために利用する．

全ての受信メールの記録について，必要な情報を集めた後，SPF 認証が pass した送信元 IP アドレスが，転送メールの送信元 IP アドレスに含まれていれば，その SPF 認証ドメイン名を受け取るべき正規のメール送信元ドメイン名 L として集める（12 行目から 15 行目）．次にメール転送時に SPF 認証ドメイン名を書き換える転送元のドメイン名を抽出するために，SPF 認証ドメイン名と DKIM 認証ドメイン名の対の集合を調べる（17 行目から 22 行目）．本アルゴリズムでは，メール転送時に RFC5321.From を書き換えるメール転送元を求める基準として，SPF 認証されたドメイン名に対して，DKIM 認証されたドメイン名の数が複数である場合を，2 以上とした（19 行目）．

受信メールに関する情報 m_i は，受信メールサーバの受信記録情報（ログ）に一般的に含まれる情報であり，本手法の評価には，実際のメールサービスで受信したメールの受信ログを利用した．

3.3 送信者レピュテーションの構築と評価

本節では，提案した送信者レピュテーションの構築アルゴリズムを，実際のメールサービスで受信したメールの受信記録情報（ログ）を対象に適用し，送信者レピュテーションを構築した結果を示す．さらに，構築した送信者レピュテーションをさらに別のログに適用させることで，構築した送信者レピュテーションの評価を行う．

3.3.1 送信者レピュテーションの構築

受信メールのログ情報を利用し，Algorithm 1 を適用させ，送信者レピュテーション L を構築する．対象とした受信メールは，2019 年 9 月の 1ヶ月間に受信した約 3 億 4 千万通である．受信メールは，全て迷惑メールフィルタおよびアンチウイルスフィルタ等の複数のメールフィルタを適用し，迷惑メールかどうかの判定を行っている．また，受信時に SPF, DKIM, DMARC の全ての送信ドメイン認証を実施している．受信したメールのそれぞれの送信ドメイン認証結果とドメイン名，送信元 IP アドレスは，受信メール毎にログ情報に記録されている．受信したメールが迷惑メール（spam）か迷惑メールでない（ham）かは，メールフィルタの判定結果を用いて分類した．実験に利用した受信メールの概要を表 3.3 に示す．この期間に受信したメールの迷惑メール（spam）割合は，11.7%であった．受信メール全体の SPF 認証割合は 71.1%であったが，spam 判定されたメールに対しては低く 2.3%であった．DKIM 認証については，受信メール全体でも 38.1%と低く，spam 判定されたメールについてはさらに 0.3%と低い割合だった．

表 3.3: 受信メールログ情報の概要

	判定分類 (%)	SPF 認証割合 (%)	DKIM 認証割合 (%)
ham	88.3	68.8	37.7
spam	11.7	2.3	0.3
total	100.0	71.1	38.1

この受信ログから，SPF と DKIM の認証結果を用いて転送メールの送信元 IP アドレスの集合 FW を抽出する．この抽出した FW と SPF と DKIM の認証結果と認証ドメイン名から，受け取るべき SPF の認証ドメイン名の集合 L を抽出する．今回，転送時に RFC5321.From を書き換えない転送元からの SPF 認証ドメイン数を L_1 として抽出し，RFC5321.From を書き換える転送元からの SPF 認証ドメイン数を L_2 として抽出した．よって，正規の SPF 認証ドメイン名 L は，$L = L_1 \cup L_2$ の関係となる．いずれも，SPF の認証ドメイン名とし

ては，RFC5321.From を対象とし EHLO/HELO のドメイン名は対象外とした．Algorithm 1 を適用した結果を表 3.4 に示す．

表 3.4: 送信者レピュテーションの抽出

送信者レピュテーション	抽出数
転送 IPs (FW)	15,169
legit SPF (L_1)	744,659
legit SPF rewrite (L_2)	11,163
legit SPF new (L)	753,017

表 3.4 の結果から，メール転送時に SPF の認証ドメイン名である RFC5321.From を書き換えない転送元のドメイン名が，RFC5321.From を書き換える転送元ドメイン名より約 66 倍多いことがわかった．この結果から，メール転送時に SPF 認証が失敗しないようにするメールサーバはまだそれほど多くは無いことがわかった．

送信者レピュテーションとして，受け取るべきメールの送信元情報としては，より広く判断しようとすればこの抽出した FW と L となる．つまり送信者レピュテーションは，以下のような使い方で受け取るべきメールかどうかの判断に利用することができる．

- 送信元の IP アドレスが L に含まれる場合
- SPF 認証が pass し，その認証ドメイン名が L に含まれる場合

メール転送元 IP アドレスの集合 FW は，IP アドレスであるため，メールシステムの変更やアドレス移転等によって変わる可能性がある情報であり，これを送信者レピュテーションとして採用することには議論の余地がある．メール転送元 IP アドレスの集合 FW を含める場合の理由としては，RFC5321.From を書き換えない通常の転送メール送信元からの転送メールを受け取るメールと判断させるためである．この転送メールについては，SPF の認証が必ず失敗してしまうことになるため，本手法の送信者レピューテーションを利用して，この転送メールを受け取るためには，必要となるレピュテーション情報となる．転送メールについては，既に述べた通り迷惑メールも含めて転送される可能性も高いため，このため，通常の受け取るべきメールと，転送メールとが区別できる仕組みを備えるという対策も考えられる．送信者レピュテーションの利用者のポリシーによる選択肢を提供できるという意味で，利点であると考える．例えば，転送メールについてはメールフィルタを適用することで，迷惑メールやセキュリティ的な脅威となるようなメールであるかを内容から判断させる，と言った使い方が考えられる．なお，転送されたメールだけを区別したい場合は，以下のような手順となる．

- SPF の認証結果が失敗（fail）であり，メールの送信元 IP アドレスが FW に含まれている場合
- SPF の認証ドメイン名が L_2 に含まれていて，DKIM の認証ドメイン名がその SPF 認証ドメイン名と無関係な管理元のドメイン名である場合

1 つ目は，メール転送時に SPF の認証ドメイン名が含まれる RFC5321.From を書き換えない転送メールを判断する手法である．2 つ目は，メール転送時に RFC5321.From を書き換えて転送するメールを判断する方法となる．

3.3.2 評価

抽出した送信者レピュテーションを利用し，受信したメールのログ情報を利用して受信メールに適用し，どの程度の受け取るべき正規のメールを判断できるかを検証する．評価の対象とした受信メールは，2019 年 10 月 1 日から 7 日までの 1 週間で受信した約 8 千万通である．概要を表 3.5 に示す．

表 3.5: 評価用受信メールログ情報の概要

	判定分類 (%)	SPF 認証割合 (%)	DKIM 認証割合 (%)
ham	91.0	72.2	38.9
spam	9.0	1.9	0.3
total	100.0	74.1	39.2

ここで示した ham と spam の分類は，メールフィルタによって迷惑メールと判定されたメールを spam として，迷惑メールと判定されなかったメールを ham とした．評価については，抽出した受け取るべき送信者情報による送信者レピュテーションを適用し，ham と分類したメールに対してより多くメールを抽出し，spam と分類したメールに対して抽出したメールが少なければ，受け取るべき送信者レピュテーションとしての性能が良いといえる．

構築した受け取るべき送信者レピュテーションの種類毎に，同じ受信メールに適用してそれぞれ含まれる割合を求める．適用の組み合わせを以下に示す．

FW: 転送メールと判定された IP アドレス FW から送信されたメール

legit SPF: メール転送時に RFC5321.From を書き換えない転送元 SPF 認証ドメイン名から送信されたメール

legit SPF+FW: Legit SPF あるいは FW から送信されたメール

legit SPF rewrite: メール転送時に RFC5321.From を書き換える転送元 SPF 認証ドメイン名から送信されたメール

legit SPF new: メール転送時に RFC5321.From を書き換えない転送元と書き換える両方の SPF 認証ドメイン名から送信されたメール

legit SPF new+FW: legit SPF new あるいは FW から送信されたメール

適用した結果を表3.6 に示す．表に示した割合は，受信メール全体に対してではなく，メールフィルタで判定された ham と spam それぞれを全体を 100%とした場合に，抽出できたメールの割合を示している．つまり，ham については割合が高いほど，より多くの受け取るべきメールを判定（TP: True Positive）できたということになる．逆に spam については，誤判定（FP: False Postive）したの割合となる．

表 3.6: 送信者レピュテーションの適用結果

送信者レピュテーション	ham (%)	spam (%)
FW	31.4	2.5
legit SPF	35.7	0.5
legit SPF+FW	45.8	2.7
legit SPF rewrite	25.6	0.5
legit SPF new	46.2	0.7
legit SPF new+FW	56.3	3.0

受け取るべきメールをより多く判定したいと考えれば，ham に対する割合が最も高い legit SPF new+FW の組み合わせを利用するべきである．しかしながら，迷惑メール（spam）を受け取るべきと判断した，いわゆる誤判定（FP: False Positive）の割合も 3.0%となる最も高い組み合わせでもある．この誤判定の主な原因は，受け取るべき送信者レピュテーションとして FW の IP アドレスを加えたことによるものと表からも推測することができる．FW 単体だけでも，spm に対して 2.5%と比較的高い誤判定割合となっている．その一方で ham に対しても 31.4%とそれなりに高い判定割合となっている．他の受け取るべき送信者レピュテーションの SPF 認証ドメイン名についても，FW を加えることで，10.1%多く ham に対しての割合が増加している．また，spam に対する割合が最も高い 3.0%は，受信メール全体の割合としては 0.27%であり，受信メールしたメール全てを迷惑メールかど

うかを判定する商用の迷惑メールフィルタの誤判定が，一般的に数%は生じていることを考えれば，十分に小さい値であると考える．

このデータからも転送メールには，迷惑メールも迷惑メールでない受け取るべきメールの両方が含まれており，メール転送元はそれらを区別することなく転送していることが推測できる．これらの転送メールをメール受信者に届けたく無い場合には，転送されたメールを判断する方法については前節で示したので，この方法を利用して転送メールをメールフィルタに適用させる，といった対策をとることもできる．

次にメール転送時に SPF の送信ドメイン認証である RFC5321.From を書き換える legit SPF rewrite からのメールを，受け取るべきメールとして送信者レピュテーションに加えた効果について検討する．RFC5321.From を書き換えるメール転送元からのメールについては，ham では 25.6%が含まれていた．割合としては単体の判定手法としては最も低いが，表 3.4 に示した通り，利用したドメイン数としては最も少なく，RFC5321.From を書き換えない legit SPF のドメイン数の方が 66 倍あり，効果を得やすい（受け取るべきメールをより送信している）メール送信元であるといえる．また，この legit SPF rewrite のドメイン名を併合（legit SPF new）したことで，既存の legit SPF の場合より 10%程度より多く受け取るべきメールを判定することができている．さらに，受け取るべきではない spam に対する誤判定割合は，0.2%と比較的少ない増加に抑えられている．これらのことから，メール転送時に SPF の認証ドメイン名を書き換える転送元を加えたことは，受け取るべき送信者レピュテーションの構築手法として有益であったと考える．

さらに，それぞれの受け取るべき送信者レピュテーションのデータについて，評価指標を用いて評価を行った．各分類は以下とした．

TP: 受け取るべきメール ham を受け取るべきメールと正しく判断できた（送信者レピュテーションを利用して判断できた）

FP: 受け取るべきではないメール spam を受け取るべきメールと誤って判断した（送信者レピュテーションに含まれていた）

FN: 受け取るべきメール ham を受け取るべきメールと判断できなかった（送信者レピュテーションに含まれていなかった）

これらの分類を用いて，Precision（適合率），Recall（再現率），F 値（F-score）を計算する．それぞれの計算式は以下の通りである．

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

$$F = 2\frac{Precision \cdot Recall}{Precision + Recall}$$

それぞれの送信者レピュテーションの評価指標値を表 3.7 に示す.

表 3.7: 送信者レピュテーションの評価指標

送信者レピュテーション	Precision	Recall	F 値
FW	0.9921	0.3138	0.4768
legit SPF	0.9987	0.3566	0.5255
legit SPF+FW	0.9941	0.4576	0.6268
legit SPF rewrite	0.9983	0.2558	0.4072
legit SPF new	0.9985	0.4622	0.6319
legit SPF new+FW	0.9948	0.5632	0.7193

この結果からも，より正確性を高めるためには FW を利用しないほうが良いことがわかる．しかしながら，FW を利用したことによる誤判定の影響は F 値からもそれほど大きく無いことがわかった．総合的には抽出した全ての分類を含めた，legit SPF new+FW を受け取るべきメールの送信者レピュテーションとして利用することが良いことが，評価指標から読み取れる．

3.4　考察

メールフィルタを利用して，受信メールを迷惑メール（spam）と迷惑メールでないメール（ham）とに分類し，それぞれの送信者を示す情報，IP アドレス，SPF 認証ドメイン名，DKIM 認証ドメイン名を利用して，送信者レピュテーションとしてどの程度利用できるのかについて調査した．またこれらの調査結果から，最近の迷惑メールの送信傾向について

も検討した．いずれの送信者情報についても，ham（受け取るべきメール）についてはある程度利用できるレベルの結果を得ることができた．しかしながら，spam については ham と比較して継続して利用できるような結果は得られなかった．このことから，迷惑メールの送信者は，できる限り対策されないよう送信者を識別できないように送信していることが推測できる．

メールフィルタを利用する手法は，ある程度の送信者レピュテーションのデータを集めるまで，メールフィルタを利用しなければならない．その収集期間では，本論文での提案手法の目的の 1 つである，メールフィルタの処理負荷を軽減するための送信者情報を利用した送信者レピュテーションの構築手法としては，不十分な手法かもしれない．送信者レピュテーションとしてのデータが十分に集まった段階では，メールフィルタに適用させるメールは限定的となるため，その時点では十分に目的を果たせていると考える．

これに対して，送信ドメイン認証技術を利用して転送メールの送信元から送信者レピュテーションを構築する本手法による提案は，メールフィルタの適用もメールの内容自体も確認する必要がない，迷惑メール対策としてはある意味では画期的な手法である．実際に，本手法の評価として，送信者レピュテーションの構築のために利用した情報は，メールの受信ログだけであった．つまり，本手法を利用して送信者レピュテーションを構築するためには，何か新しい装置やメールフィルタ等のシステムを必要とせず，なりすましメール対策としてほぼ必須となっているメール受信側での送信ドメイン認証処理を導入していれば，メールの受信ログあるいはそれと同等の情報があれば構築できることになる．つまり，現在利用しているメールシステムに対して，受信メールの記録を 1 度参照する程度の計算量の追加だけで，受け取るべき送信者レピュテーションを構築でき，その受け取るべき送信者レピュテーションに適用できた受信メール量（現時点で受信メールのおよそ半分）に対して，メールフィルタによる検査のために費やされる計算量を減らすことができることになる．また，送信者レピュテーションの参照に関する処理部分については，登録するドメイン名が増えれば参照にかかる時間が問題になる可能性がある．しかしながら，受け取るべきメール送信元のドメイン数については限定的であると考えいる．また受け取るべきでは無いドメイン名については，次々と新規のドメイン名を取得して利用することが予想されるが，定期的にドメイン名の存在や利用状況を確認することで，不要なドメイン名を保持しないなどの工夫も可能と考えている．

今回は，送信者レピュテーションの構築のための期間を 1ヶ月としたが，この処理を継続的に実施していくことで，受け取るべきメールをより多く判定できることも期待できる．

メールフィルタを利用する手法と送信ドメイン認証技術を利用する手法との比較

本論文では，送信者レピュテーションの構築手法として，メールフィルタを利用する方法と送信ドメイン認証技術を利用する方法の，2つのアプローチを示した．それぞれの手法については，上記で説明した通り評価の観点が異なるが，結果としてどちらが優れているかについても比較した．

送信ドメイン認証技術を利用した送信者レピュテーションの評価と同様に，メールフィルタを利用した送信者レピュテーションについても，2019年9月に受信したメールを利用して受け取るべき送信者レピュテーションを構築し，その後に受信したメールに適用して，それぞれの割合を比較する．

allow IPは，メールフィルタを利用して収集した受け取るべきIPレピュテーション，allow SPFは，同様のSPFレピュテーションである．これを送信ドメイン認証技術を用いたlegit SPF new+FWと比較する（表3.8）．

表 3.8: 送信者レピュテーションの比較

送信者レピュテーション	ham (%)	spam (%)	Precision	Recall	F 値
allow IP	58.8	0.6	0.9906	0.5884	0.7407
allow SPF	56.0	0.1	0.9998	0.5599	0.7178
legit SPF new+FW	56.3	3.0	0.9948	0.5632	0.7193

表3.8の結果では，それぞれの評価指標でわずかながらの差で異なる部分があるため，結果だけからはどれが優れたレピュテーションと判断するかは難しいが，送信者レピュテーションとしての構築の過程も考えれば，送信ドメイン認証技術を用いた本提案手法は，非常に優れた手法であるといえる．

送信者レピュテーションのさらなる改善

本論文で提案する送信者レピュテーションの構築手法は，ドメイン名を利用した受け取るべきメールの判定を目的としている．そこで，メールフィルタを利用したallow SPFと送信ドメイン認証技術を用いたlegit SPF newそれぞれのSPF認証ドメイン名について，併合した送信者レピュテーションを構築した場合について評価を行った．併合した送信者レピュテーションは，hybrid SPF = allow SPF ∪ legit SPF newである．今回は，IPアドレスによる送信者レピュテーションであるallow IPやFWを含んでいないレピュテーションである．同様の適用結果を表3.9に示す．

表 3.9: ドメイン名の送信者レピュテーションの比較

送信者レピュテーション	ham (%)	spam (%)	Precision	Recall	F 値
allow SPF	56.0	0.1	0.9998	0.5599	0.7178
legit SPF new	46.2	0.7	0.9985	0.4622	0.6319
hybrid SPF	74.3	0.8	0.9989	0.7432	0.8523

適用結果からは，ham から判断できた受け取るべきメールの割合，Recall, F 値が大幅に改善できることがわかった．特に ham から判断できた割合は，そもそも SPF 認証できた ham のメールの割合が 79.4%であるため，その大部分（SPF 認証できた ham の中では 97.3%）を判定できたことになる．送信側の SPF 認証がより進めば，より多くの受け取るべきメールを判定できるようになると考えている．

送信者レピュテーションの誤判定の改善と対策

本論文で示した，送信ドメイン認証技術を用いた送信者レピュテーションの構築手法は，メールフィルタによる手法と比較しても，spam を受け取るべきメールと判断する誤判定の割合が高い結果となった．転送元の IP アドレスである FW を利用しない場合でも，わずかな差だが高い結果となった．これは，転送メールも受け取るために送信者レピュテーションを構築したことが理由の 1 つになっていると考えている．これを改善するための手法について述べる．

1 つは迷惑メールを送信するために利用している SPF 認証ドメイン名を除外することである．迷惑メール送信者は，SPF の認証ができない（none）あるいは失敗するよりは，pass するほうがメール受信側に受け取ってもらえると考える場合がある．本研究でも，メールフィルタを用いた SPF レピュテーションの構築過程で，迷惑メールだけを送信する SPF 認証ドメイン名を収集し，受信メールに適用させた結果を示した．このようなドメイン名の SPF レコードには特徴がある場合がある．SPF の認証が pass するためには，メールの送信元 IP アドレスが，認証対象のドメイン名から取得した SPF レコード中に含まれていることが条件となる．しかしながら SPF レコードの記述方法の中には，広いネットワークレンジを登録したり，どこの送信元 IP アドレスであっても SPF 認証が pass するような設定もできる．一般的な SPF レコードの例を以下に示す．

```
v=spf1 +ip4:192.0.2.1 -all
```

SPF レコードは，DNS の TXT（テキスト）資源レコードという汎用的なレコードに記述

するため，SPF レコードであることを示す “v=spf1” という文字列から始まることになっている．それ以降，IP アドレスやネットワークアドレス，ホスト名などを記述して正規のメールサーバの IP アドレスを示す．各項の接頭語の “+” あるいは記号を省略した場合，それに続く IP アドレスにつながるホスト情報に適合した場合は SPF の認証結果は pass となる．逆に接頭語が “-” であるホスト情報に適合した場合認証失敗となる．正規のメールサーバ以外の意味で，SPF レコードの末尾に “all” を記述し，その接頭語に “-” をつけて “-all” とすることで，正規のメールサーバ以外は認証失敗であることを示す．この構文を悪用し，例えば “+all” という項を記述をすれば，どこからメールを送信しても pass する SPF レコードとなる．

```
v=spf1 +ip4:192.0.2.1 +all
```

こうした不正な SPF レコードを設定したドメイン名を利用してメール送信された場合で，そのメールが転送メールサーバを経由して届いた場合，その不正な SPF レコードが設定されているドメイン名を受け取るべき正規の SPF 認証ドメイン名と判断してしまうことになる．実際に，さまざまなドメイン名の SPF レコードを調べていく中で，こうした不正な SPF レコードを設定しているドメイン名が存在することがわかっている．SPF レコードで，不正に送信メールサーバを広げる手法としては，極端に広いネットワーク幅（ex. /8 など）を指定するような場合もある．実際に以前の研究では，転送元の IP アドレスから SPF 認証されたドメイン名を収集する過程で，迷惑メールだけを送信する SPF 認証ドメイン名を除外することで，ham のメールを受け取るべきと判断した割合が，わずかであるが減少させることができた．

もう 1 つの方法は，転送された迷惑メールを送信者情報を利用して判断して除外する方法である．メールフィルタを利用した送信者レピュテーションの構築手法として，SPF 認証ドメイン名や DKIM 認証ドメイン名を利用する手法を 3.1 節で示した．これもわずかではあるが，受け取るべきではない spam のメールを判定することができた．この SPF および DKIM の受け取るべきではないドメイン名のブロックリストを，メール受信時に適用することができれば，メール転送される迷惑メールを減らすことができる．以前の研究でも，spam を受け取るべきとする誤判定をわずかではあるが減らすことができた．

送信ドメイン認証を用いた送信者レピュテーションの構築手法は，送信ドメイン認証技術で SPF が fail し，DKIM が pass したメール送信元をメール転送の送信元として判断し，受け取るべきメールの送信元とする非常にシンプルな手法であるといえる．そのため，こうした手法で受け取るべきメールの送信元であると判断することを悪用することも考えら

れる．具体的には，わざとこうしたSPFとDKIMの認証パターンとなるようなメールを迷惑メールの送信サーバから送信することである．またメール転送時にSPFの認証ドメイン名を書き換える転送サーバと同じ認証結果となるような，メールを送信することで，同様に受け取るべきドメイン名に登録させてしまうことも考えられる．こうした悪用の手法の対策としては，いずれの手法でも，送信ドメイン認証技術によって認証されたドメイン名を利用しているので，それらドメイン名が不正なものであるかを判断する手法が考えられる．これも既に3.1節で示したように，SPFおよびDKIMの受け取るべきではないドメイン名のレピュテーションの構築手法を示した．これらのドメイン名をブロックリストとして，転送メールの判断時に利用すれば，不正なドメイン名によってメール転送元と判断してしまうことを防ぐことが期待できる．また，過去にメールの送信履歴が無く，新たに取得したドメイン名を利用して同様の悪用を行うような場合には，ドメイン名の履歴などをWHOIS等で参照し，新規のドメイン名についても，同様の抑制を行うなどの方法も考えられる．

さらに送信者レピュテーションの誤判定ではなく，spam判定されるメールが，実際に受け取るべき正規のメール送信元から送信される可能性も考えられる．これは，メール送信者（メールサービスの利用者）が，迷惑メール送信者である場合も考えられるが，正規のメールサーバが踏み台送信に悪用されている場合が考えられる．メールサーバの踏み台利用は，メール送信時に利用する認証情報（メールアドレスとパスワード）が何らかの手法で摂取され，実際のメール利用者ではない第三者（迷惑メール送信者）が悪用し，迷惑メールを誠意のメールサーバから送信するような手法である．送信者レピュテーションを効果的に利用していくためには，この正規のメールサーバの踏み台送信の対策を考える必要がある．このメールサーバの踏み台送信問題の対策として，フィードバックループの利用を提案する．その仕組みについて4章で述べる．

第4章　フィードバックループの提案

本章では，受け取るべき正規のメール送信元から送信される迷惑メールに対する対策として，フィードバックループの利用を提案する．送信者レピュテーション，特に受け取るべき正規のメール送信元をメールの受け取り判断に許可リストとして利用する場合，課題となるのがこの正規のメール送信元から送信される迷惑メールである．この正規のメール送信元から送信される迷惑メールは，正規のメールサーバを踏み台のように利用することから，踏み台送信攻撃とも呼ばれる．あるいは，メール送信に用いられるアカウントの認証情報が窃用されていると考えられることから，Compromised Account（アカウント情報の漏洩）問題ともよばれる．

フィードバックルーループおよびその関連技術（フィードバックメールの形式など）は，既に提案されているもので新しい技術ではない．しかしながら，あまり利用されていない背景には，フィードバック自体の重要性，つまりメール送信側のセキュリティ的な危険性が正しく理解されていないことが考えられる．また，フィードバックあるいは類似のシステムでの通知機能も含めて，それらが活用されていない背景には，フィードバック自体の情報の信頼性の問題があると考えている．本提案では，フィードバックを受け取るべきフィードバックの送り手を，送信ドメイン認証技術によって確認し，あらかじめ登録しておく仕組みを組み込むことで，受け取るフィードバック情報の信頼性を高める手法を提案する．また，フィードバックループ全体の信頼性を高める目的で，フィードバックすべき迷惑メール送信者を送信ドメイン認証技術を用いて認証させること，フィードバックを受け取らない迷惑メール送信者に不要なフィードバックを送らないために，フィードバック先をあらかじめ登録しておくことを提案する．

まず，踏み台送信攻撃が行われる背景と，その影響について述べる．次に踏み台送信攻撃について，メールの受信ログ情報を利用して検知する手法を示し，実際に適用することで，実際に正規のメールサーバから送信されていることを示す．これら，踏み台送信攻撃に対する対策として，より信頼性を高めたフィードバックループの仕組みを提案する．

4.1　踏み台送信

本節では，正規のメールサーバが迷惑メール送信に利用される，踏み台送信に関連したセキュリティ上の問題を述べ，対策すべき重要な課題であること示す．また，踏み台送信が行われていることを検知する手法を述べ，実際のメール受信ログを用いて踏み台送信が行われていることを示す．

4.1.1　踏み台送信攻撃の問題

一般に，メールサービスを利用してメール送信する場合，指定された送信用メールサーバに対して，メールアドレスなどの ID（Identifiation）とパスワードによる送信者認証（SMTP-AUTH[1]）が必要となる．MUA などのメールソフトウェアを利用している場合は，設定で ID やパスワードを登録すれば，メール送信時に自動的に SMTP-AUTH が実行される．メールサービス事業者は，これら認証の記録とともにメール送信の記録をログ情報として一定期間保管している．

メールの踏み台送信は，このメール送信時の認証情報が，なんらかの手段で摂取されたり，簡単なパスワード設定によって類推されたなどで窃用され，迷惑メール送信に悪用される不正行為である．または，迷惑メール送信を目的にメールサービスの契約を行い，受け取ってもらうために正規のメールサーバから迷惑メールを送信するような行為も考えられる．いずれにしても，正規の送信元から送信される迷惑メールは，送信ドメイン認証技術にも pass するためなりすましメールとして対策もできず，送信者レピュテーションによって逆に届けられる可能性の高い，メール受信側の対策が難しい送信手法である．

メール送信時の認証情報が摂取されている場合，問題は迷惑メール送信にとどまらない．メール送信に利用する認証情報は，受信したメールの参照時（POP や IMAP などのプロトコルを利用）にも利用される場合が多い．そのため受信メールを参照され，何らかのビジネス上の取引のメールを見つけることで，取引先を騙すようなメールを送信する BEC（Business Email Compromise）へと発展する可能性もある．

米国 FBI のレポート [35] によれば，2021 年に IC3[2]に報告があった BEC の被害は 19,954 件で，調整後の損失は 24 億米ドル近くであったと報告されている（表 4.1）．この被害額は，フィッシングや投資詐欺（Investment）などより分野別で最も多い被害額であった．さらに正規のメールサーバを踏み台にして送信することにより，受信者を信頼させ，不正プ

[1]SMTP Service Extention for Authentication, RFC2554
[2]Internet Crime Complaint Center

表 4.1: FBI Internet Crime Report 2021 より

Crime Type	Victim Loss (USD)	Victim Count
BEC/EAC	2,395,953,296	19,954
Investment	1,455,943,193	20,516
Confidence Fraud/Romance	956,039,740	24,299
Personal Data Breach	517,021,289	51,829
Real Estate/Rental	350,328,166	11,578
Tech Support	347,657,432	23,903
Non-Payment/Non-Delivery	337,493,071	82,478
Identity Theft	278,267,918	51,629
Credit Card Fraud	172,998,385	16,750
Corporate Data Breach	151,568,225	1,287
...	...	...
Phishing/Vishing/Smishing/Pharming	44,213,707	323,972

ログラム（マルウェア）に感染させるなど，更なる被害を増やす要因にもなる．そのため，正規メールサーバの踏み台送信は，単なる迷惑メール送信だけにとどまらず，さまざまなセキュリティ被害に発展する可能性のある，対策すべき不正行為である．

しかしながら，メールの送信側では迷惑メールが送信されていることを検知することは一般に難しい．メールの送信時にメールフィルタを適用させて迷惑メールが送信されているかを確認する手法もあるが，新たなメール設備も必要となるため，実際にはあまり行われていない対策である．メール受信側も，迷惑メール送信者にメールの到達状況を伝えるような，受け取らなかったことを示すエラーコードを返すことも少なくなった．そのため，別途メール受信側からの迷惑メールが届いたことの通知を行う，フィードバックループの仕組みが必要とされているが，利用のためには改善すべき幾つかの課題もある．

4.1.2 踏み台送信の検知手法

本節では，受信したメールの中で，正規のメールサーバから送信された迷惑メール，つまり踏み台送信が行われているのかを確認する手法について述べる．

踏み台送信が行われているとすれば，正規のメール送信者から迷惑メールが送信されていることになる．つまり，送信者レピュテーションの評価（3.3.2 節）での表 3.6 の spam 部分にも含まれているはずである．正規のメール送信元には，転送メールの送信元も含まれているため，受信したメールが迷惑メールであっても，転送された迷惑メールである可

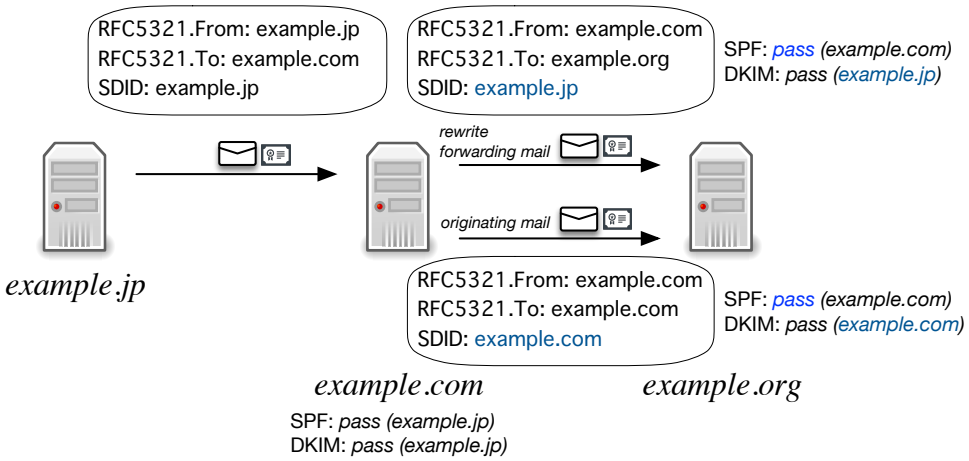

図 4.1: 転送メールと直接送信メールの送信ドメイン認証

能性もある．踏み台送信が行われていることを示すには，受信したメールが迷惑メールであって，その送信元が正規のメール送信元であって，かつ転送メールでないことを示す必要がある．転送されたメールかどうかは，転送の方法（RFC5321.From を書き換えるかどうか）にもよるが，3.3.1 節で述べた通り，それぞれの転送方法に応じた判断手法がある．

つまり，メール転送時に SPF の認証ドメイン名である RFC5321.From を書き換えない通常のメール転送の場合，転送先では SPF 認証が失敗する．メール転送時に SPF の認証ドメイン名である RFC5321.From を書き換えるメール転送の場合，転送先では SPF 認証が pass するが，DKIM の認証 pass だった場合に，DKIM 認証ドメイン名を確認することで区別することができる．

図 4.1 に示した通り，`example.com` からのメールを受信した場合，いずれも SPF の認証は pass し認証ドメイン名も `example.com` と同じであるが，転送メールであって元々の送信元が DKIM 認証に対応していた場合，DKIM の認証ドメイン名は受信時の送信元のドメイン名 `example.com` ではなく，無関係の `example.jp` ドメイン名となるはずである．一方，メール送信元の `example.com` が DKIM 認証に対応していれば，受信時の DKIM 認証ドメイン名は，SPF 認証ドメイン名と同じ `example.com` となるはずである．よって，転送メールではなく送信元のメールサーバから直接送信されたメールであるかを判断するためには，以下の条件に適合していれば，直接送信されたメールであると考えることができる．

- SPF 認証が pass である
- DKIM 認証が pass であり，DKIM 認証ドメイン名が SPF 認証ドメイン名と同じか同じ管理元のドメイン名である

受信したメール全てが，SPF および DKIM に対応したメールであるとは限らないため，この条件だけで全ての受信メールが直接送信されたメールであるかは判断できないが，少なくともこの条件に適当しているメールは，転送メールではなく直接送信されたメールと考えることができる．SPF と DKIM のそれぞれの認証ドメイン名が同じ管理元であるかを判断するために，送信ドメイン認証技術 DMARC の認証方法と同じ手法，同じドメイン名かそれぞれの組織ドメイン名が同じである場合，とした．組織ドメイン名の考え方は，2.1 節で述べた．この条件に適合し，迷惑メールと判断されるメールは，その送信元から直接送信された迷惑メールであると判断することができる．

4.1.3 踏み台送信の検出

正規のメール送信元からの受信メールの中で，迷惑メール（spam）であって，転送メールではなく直接送信されたメールがあるかを調べた．正規のメール送信元については，3.3.1 節で構築した，2019 年 9 月の 1ヶ月間に受信した約 3 億 4 千万通の受信メールによる送信者レピュテーションを利用した．これを 2019 年 10 月 1 日から 1 週間に受信した約 3 千 6 百万通の受信メールに適用した結果を利用して，spam 判定されたメールに適合したメールについて，直接送信されたメールであるかを調べた．

表 3.6 では幾つかの送信者レピュテーションの組み合わせを適用させたが，ここでは転送元 IP アドレスと正規の SPF ドメイン名からブロックすべき SPF ドメイン名を除いた，(3) の送信者レピュテーションを適用させた結果を用いた．この適用結果では，spam 判定されたメールのうち 3.25%が正規のメール送信元から送信されたメールであった．この中で，直接送信されたメールがどの程度あるかを調べた．それぞれの手順の段階毎に抽出した結果を表 4.2 に示す．

表 4.2: 踏み台送信メールの抽出

条件番号	メール抽出条件	spam での割合 (%)
(i)	送信者レピュテーションに適合	3.25
(ii)	spam の中で SPF および DKIM 認証が pass	2.52
(iii)	(ii) の中で SPF と DKIM 認証の組織ドメイン名同じ	2.32
(iv)	(i) であって (iii) である割合	0.23

表 4.2 の中で，(ii) の割合が 2.52%と少ないのは，迷惑メール自体が SPF と DKIM の両方の送信ドメイン認証に対応することが少ないことを示している．送信ドメイン認証によって，迷惑メールのドメイン名が識別できてしまえば，その認証ドメイン名自体を受け取ら

ないことで対策ができてしまう．にもかかわらず，迷惑メールが送信ドメイン認証に対応している理由は，送信ドメイン認証によってなりすましメールと判断されるほうがまだ受け取られないと考えているか，踏み台送信によって正規のメールサーバが悪用されている場合と考えられる．このことは，(iii) の割合が (ii) の割合と近いことからも推測できる．つまり，迷惑メール送信者が SPF および DKIM の送信ドメイン認証に対応しようと考える場合，それぞれ別の認証ドメイン名を利用することは考えにくく，同じ認証ドメイン名を利用する可能性が高いと考えられる．また，踏み台送信の場合でも，正規のメールサーバを利用しているのであれば，SPF と DKIM の認証ドメイン名も同じドメイン名，少なくとも同じ組織ドメイン名となるはずである．これは，DMARC 対応のためにも必要な条件であるため，転送メールではない直接送信されたメールであれば，なるべく SPF と DKIM の両方の送信ドメイン認証に対応させたいと考えるはずである．この中で踏み台送信である可能性が高いメールは，(iv) の送信者レピュテーションに適合し，SPF と DKIM の認証が pass し，かつその認証ドメイン名が同じ組織ドメイン名である場合である．SPF の認証ドメイン名である RFC5321.From を書き換えない通常の転送メールではないことは，SPF の認証が pass していることから明らかである．RFC5321.From を書き換える転送元からの転送メールでないことは，SPF と DKIM の認証ドメイン名が同じ管理元（同じ組織ドメイン名）であることから推測できる．よって (iv) のメールは，転送メールではなく受信時の送信元から直接送信されたメールであって，送信者レピュテーションによって正規のメール送信元からの迷惑メールである可能性が高いといえる．

(iv) の割合が 0.23%と低い理由は，そもそも迷惑メールの中で，SPF と DKIM の両方に対応したメールが 2.52%と少ないことが理由と考えられる．同じ期間で，迷惑メールでない ham と判定されたメールで，SPF と DKIM の両方の送信ドメイン認証の結果が pass だったメールの割合は，39.7%であった．踏み台送信メールの調査対象となったメール量自体が少ないため，検知できた踏み台送信メール自体も少ない結果となったと考えられる．調査対象である表 4.2 の (iii) に対する (iv) の割合としては，10.0%であり，送信ドメイン認証に対応していない送信元からの踏み台送信メールを考えると，0.23%という割合ではなく，より多く送信されてていると推測できる．今回の調査で，少なくとも踏み台送信による迷惑メールが 0 ではなくある程度存在することを示すことができた．

4.2 フィードバックループの提案

正規のメール送信元からの迷惑メール対策としては，メール受信側からメール送信側へ迷惑メールが送信されていることを伝えることが必要である．既に述べた通り，メールの送信側では，送信したメールが通常のメールであるか迷惑メールであるかの検査をしているメールサーバは少なく，一般的にメールの送信側では把握できないからである．そのため，メールが届いたメール受信側でメールを判断し, 迷惑メールの場合はメール送信側に通知することが必要になる．こうした通知の仕組みがない場合，メール送信側では踏み台送信対策が行われず，迷惑メールが送信し続けるため，メール受信側の対策としてこうした踏み台送信するメール送信元をブロックリスト等で受け取らない，といった対策をする可能性もある．こうした状況が続けば，メールの疎通はますます悪くなり，メール自体が使われなくなる可能性もある．

本節では，フィードバックループがどの様に踏み台送信対策となりえるのかについて述べ，フィードバックループを実現する上での要件について検討し，どの様にフィードバックループの仕組みを実現すべきなのかについて述べる．

4.2.1 フィードバックループの仕組み

メール送信側では，メール送信時に利用された認証情報とともに，通常メールの送信記録がログとして一定期間保存される．つまり，どの送信メールが迷惑メールであったかが把握できれば，そのメールの送信時の認証情報から，どのメール利用者が送信したのかを把握することができる．迷惑メールを送信したメール利用者が確認できれば，実際に迷惑メールを送信したのか，誰かに認証情報を窃用されたのかを確認することもできる．また，メール送信時の接続元 IP アドレスを確認することでも，認証情報が窃用されている可能性を推測することができる．IP アドレスは，それが利用されている（割り当てられている）国情報などを調べることができる．例えば，短時間で物理的に移動が難しい複数の国地域からメールが送信されている場合，メール送信時の認証情報を誰かと共有していないとすれば，窃用されている可能性が高いと推測することができる [42]．マルウェアに感染させられた PC（ボット）を利用して，迷惑メール送信を行う行為が，一般利用者が利用する動的 IP アドレスからの直接メール送信が OP25B[3][18] といった対策の普及で難しくなったことから，正規の送信メールサーバを悪用する手法が利用されるようになってきている．

[3]Outbound Port 25 Blocking

メール送信側では，こうしたメール送信時の認証情報が窃用されていることがわかれば，一時的に認証をできないようにし，その認証情報を利用したメール送信をできないようにすることができる．その間，メール利用者に連絡をとり，メール送信時の認証情報が利用できない様にしていることを伝えつつ，認証情報のパスワードの変更を促したり，利用している PC がマルウェアに感染していないか，アンチウイルスソフトウェアの実行をお願いするなどの対策を講じることができる．こうしたメール利用者側での対策を行ったことを確認して，メールの送信時の認証の利用を再開させる．このように，どの送信メールが迷惑メールであったかがわかれば，メール送信側では同じ様な手法で迷惑メールが送信できない様に対策をすることができる．課題は，どの様に迷惑メールが送信されていることを伝えるかである．

メールの受信者が，メール送信側に迷惑メールを受信したことを通知する仕組みは，メールの業界内でも議論が行われ [14]，メールで通知するためのフォーマットが ARF（Abuse Reporting Format）として規格 [32][13] が作られた．ARF 形式は，受信した元のメールをいわゆる添付ファイルと同じ形式の MIME（Multipurpose Internet Mail Extensions）で取り込み，メール運用者へ通知の目的とともに送信する．メールが ARF 形式であることを，メールヘッダの `Content-Type:` で `multipart/report; report-type=feedback-report;` と設定し，レポートの種類（`report-type`）が `feedback-report` であると指定することで，マルチパートのメールであり，ARF 形式のフィードバックであることを示す．以下に，ARF 形式のフィードバックの例を示す．

```
From: <abusedesk@example.com>
Date: Thu, 8 Mar 2005 17:40:36 EDT
Subject: FW: Earn money
To: <abuse@example.net>
MIME-Version: 1.0
Content-Type: multipart/report; report-type=feedback-report;
     boundary="part1_13d.2e68ed54_boundary"

--part1_13d.2e68ed54_boundary
Content-Type: text/plain; charset="US-ASCII"
Content-Transfer-Encoding: 7bit

This is an email abuse report for an email message received from IP
192.0.2.1 on Thu, 8 Mar 2005 14:00:00 EDT. For more information
about this format please see http://www.mipassoc.org/arf/.

--part1_13d.2e68ed54_boundary
Content-Type: message/feedback-report

Feedback-Type: abuse
User-Agent: SomeGenerator/1.0
Version: 1

--part1_13d.2e68ed54_boundary
Content-Type: message/rfc822
Content-Disposition: inline

Received: from mailserver.example.net (mailserver.example.net [192.0.2.1])
  by example.com with ESMTP id M63d4137594e46;
  Thu, 08 Mar 2005 14:00:00 -0400
From: <somespammer@example.net>
To: <Undisclosed Recipients>
Subject: Earn money
MIME-Version: 1.0
Content-type: text/plain
Message-ID: 8787KJKJ3K4J3K4J3K4J3.mail@example.net
Date: Thu, 02 Sep 2004 12:31:03 -0500

Spam Spam Spam
Spam Spam Spam
Spam Spam Spam
Spam Spam Spam
Spam Spam Spam

--part1_13d.2e68ed54_boundary--
```

まず，通常のメールと同様にメールヘッダから始まり，メール本文とは空行で区切られる．メールヘッダに`MIME-Version:`ヘッダと`Content-Type:`ヘッダがあることから，MIME形式メールであることがわかる．各MIMEパートは，境界を示す文字列（boundary）で区切られる．最初のパートは，人間が読むための情報であり，この例では迷惑メール（spam）が送られたことによるabuseレポートであることを記述している．二つ目のパートで，機械的にレ

ポートの種類がわかるようなMIMEヘッダが記述されている．この例では，Feedback-Type: abuse と記述されていることから，フィードバックの種類が abuse であることがわかる．三つ目のパートで，実際に送られてきた迷惑メールの内容が示される．

フィードバックの種類として，現在は以下が定義されている．迷惑メールが送られてきたことをフィードバックするためには，例と同様に abuse タイプを指定する．

表 4.3: フィードバックの種類

Feedback-Type	意味
abuse	未承諾メールやその他のメールの悪用
fraud	ある種の詐欺やフィッシングなどを示す
other	他の登録タイプに当てはまらないその他のフィードバック
virus	元のメッセージでみつかったウイルスのレポート
auth-failure	メール認証失敗報告

この様に，送られてきたメールに関する情報，特に受け取った時のメールヘッダ情報があれば，送信された日時や送信元 IP アドレス，送信者のメールアドレスなどを取り出すことができる．これら取り出した情報を用いて，送信メールサーバのログ情報を参照し，実際に送信されたメールであるかどうかを確認することができる．該当する送信メールの情報があった場合，その送信に用いられた認証情報を取り出し，利用ユーザを特定し，各種対策を講じるといった対応を行うことで，踏み台送信を防ぐことができる．

次に，フィードバックを含めた実際のメールの流れを説明する（図 4.2）．(1) メールの利用者は，メール送信時に送信者認証（SMTP-AUTH）を行い，送信メールサーバを利用して送信する．この認証のための情報は，送信側のメールシステムで一般的に管理されている．(2) 送られたメールがメール受信側に届き，メール受信者が当該メールを参照し，迷惑メールと判断した場合，ウェブメールなどのインターフェースを通じて迷惑メールであることを受信側メールシステムに報告する．(3) 受信側のメールシステムでは，報告された迷惑メールの送信者を特定し，その送信メールシステムの管理元に対してフィードバックを行う．このフィードバックは，ARF 形式で行われ，メール受信者から報告された迷惑メールを含む MIME 形式で送信側に送信される．メール送信側では，届いたフィードバックのメールを参照し，フィードバックの種類を取り出し，報告された迷惑メールを参照する．報告された迷惑メールの情報から，(4) 実際に送信したメールであることがわかれば，メール送信時の認証情報にアクセスし，一時的に認証を停止するなどの一時的な対応を行う．これら一連の対応処理は，こうした対応をあらかじめ想定している場合は，メールが ARF 形式で決まっているため，ある程度機械的に処理することも可能である．メール送信

側が，こうした処理を迅速に行うことで，迷惑メール送信がもたらす被害の拡大を防ぐことができる．

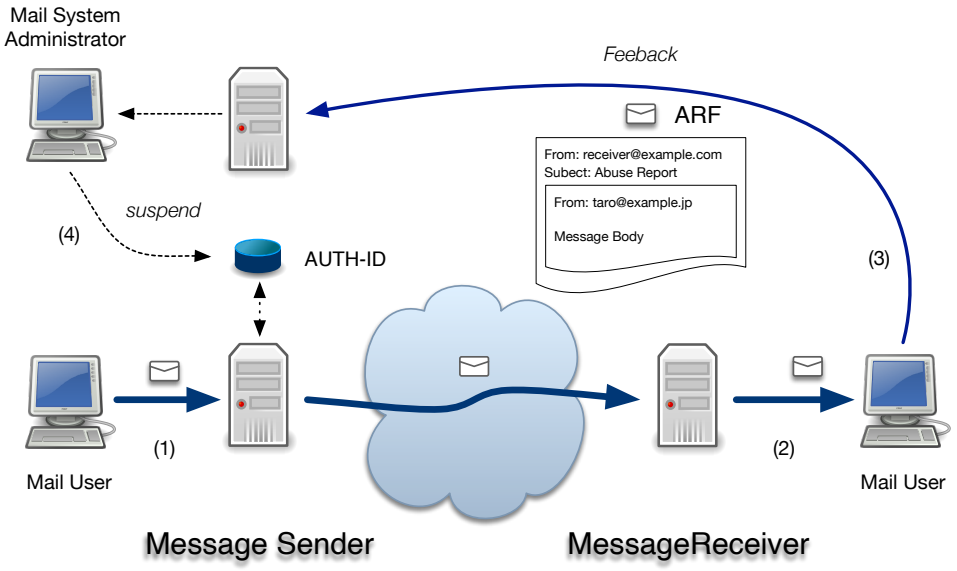

図 4.2: フィードバックループの流れ

このように，一旦送信されたメールが，フィードバックによってメール送信側に戻ることから，これら一連の対策のためのメールの流れは，フィードバックループと呼ばれる．

4.2.2 送信ドメイン認証を用いたフィードバックループ

フィードバックループを実現する上で重要なことは，正しく最初のメール送信元が認識できること，その送信元がフィードバックを受け取る送信元であるかを判断できることである．受け取ったメールの送信者を正しく認識できなければ，フィードバックすべき相手を判断できず，また誤ったフィードバック先に受信メールを送信することがあれば，迷惑メールであっても第三者にメールが送信されたこと，そのメールが受信側に届いたことを伝えてしまうことになる．誤ってフィードバックを送信される受け取る方にとっても，フィードバック自体が不要な迷惑メールと受け止められる可能性もある．

メールの送信者を正しく認識するためには，メール受信時に送信ドメイン認証によって送信元を確認することである．同様にフィードバックを受けるメール送信側にとっても，フィードバックが間違いなく送信された迷惑メールの情報であることが重要である．例えば，虚偽のフィードバックが多く寄せられるようであれば，フィードバック自体が信用できない情報と捉えられ，たとえそのフィードバックの中に正しい情報があったとしても，対

策に活用されなくなってしまうかもしれない．フィードバックを受けるメール送信側にとっても，フィードバック元が信頼できるメール受信者であるかを，送信ドメイン認証によって確認することが考えられる．

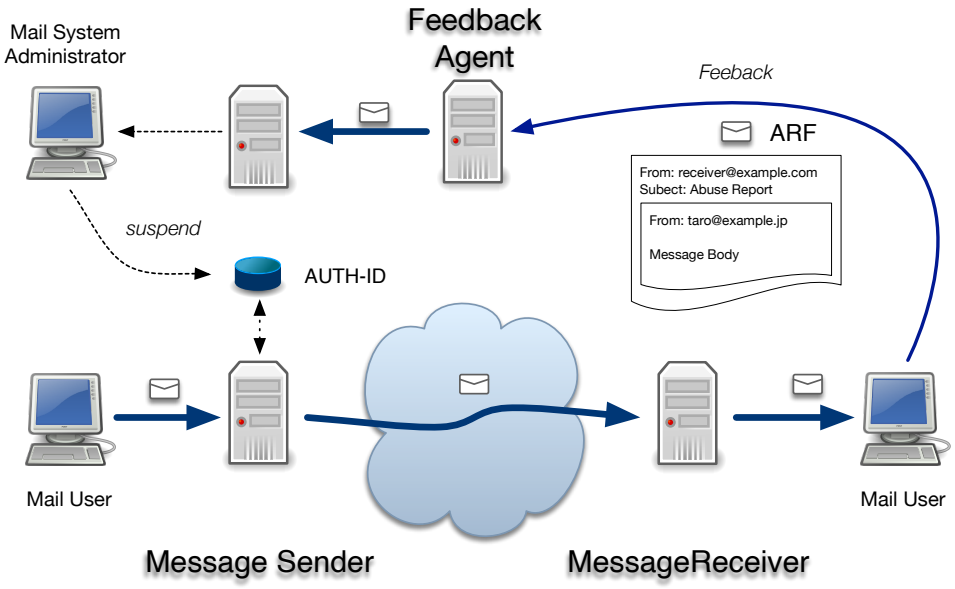

図 4.3: 仲介者を含むフィードバックループの流れ

こうした課題を解決するため，メール受信側からメール送信者へフィードバックを直接送信せず，フィードバックの仲介を信頼できる第三者（Feedback Agent）を経由して送信する手法の提案がある [52]．概要を図 4.3 に示す．フィードバックを送信するメール受信側は，フィードバックの送信先を気にすることなく，仲介者（Feedback Agent）に全て送信する．仲介者がフィードバックされた迷惑メールを確認し，適切なフィードバック先が存在する場合にフィードバックを送信する．フィードバック先を判断するために，最初の受信者（フィードバック元）による送信ドメイン認証の結果を利用する．フィードバックを受け取るメール送信側は，フィードバックを送信する仲介者からのメールだけを受け取る．これにより，フィードバック送信者もフィードバックの受信者も仲介者だけを信頼することで，信頼できるフィードバックループを構成することができる．仲介者は，フィードバックの送信元（メール受信側）とフィードバック先（メール送信側）をそれぞれ増やしていくことで，より多くのフィードバックループを構成することができる．

本論文では，もう一つの手法として，仲介者を介さずに直接メール受信者（フィードバック元）がメール送信者（フィードバック先）にフィードバックする，フィードバックループを提案する．本手法では，転送されたメールのフィードバック先は，メール受信時の送

信者ではなく最初のメール送信者であるため，これを適切に判断するする手法についても述べる．これらを整理し，フィードバックループを機能させるために必要な要件を以下に述べる．

1. 受信したメールが送信ドメイン認証によってメールの送信元がどのドメイン名であるかが判断できる
2. 受信したメールが，メール転送されたものではなく，直接送信されたメールであることが判断できる
3. メールの送信ドメイン名からフィードバックを送信する宛先がわかる
4. フィードバックを受け取るメール送信元は，フィードバックの送信元が送信ドメイン認証技術で認証できる
5. フィードバックを受け取るメール送信元は，フィードバックの送信ドメイン名から受け取るべきかを判断できる
6. フィードバックを受け取るメール送信元は，フィードバックされたメールから送信したメールおよび送信時に用いられた認証情報を抽出できる

受信したメールが，迷惑メールなどフィードバックすべきメールであった場合，その送信者を正しく認識できることが重要となる．誤った送信者を認識してしまった場合，誤ったフィードバック先に通知が行われることになり，そうしたことが頻発すれば，フィードバックループ自体の信頼性が損なわれる．フィードバックループが信用されなくなれば，メール送信側とメール受信側の双方にとって必要な情報が伝わりにくくなり，踏み台送信対策が進まないことにもつながる．そのためフィードバックループの信頼性を高めるためには，メールの送信者を送信ドメイン認証によって正しく認識することが必要となる．送信者を判断するための送信ドメイン認証技術は，メールの配送経路によらない電子署名方式の DKIM による認証が望ましいといえるが，ネットワーク方式の SPF であっても，転送メールの取り扱い，特に転送時に RFC5321.From を書き換える転送元を識別できれば，送信元の判定にも十分に利用できる．総合的には，DMARC による認証がメール送信元を認識する手法として望ましいが，DMARC で認証できるメールの割合を増やす必要がある．送信ドメイン認証技術は，メールの送信者をドメイン名単位で認証するため，フィードバックの宛先もドメイン名単位での対応となる．

フィードバックを受けるメール送信側は，まずフィードバックの送信元が受け取るべきフィードバック元であるかを確認する必要がある．フィードバックはメールで送信されるため，メールアドレスが判明すれば様々なメールが送信される可能性がある．その中でフィードバックであるメールを抽出し，さらに受け取るべきフィードバック送信者（メール受信者）かを判断する必要がある．これらの判断にも送信ドメイン認証を利用する．フィードバックの送信者を認識し，そのメールが ARF 形式であるか，必要な情報が含まれているかを確認する．

メール送信側は，受け取ったフィードバックから，送信された迷惑メールのヘッダ情報などから送信メールを抽出するために必要な情報を抽出する．これらの情報から実際にメールが送信されていること，その送信に用いられた認証情報を抽出し，利用ユーザを特定する．

これらのフィードバックループの流れの中で，重要となるのはフィードバックの送り先の確認と，フィードバックを受け取る側のフィードバック送信者の確認である．これらの機能を備えた送信ドメイン認証を用いたフィードバックループの実現例を図 4.4 に示す．

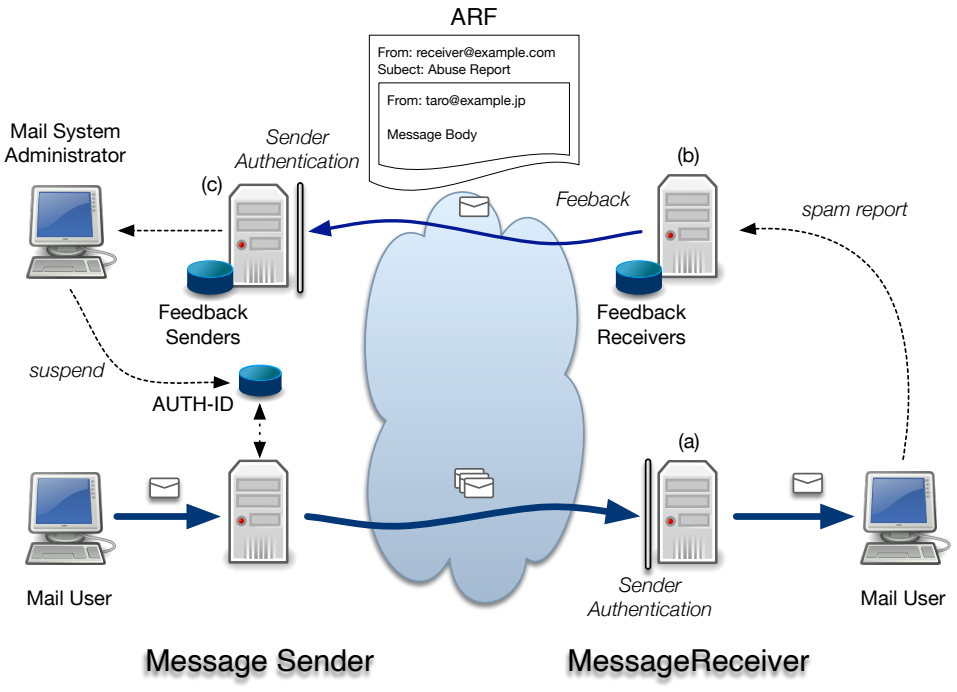

図 4.4: 送信ドメイン認証を利用したフィードバックループ

まずメールの受信側は，メール受信時に受信メールサーバ (a) で送信ドメイン認証を行う．送信ドメイン認証は，SPF, DKIM, DMARC それぞれで認証する．メールの受信者は受信したメールを確認し，もし迷惑メール（spam）が含まれていれば，ウェブメールなどで迷惑メール報告ボタン等で申告する（spam report）．spam 報告を受けたフィードバッ

クループのサーバ (b) は，受信時の送信ドメイン認証の結果から，送信側のドメイン名を取得し，フィードバック先（Feedback Receivers）が存在するかをデータベース等で確認を行う．フィードバック先が存在していれば，送信されたメールを ARF 形式でフィードバックのメールを構成し，フィードバック先へメール送信する．フィードバックを受け取ったメール受信サーバ (c) は，メール受信時に送信ドメイン認証（SPF, DKIM, DMARC）を行い，フィードバックの送信元ドメイン名を抽出する．フィードバックの送信元ドメイン名が得られたら，それが受け取るべきフィードバック元（Feedback Senders）であるかをデータベース等で確認する．受け取るべきフィードバック送信元であった場合，ARF 形式のフィードバックされたメールから，元の送信メールを取り出し，その受信時の送信ドメイン認証の結果を確認する．送信ドメイン認証の結果は，`Authentication-Results:` ヘッダに記載することになっているため，そのヘッダ情報からフィードバックの理由となったメールが，実際に送信されたメールであるのか,，自ドメインから送信されたのかを確認する．確かに自ドメインから送信されたメールであることが確認されれば，そのメールヘッダ等からメールの送信日時や送信者などの情報を取得する．送信メールサーバのログから実際に送信に利用された認証情報を抽出し，メール送信者のユーザ情報を取得し，必要に応じて認証の一時停止やメール利用者への連絡，認証パスワードの変更等の対応を行う．迷惑メール送信を意図して契約した利用者だった場合は，約款等に従い契約を解除するなどの対応を行う．これらの処理によって，迷惑メールの踏み台送信が当該認証情報を利用して行われないよう対策をする．

4.3 評価

送信ドメイン認証の結果を利用して，受信したメールが転送メールによるものではなく，送信元のメールサーバから直接送信されたメールであることを判断する手法を示した．この手法を実際に受信したメールのログ情報に適用させ，3 章で構築した受け取るべき送信者レピュテーションを利用した結果，迷惑メール判定されたメールが送信元のメールサーバから直接送信されていることを示すことができた．これにより，実際に正規のメールサーバを踏み台利用した迷惑メール送信が行われていることがわかった．送信ドメイン認証技術に対応したメール，特に迷惑メールに関してはあまり多く無いために，検出できた踏み台送信を多くは検出できなかったが，それでも実際に送信されたメールの中で検出できたことは重要であると考える．

迷惑メールの踏み台送信に関わるセキュリティ的な問題は大きいため，こうした踏み台

送信を検出し，対策していくことは重要である．本論文では，送信ドメイン認証技術を利用し，フィードバック送信側と受信側双方が確認できる仕組みを備えたフィードバックループの仕組みを提案した．この仕組みにより，フィードバックされる通知される迷惑メール送信の情報の信頼性を高め，迷惑メールの踏み台送信の対策が進むことが期待できる．

4.4　考察

メール受信側からメール送信側に対して，迷惑メールやフィッシング，ウイルスが添付されているメールの情報を伝える ARF 形式の通知は，現在も含めて特定のメールサービス事業者間以外では，あまり利用されてこなかった．その理由としては，まず通知先が明確であるのか，通知を送信して対応できる信頼できる相手であるかが不明であった点がある．既に述べたように，これまでメールの送信者情報は基本的に信頼できない情報であり，特にフィッシングなど迷惑メールなどではほぼ詐称されているため，通知先としては適さない情報であった．そのため，迷惑メールの送信元の IP アドレスをインターネット上の WHOIS データベースで検索し，不正行為などを連絡する abuse のメールアドレスに連絡する，といった方法がとられていた．以下に，WHOIS データベースを検索した例を示す．この中で，“`o.[Abuse]`” の項目が abuse の連絡先メールアドレスである．

```
$ whois -h whois.nic.ad.jp 192.41.192.145 | nkf
[ JPNIC database provides information regarding IP address and ASN. Its use   ]
[ is restricted to network administration purposes. For further information,  ]
[ use 'whois -h whois.nic.ad.jp help'. To only display English output,        ]
[ add '/e' at the end of command, e.g. 'whois -h whois.nic.ad.jp xxx/e'.      ]

Network Information: [ネットワーク情報]
a. [IP ネットワークアドレス]     192.41.192.0/24
b. [ネットワーク名]              JPNICNET
f. [組織名]                      一般社団法人 日本ネットワークインフォメーションセンター
g. [Organization]                Japan Network Information Center
m. [管理者連絡窓口]              SS54384JP
n. [技術連絡担当者]              YK11438JP
n. [技術連絡担当者]              EK6175JP
n. [技術連絡担当者]              AS5496JP
n. [技術連絡担当者]              TK74577JP
o. [Abuse]                       hostmaster@nic.ad.jp
p. [ネームサーバ]                ns3.nic.ad.jp
p. [ネームサーバ]                ns5.nic.ad.jp
[割当年月日]                     1993/02/01
[返却年月日]
[最終更新]                       2022/08/29 20:59:02(JST)

上位情報
----------
該当するデータがありません。

下位情報
----------
該当するデータがありません。
```

しかし，こうしたabuseのメールアドレスを公開することで，逆に迷惑メールが大量に送信されるなど，連絡窓口として機能しづらい状況も発生してきている．さらにこうした状況から，abuseの連絡が簡単にできないような仕組みとしたり（ウェブフォームのみを連絡窓口とする等），abuseの問い合わせ先を正しく設定しない回線利用者も増えている．

メールでは，送信ドメイン認証技術が普及し利用できるメールが増えたことにより，認証されたドメイン名をメールの送信者をとして利用できるようになってきた．この認証された送信ドメイン名を活用し，フィードバックループの信頼性をより高めてようとするのが本手法の特徴である．フィードバックの送信者と受信者間で，相互に信頼できる情報を通知できる本手法の枠組みを実現することで，迷惑メール送信を検知し，メール送信側で

メール送信の認証情報の漏洩を対策でき，迷惑メールを送りにくくする環境を実現することが期待できる．

第5章　送信者レピュテーションとフィードバックループによるメールシステム

本章では，これまで述べた送信ドメイン認証を利用した，送信者レピュテーションとフィードバックループを利用したメールシステム（図 5.1）について述べる．

メール送信側では，送信ドメイン認証技術に対応し，メール受信側で送信ドメイン名を認証できるように設定する．導入する送信ドメイン認証技術は，SPF, DKIM, DMARC 全てを導入することが望ましい．これによりメール送信先で別のメール宛先にメール転送された場合でも，転送先で DKIM あるいは DMARC によって，最初のメール送信者を識別できるようになる．また，メール送信時には送信者認証（SMTP-AUTH）による認証を行い，この送信者認証時の送信者 ID 情報とともに送信メールサーバの送信ログに保存する．

メール送信側として，フィードバックを受け取るためのメールアドレスとメール受信サーバを用意する．このフィードバック受信サーバでは，受け取るべきフィードバック元のドメイン名のリスト（Feedback Senders）をデータベース等で保持する．メールによるフィードバックを受信した場合，そのメール送信者を送信ドメイン認証技術で認証を行う．送信ドメイン認証技術で認証されたフィードバックは，その認証ドメイン名が Feedback Senders 含まれているかを確認し，含まれている場合には，フィードバックの ARF 形式のメールから，送信された迷惑メールを取り出し，そのヘッダ部分から受信時の送信ドメイン認証の結果（`Autentication-Results:` ヘッダ）と，受信時の時間等を `Received:` ヘッダなどから取り出す．これらの情報から，確かに送信された迷惑メールであることを確認できた場合，送信メールサーバのログ情報から，メール送信に利用された送信者認証 ID を確認し，メール利用者を特定する．状況に応じて，メール送信の送信者認証が許可されないよう認証 DB 等を設定する．これにより，当該送信者認証 ID によるメール送信が一時的にできなくなり，これ以上迷惑メール送信ができなくなる．この間，迷惑メールが送信された理由を調査し，送信者認証のパスワードを変更したり，メール利用者の PC のウイルス検査を

実施するなどの対応を行い，メール送信が行えるよう認証 DB の設定を行う．

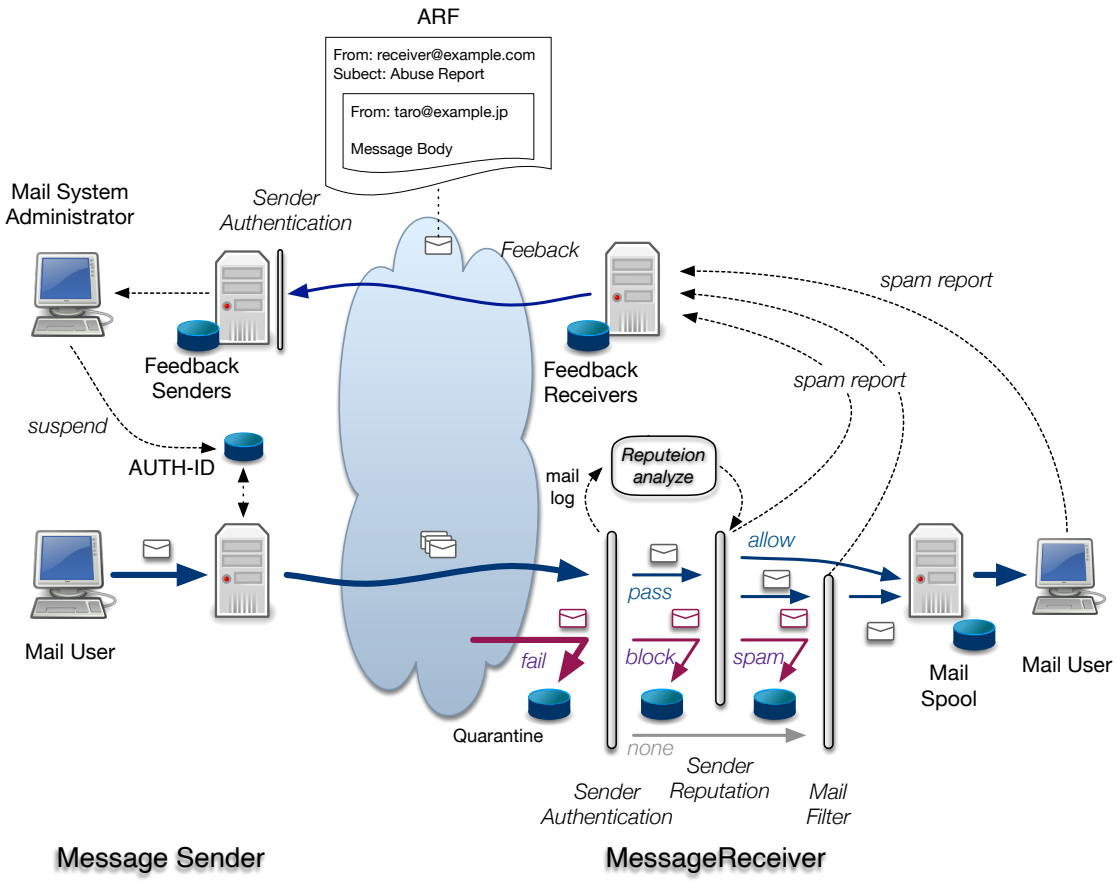

図 5.1: 送信者レピュテーションとフィードバックシステムによるメールシステム

メール受信側では，受信メールに対して送信ドメイン認証を行う．実施する送信ドメイン認証技術は，SPF, DKIM, DMARC の全てを実施することが望ましい．メール送信側が，どの送信ドメイン認証技術に対応しているかが不明なため，利用可能な全ての送信ドメイン認証技術に対応することが求められる．送信ドメイン認証で，認証が失敗（fail）した場合，なりすましメールの可能性が高いため，メール受信を拒絶するかそのままメール受信せずにメール隔離領域（quarantine）か，迷惑メールフォルダ等通常の受信メールとは異なる保存領域に保存する．これらの隔離領域の保存期間を，通常の受信メールの保存期間より短い期間とすることで，本来不要な可能性の高いメールの保存領域の利用効率を高めることができる．送信ドメイン認証によって認証が失敗した場合，特に DMARC で認証が失敗した場合は，送信ドメインの DMARC レコードに設定されたポリシーに沿った受信処

理を行う．送信ドメイン認証が pass した場合，認証された送信ドメイン名を送信者レピュテーションを利用して評価する．送信者レピュテーションが，受け取るべき送信ドメイン名であると判断した場合は，メールフィルタ等を経由せず，受信メール領域（Mail Spool）に保存する．これにより，メールフィルタの処理を軽減するとともに，メールフィルタの誤判定（False-Positive）を軽減することもできる．送信者レピュテーションで，受け取るべきでないブロックリストを保持している場合で，送信ドメイン認証結果や送信元 IP アドレスがブロックリストに適合している場合は，その後のメール配送を継続せず，メール隔離領域に保存する．送信ドメイン認証ができず（結果が none の場合），送信元の IP アドレスによる送信者レピュテーションでの判断ができなかった場合や，送信者レピュテーションで判定できなかった場合は，メールフィルタによる迷惑メールかどうかの判断を行う．迷惑メールと判断された場合は，メール隔離領域に保存する．送信者レピュテーションや，メールフィルタで受け取るべきではない迷惑メールと判定された場合は，そのまま機械的に迷惑メール通知システムに迷惑メールとして通知（spam report）する手法も考えられる．メールフィルタによって迷惑メールと判断されなかった場合は，メール保存領域に保存する．

メールの受信者は，メール取得サーバ（MRA[1]）から受信メールを参照する．参照方法としては，PC やスマートフォン等の MUA やウェブメールの利用が考えら得る．特にウェブメールや，スマートフォンでの専用アプリケーションでは，新たな機能を追加しやすいため，例えば迷惑メールであった場合に，メールサービス側に通知する迷惑メール報告ボタンの機能追加が考えられる．メールシステム側で，こうした機能を実現する方法としては，まず報告を受けたメールを迷惑メール報告システムに通知（spam report）する．迷惑メール報告システムでは，報告されたメールの送信ドメイン認証結果を参照し，メールの送信側のドメイン名を特定する．メールの送信ドメイン名が特定できて，そのドメイン名がフィードバック送信先の情報（Feedback Receivers）に含まれている場合，報告された受信した迷惑メールを ARF 形式のメールに取り込み，メールとしてフィードバック送信先に送信する．このメール送信サーバでも，フィードバック先で送信ドメインを認証できるように，送信ドメインに対応した設定を行う．フィードバックループのメールが，途中でメール転送されたりすることは考えにくいが，対応する送信ドメイン認証技術としては，SPF，DKIM，DMARC 全てに対応することが望ましい．

[1]Mail Retrieval Agent

第6章　結論

本章では，本研究における課題，提案手法についてまとめ，最後に今後の課題について記述する．

6.1　まとめ

本研究では，迷惑メールに関わるセキュリティ的な問題の解決に貢献するために，送信ドメイン認証技術を用いた送信者レピュテーションの構築手法を開発し，その構築手法と適用例を示した．本研究では，特に (1) 送信ドメイン認証技術を利用して，認証した送信者のドメイン名からメールを受け取るための判断基準，(2) 送信者レピュテーションについて，メール受信ログに記録されるような情報を利用して自動的に収集し構築できるような手法，(3) 送信メールサーバの踏み台利用に対する対策手法を提案している．

(1) に関しては，送信ドメイン認証技術の認証結果を利用して，転送メールの送信元 IP アドレスを取得する手法を示し，転送メールが受け取るべきメール送信元であることを述べ，これら送信元 IP アドレスを受け取るべき送信者レピュテーションに加える手法を示した．さらにこの転送メールの送信元 IP アドレスから，受け取るべき送信ドメイン名を取得する方法を述べ，これらも送信者レピュテーションとすることを示した．これらの手法による判断基準が有効であることを，実際に送信者レピュテーションを構築し，それをまた実際の受信メールに適用することで，本提案手法を実際的に評価することで示した．この評価により，本手法を用いて構築した送信者レピュテーションを適用したメールの受け取りの判断では，本来受け取るべきメールの半分以上のメールを判断することができた．さらにメールフィルタを利用した受け取るべき送信者レピュテーションを組み合わせることで，SPF 認証できた受け取るべきメールの大部分を判断することができた．受け取るべきではないメールを受け取るべきと誤判定してしまうメールもあったが，その割合は限定的であり，改善するための手法についても示した．それらの要因や改善のための手法，対策についても示した．

メール内容を利用せず送信者情報だけを用いて構築した送信者レピュテーションが，実

際の受信メールへの適用でこれだけの精度で判定できたことは，大きな成果の一つだと考えている．また，これまで課題だとされてきた，転送メールの SPF 認証の失敗について，それを逆に活用する本手法は，SPF 認証に対応したメールシステムをより増やす可能性もあり，なりすまし対策としての送信ドメイン認証技術の普及に貢献することも期待できる．

(2) に関しては，メールサーバの受信ログを実際に利用することで，送信者レピュテーションを構築できることを示した．今回の評価で利用したデータは，実際のメールサービスで受信したメールの受信ログから抽出した情報であり，一般的なメールサーバの受信ログから送信者レピュテーションが構築できることを示した．さらに，送信者レピュテーションの構築手法を実現するアルゴリズムを示し，それを機械的に適用させることで送信者レピュテーションを構築できることを示した．こらメールの受信ログは，メール受信の都度自動的に記録される情報であり，多くのメールサーバで基本機能として実装されている．そのため，送信者レピュテーションの構築のために，新規にメール情報を集めたり新たな調査等を行うことなく，既に存在している受信メールログの情報を活用することで，構築できる手法であることを示した．

(3) に関しては，送信者レピュテーションのいわば誤判定を改善するためにも重要であり，踏み台送信に関連する諸々の問題を改善するための手法として，フィードバックループの利用を提案した．フィードバックループの導入を促進するためには，フィードバックされる情報の信頼性を高めることが必要である．フィードバックされた情報が信頼でき，それを利用して踏み台送信などの問題が解決できれば，フィードバックループを採用するメールシステムが増えることが期待できる．フィードバックの信頼性を向上させるための仕組みとして，送信ドメイン認証技術を組み込んだ手法を示した．これにより，フィードバックされる迷惑メールの情報の信頼性を高め，フィードバック送信先および受信元についてはその送信元について確認する手法を示すことで，フィードバックループ全体の信頼を高めることができる．この仕組みが実現できれば，これまでメール送信側で検知することが難しかった，メール送信時の認証情報の窃用を検知することができ，その認証情報を摂取された利用者のセキュリティも改善することも可能となる．この迷惑メールの踏み台送信を改善することは，送信者レピュテーションの効果を高めることにもつながることが期待できる．これらの手法を実際にメールシステムに組み込むことで，メールの送受信環境を改善し，メールがより使いやすいコミュニケーションツールとなっていくことが期待できる．

6.2 今後の課題

本研究を通して得られた課題として，送信者レピュテーションの誤判定が挙げられる．これは，送信者情報を利用して判断する上では，迷惑メールの踏み台送信の問題などもあり，本質的に解決が難しい課題ではある．しかしながら，課題を緩和していくためのフィードバックループの提案や，受信メールのSPFによる送信ドメイン認証時の不正なSPFレコードの確認手法，ブロックリストの適用など，幾つか解決の手法についても提案した．これらの解決手法を実際に適用してみることで，送信者レピュテーションの誤判定に関する課題がどの程度改善するのか確認したいと考えている．

また，正規のメールであっても送信ドメイン認証が正しくpassしないメールの配送形態として，メーリングリストがある．メールリングリストでは，SPF認証でのメールの送信元がメーリングリストの管理元に変更され，さらに“Subject:”ヘッダの変更などの処理が行われるため，メーリングリストへ投稿した最初メール送信者のDKIMの署名情報が一致しなくなるという課題がある．現在では，メーリングリストソフトウェア側で，DKIMの再署名を行なった上で，DMARCの認証情報であるヘッダFrom（RFC5322.From）をメーリングリストのドメイン名に書き換える，といった対応方法が標準となりつつある．この場合，メールの送信元は明らかにメーリングリスト側として認識されるため，送信者レピュテーションとしては通常のメール送信元として扱うことができる．しかしながら，既存の配送形態のままであるメーリングリストも多いため，これらの送信元としての評価も検討する必要がある．特にメーリングリストは，設定によりメンバだけの投稿に限る場合と，メンバ外からの投稿もメンバに再配送する運用がそれぞれ可能となっている．メンバ外からの投稿が可能な運用では，メーリングリストはメール配送の増幅装置のように機能してしまう．そのため，既存のメーリングリストの送信元はどこであるのか，その送信元の評価をどう考えるかについての検討も必要と考えている．

フィードバックループは，現在の提案方法ではフィードバック送信元（迷惑メール報告者）と，フィードバック受信側（迷惑メールの対応者）との間で，フィードバックが送信されることを何らかの契約等であらかじめ認識し，相互で利用するドメイン名などを登録する仕組みとしている．この方法は，フィードバックループの利用時点では，プロトタイプ的に相手を増やしていけるという利点はある．しかしながら相互の参加者が増えてくると，フィードバックの送信元と受信側との間で，マトリックスのような構造となり，相互の認証のためのデータベースへの登録はともかく，相互の参加者が増えていく過程でその都度契約等が必要となってしまい，手続きが煩雑になる恐れがある．フィードバックルー

プを利用するメールサービス事業者等が増えることは，踏み台送信の検知やそれに対応した対策が進む上で好ましいことであるが，相互参加者が増えてきた場合は，フィードバック送信側とフィードバック受信側との仲介者を利用することも検討すべきと考えている．

本研究で提案している手法は，いずれも送信ドメイン認証技術を基盤としている．これらの手法が，より効果を得るためには送信ドメイン認証技術がより普及していくことが必要である．引き続き，送信ドメイン認証を普及させていくことが課題であり，それにより認証された送信者をより多く特定できていくことが，迷惑メール対策にとっても重要と考えている．

謝辞

本研究にあたり，ご多忙の中適切なご指導をくださった主任指導教員の大須賀昭彦教授をはじめ，田原康之准教授，清雄一准教授に感謝いたします．研究生活において，様々な面でお世話になりました大須賀・田原・清研究室の秘書の皆様，研究室の皆様に感謝の意を表します．また，株式会社インターネットイニシアティブには本研究に関する貴重なデータを提供頂き，また研究の機会を頂き大変感謝申し上げます．また，迷惑メール対策推進協議会の技術ワーキンググループのメンバの皆様には，迷惑メール対策および踏み台メール送信問題に関しての議論に協力して頂き大変感謝申し上げます．また，JEAG（Japan Email Anti-Abuse Group）でともに迷惑メール対策に関して議論および対策技術の推進の活動をしていただいたメンバの皆様，迷惑メール対策に関する情報共有や議論の場を提供頂いた M^3AAWG（Messaging, Malware and Mobile Working Group）メンバの皆様, 迷惑メール対策を含むセキュリティ対策を共に活動していただいている JPAAWG（Japan Anti-Abuse Working Group）のメンバの皆様に大変感謝申し上げます．特に株式会社 TwoFive 代表の末政延浩様をはじめとする皆様には様々な協力を頂き感謝申し上げます．審査を快く引き受けてくださいました大学院情報システム学研究科の田中健次教授，南泰浩教授，大坐畠智准教授に感謝申し上げます．最後に，これまであらゆる面で支えてくれた家族に感謝いたします．

参考文献

[1] Manos Antonakakis, Roberto Perdisci, David Dagon, Wenke Lee, and Nick Feamster. Building a dynamic reputation system for dns. In *USENIX Security Symposium*, pp. 273–290, 2010.

[2] Leyla Bilge, Sevil Sen, Davide Balzarotti, Engin Kirda, and Christopher Kruegel. Exposure: A passive dns analysis service to detect and report malicious domains. *ACM Transactions on Information and System Security (TISSEC)*, Vol. 16, No. 4, pp. 1–28, 2014.

[3] Seth Blank, Peter Goldstein, Thede Loder, Terry Zink, Marc Bradshaw, and Alex Brotman. Brand Indicators for Message Identification (BIMI). Internet-Draft draft-brand-indicators-for-message-identification-02, Internet Engineering Task Force, October 2022. Work in Progress.

[4] Renée Burton and Laura Rocha. Whitelists that work: Creating defensible dynamic whitelists with statistical learning. In *2019 APWG Symposium on Electronic Crime Research (eCrime)*, pp. 1–10. IEEE, 2019.

[5] Godwin Caruana and Maozhen Li. A survey of emerging approaches to spam filtering. *ACM computing surveys (CSUR)*, Vol. 44, No. 2, pp. 1–27, Mar 2008.

[6] Pin-Ren Chiou, Po-Ching Lin, and Chun-Ta Li. Blocking spam sessions with greylisting and block listing based on client behavior. In *2013 15th International Conference on Advanced Communications Technology (ICACT)*, pp. 184–189, 2013.

[7] Bryan Costales, Claus Assmann, George Jansen, and Gregory Neil Shapiro. *sendmail, 4th Edition*. O'Reilly Media, Inc., October 2007.

[8] Emmanuel Gbenga Dada, Joseph Stephen Bassi, Haruna Chiroma, Shafi'i Muhammad Abdulhamid, Adebayo Olusola Adetunmbi, and Opeyemi Emmanuel Ajibuwa.

Machine learning for email spam filtering: review, approaches and open research problems. *Heliyon*, Vol. 5, No. 6, p. e01802, 2019.

[9] Kenya Dan, Naoya Kitagawa, Shuji Sakuraba, and Nariyoshi Yamai. Spam domain detection method using active dns data and e-mail reception log. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, Vol. 1, pp. 896–899, 2019.

[10] dnswl.org. E-Mail Reputation – Protect against false positives. `https://www.dnswl.org`. Accessed: 2022-09-26.

[11] David Erickson, Martin Casado, and Nick McKeown. The effectiveness of whitelisting: a user-study. In *CEAS*, 2008.

[12] Holly Esquivel, Aditya Akella, and Tatsuya Mori. On the effectiveness of ip reputation for spam filtering. In *2010 Second International Conference on COMmunication Systems and NETworks (COMSNETS 2010)*, pp. 1–10, 2010.

[13] J.D. Falk and Murray Kucherawy. Creation and Use of Email Feedback Reports: An Applicability Statement for the Abuse Reporting Format (ARF). RFC 6650, June 2012.

[14] J.D. Falk and Murray S. Kucherawy. Battling spam: The evolution of mail feedback loops. *IEEE Internet Computing*, Vol. 14, No. 6, pp. 68–71, 2010.

[15] Simon Fernandez, Maciej Korczyński, and Andrzej Duda. Early detection of spam domains with passive dns and spf. In Oliver Hohlfeld, Giovane Moura, and Cristel Pelsser, editors, *Passive and Active Measurement*, pp. 30–49, Cham, 2022. Springer International Publishing.

[16] Tushaar Gangavarapu, CD Jaidhar, and Bhabesh Chanduka. Applicability of machine learning in spam and phishing email filtering: review and approaches. *Artificial Intelligence Review*, Vol. 53, No. 7, pp. 5019–5081, 2020.

[17] Paul Graham. ハッカーと画家 : コンピュータ時代の創造者たち. Hackers and painters. オーム社, 東京, Japan, 2005.1 2005.

[18] JEAG(Japan Email Anti-Abuse Working Group). JEAG Recommendation ～Outbound Port25 Blocking について～. https://salt.iajapan.org/wpmu/anti_spam/wp-content/themes/iajapan/docs/op25b.pdf. Accessed: 2022-09-26.

[19] JEAG(Japan Email Anti-Abuse Working Group). JEAG Recommendation ～送信ドメイン認証について～. https://salt.iajapan.org/wpmu/anti_spam/wp-content/themes/iajapan/docs/senderauth.pdf. Accessed: 2022-09-26.

[20] Thiago S Guzella and Walmir M Caminhas. A review of machine learning approaches to spam filtering. *Expert Systems with Applications*, Vol. 36, No. 7, pp. 10206–10222, 2009.

[21] Shuang Hao, Nick Feamster, and Ramakant Pandrangi. Monitoring the initial dns behavior of malicious domains. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference*, IMC '11, p. 269–278, New York, NY, USA, 2011. Association for Computing Machinery.

[22] Shuang Hao, Nadeem Ahmed Syed, Nick Feamster, Alexander G. Gray, and Sven Krasser. Detecting spammers with snare: Spatio-temporal network-level automatic reputation engine. In *Proceedings of the 18th Conference on USENIX Security Symposium*, SSYM'09, p. 101–118, USA, 2009. USENIX Association.

[23] Markus Jakobsson, Nathaniel Johnson, and Peter Finn. Why and how to perform fraud experiments. *IEEE Security & Privacy*, Vol. 6, No. 2, pp. 66–68, 2008.

[24] Asif Karim, Sami Azam, Bharanidharan Shanmugam, Krishnan Kannoorpatti, and Mamoun Alazab. A comprehensive survey for intelligent spam email detection. *IEEE Access*, Vol. 7, pp. 168261–168295, 2019.

[25] Scott Kitterman. Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1. RFC 7208, April 2014.

[26] Dr. John C. Klensin. Simple Mail Transfer Protocol. RFC 5321, October 2008.

[27] Kanako Konno, Naoya Kitagawa, and Nariyoshi Yamai. False positive detection in sender domain authentication by dmarc report analysis. In *Proceedings of the 2020*

The 3rd International Conference on Information Science and System, ICISS 2020, p. 38–42, New York, NY, USA, 2020. Association for Computing Machinery.

[28] Kanako Konno, Naoya Kitagawa, and Nariyoshi Yamai. Objection, your honor!: False positive detection in sender domain authentication by utilizing the dmarc reports. *International Journal on Advances in Internet Technology*, Vol. 13, No. 1, pp. 35–45, 2020.

[29] Murray Kucherawy. Message Header Field for Indicating Message Authentication Status. RFC 8601, May 2019.

[30] Murray Kucherawy and Dave Crocker. Email Greylisting: An Applicability Statement for SMTP. RFC 6647, June 2012.

[31] Murray Kucherawy, Dave Crocker, and Tony Hansen. DomainKeys Identified Mail (DKIM) Signatures. RFC 6376, September 2011.

[32] Murray Kucherawy, Yakov Shafranovich, and John R. Levine. An Extensible Format for Email Feedback Reports. RFC 5965, August 2010.

[33] Murray Kucherawy and Elizabeth Zwicky. Domain-based Message Authentication, Reporting, and Conformance (DMARC). RFC 7489, March 2015.

[34] John R. Levine. DNS Blacklists and Whitelists. RFC 5782, February 2010.

[35] Federal Bureau of Investigation. Internet Crime Report 2021. `https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf`. Accessed: 2022-09-26.

[36] Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczyński, and Wouter Joosen. Tranco: A research-oriented top sites ranking hardened against manipulation. *arXiv preprint arXiv:1806.01156*, 2018.

[37] Vipul Ved Prakash and Adam O'Donnell. Fighting spam with reputation systems: User-submitted spam fingerprints. *Queue*, Vol. 3, No. 9, p. 36–41, nov 2005.

[38] Spamhaus Project. The Spamhaus Block List. `https://www.spamhaus.org/sbl/`. Accessed: 2022-09-26.

[39] Anirudh Ramachandran and Nick Feamster. Understanding the network-level behavior of spammers. *SIGCOMM Comput. Commun. Rev.*, Vol. 36, No. 4, p. 291–302, aug 2006.

[40] Anirudh Ramachandran, Nick Feamster, and Santosh Vempala. Filtering spam with behavioral blacklisting. In *Proceedings of the 14th ACM Conference on Computer and Communications Security*, CCS '07, p. 342–351, New York, NY, USA, 2007. Association for Computing Machinery.

[41] Mehran Sahami, Susan Dumais, David Heckerman, and Eric Horvitz. A bayesian approach to filtering junk e-mail. In *Learning for Text Categorization: Papers from the 1998 workshop*, Vol. 62, pp. 98–105. Citeseer, 1998.

[42] Carlo Schäfer. Detection of compromised email accounts used by a spam botnet with country counting and theoretical geographical travelling speed extracted from metadata. In *2014 IEEE International Symposium on Software Reliability Engineering Workshops*, pp. 329–334, 2014.

[43] Sushant Sinha, Michael Bailey, and Farnam Jahanian. Shades of grey: On the effectiveness of reputation-based "blacklists". In *2008 3rd International Conference on Malicious and Unwanted Software (MALWARE)*, pp. 57–64, 2008.

[44] Sushant Sinha, Michael Bailey, and Farnam Jahanian. Improving spam blacklisting through dynamic thresholding and speculative aggregation. In *NDSS*, 2010.

[45] Devrim Sipahi, Gökhan Dalklç, and Mehmet Hilal Özcanhan. Detecting spam through their sender policy framework records. *Sec. and Commun. Netw.*, Vol. 8, No. 18, p. 3555–3563, dec 2015.

[46] SpamCop. SpamCop. `https://www.spamcop.net/`. Accessed: 2022-09-26.

[47] Dennis Tatang, Florian Zettl, and Thorsten Holz. The evolution of dns-based email authentication: Measuring adoption and finding flaws. In *Proceedings of the 24th International Symposium on Research in Attacks, Intrusions and Defenses*, RAID '21, p. 354–369, New York, NY, USA, 2021. Association for Computing Machinery.

[48] Bradley Taylor. Sender reputation in a large webmail service ceas 2006. *Jul*, Vol. 27, p. 19, 2006.

[49] Dan Twining, Matthew M Williamson, Miranda Mowbray, and Maher Rahmouni. Email prioritization: Reducing delays on legitimate mail caused by junk mail. In *USENIX Annual Technical Conference, General Track*, pp. 45–58, 2004.

[50] Olivier van der Toorn, Roland van Rijswijk-Deij, Bart Geesink, and Anna Sperotto. Melting the snow: Using active dns measurements to detect snowshoe spam domains. In *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*, pp. 1–9, 2018.

[51] Alessandro Vesely. DNS Whitelist (DNSWL) Email Authentication Method Extension. RFC 8904, September 2020.

[52] 迷惑メール対策推進協議会技術ワーキンググループ. 送信ドメイン認証技術とフィードバックループの推進. https://www.dekyo.or.jp/soudan/data/anti_spam/fbl_16101501.pdf. Accessed: 2022-09-26.

[53] 櫻庭秀次. メールテクニカルレポート, メッセージングテクノロジー, Internet Infrastructure Review. https://www.iij.ad.jp/dev/report/iir/index.html, 2008-2020. Accessed: 2022-09-26.

[54] 櫻庭秀次. メッセージングテクノロジー, Internet Infrastructure Review Vol.47. https://www.iij.ad.jp/dev/report/iir/pdf/iir_vol47_report.pdf, 2020. Accessed: 2022-09-26.

[55] 総務省. 電気通信消費者情報コーナー 迷惑メール対策 統計データ. https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#toukei. Accessed: 2022-09-26.

[56] 迷惑メール対策推進協議会. 送信ドメイン認証技術導入マニュアル 第 3 版. https://www.dekyo.or.jp/soudan/data/anti_spam/meiwakumanual3/manual_3rd_edition.pdf. Accessed: 2022-09-26.

関連論文の印刷公表の方法及び時期

学術雑誌

1. 全著者名：**櫻庭秀次**, 依田みなみ, 清雄一, 田原康之, 大須賀昭彦
   論文題目：送信ドメイン認証を用いた送信者レピュテーションの構築手法とフィードバックループの提案
   印刷公表の方法及び時期：情報処理学会論文誌, Vol.64, No.1, pp.13–23, 2023 年 1 月
   （第 3, 4 章）

2. 全著者名：**櫻庭秀次**, 依田みなみ, 清雄一, 田原康之, 大須賀昭彦
   論文題目：送信ドメイン認証を用いた送信者レピュテーション構築手法の提案
   印刷公表の方法及び時期：情報処理学会論文誌, Vol.62, No.5, pp.1173–1183, 2021 年 5 月
   （第 3 章）

国際会議

3. 全著者名：**Shuji Sakuraba**, Minami Yoda, Yuichi Sei, Yasuyuki Tahara, Akihiko Ohsuga
   論文題目：Sender Reputation Construction method using Sender Authentication
   印刷公表の方法及び時期：2021 IEEE International Conference on Data Science and Computer Application (ICDSCA), pp.369–373, 2021 年 10 月
   （第 3 章）

4. 全著者名：**Shuji Sakuraba**, Minami Yoda, Yuichi Sei, Yasuyuki Tahara, Akihiko Ohsuga
   論文題目：Improvement of Legitimate Mail Server Detection Method using Sender Authentication
   印刷公表の方法及び時期：2021 IEEE/ACIS 19th International Conference on Software Engineering Research, Management and Applications (SERA), pp.10–14, 2021 年 6 月
   （第 3 章）