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

doi: 10.20729/00211077

情報処理学会論文誌 Vol.62 No.5 1173–1183 (May 2021)

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

櫻庭 秀次[1,2,a)] 依田 みなみ[3] 清 雄一[3] 田原 康之[3] 大須賀 昭彦[3]

受付日 2020年8月14日, 採録日 2021年2月2日

概要：迷惑メール対策には，メール内容から迷惑メールを判定する手法と送信者情報を用いる手法があげられる．送信者情報の送信元 IP アドレスや送信者のドメイン名から受け取るべきメールかを判断できれば，判定のための処理負荷の高いメール内容によるメールフィルタの処理を軽減させることができる．本論文では，送信ドメイン認証技術を利用することで転送メールの送信元を特定し，メール転送元が受け取るべき送信元であることを示し，メール転送元を含めた正規メール送信元を収集することで許可リストを構築する手法を提案する．この手法を含めた，送信者レピュテーションの構築手法を提案し，実際に受信したメールの記録を利用して送信者レピュテーションを構築し，適用することで送信者レピュテーションの構築手法の有効性を示す．

キーワード：電子メール，迷惑メール対策，送信ドメイン認証技術，SPF，DKIM，送信者レピュテーション，転送メール

Sender Reputation Construction Method Using Sender Authentication Technologies

Shuji Sakuraba[1,2,a)] Minami Yoda[3] Yuichi Sei[3] Yasuyuki Tahara[3] Akihiko Ohsuga[3]

Received: August 14, 2020, Accepted: February 2, 2021

Abstract: Anti-spam measures include methods for determining unsolicited mail from the mail content and methods for using sender information. If it can be determined from the sender's IP address of sender information and the sender's domain name whether the email should be received, it is possible to reduce the processing of the email filter by the email content that has a high processing load for the determination. In this research, we identify senders of forwarded emails by using sender domain authentication technology, show that the senders should receive the emails, and collect the legitimate email senders including mail forwarders. We propose a method to build a permission list in. We propose a sender reputation construction method that includes this method, construct the sender reputation using the records of the actually received emails, and show the effectiveness of the sender reputation construction method.

Keywords: email, anti-spam measure, sender authentication technology, SPF, DKIM, sender reputation, forarded mail

[1] 株式会社インターネットイニシアティブ
Internet Initiative Japan Inc., Chiyoda, Tokyo 102–0071, Japan
[2] 電気通信大学大学院情報システム学研究科
Graduate School of Information Systems, The University of Electro-Communications, Chofu, Tokyo 182–8585, Japan
[3] 電気通信大学大学院情報理工学研究科
Graduate School of Informatics and Engineering, The University of Electro-Communications, Chofu, Tokyo 182–8585, Japan
[a)] saku@iij.ad.jp

1. はじめに

受信者が望まない，いわゆる迷惑メール（スパム）は，総務省の統計 [1] によれば 2009 年には受信メールの 70%以上あり，2020 年時 3 月時点でも約 50%の割合となっている．迷惑メールの問題は，単に煩わしいというだけでなく，様々なセキュリティ上の問題を引き起こす要因の 1 つとなっている．たとえば，フィッシングやビジネスメール詐

欺（BEC）といった金銭搾取を目的として偽の情報を伝える手段としてメールが利用されたり，情報搾取（漏洩）を目的として不正プログラムを送り込む手段としてメールが悪用されている．さらに不正プログラムが利用 PC を外部から操作するツールとなり，ボットネットに組み込まれることで被害の拡大にも加担させられてしまうなど，迷惑メール対策はインターネット上の重要な課題となっている．

迷惑メールの判定方法には，受信したメールから特徴を抽出し内容に基づいて判定する方法と，メールの送信元の情報から判定する方法が一般的に利用されている．メール内容から判定するメールフィルタは，迷惑メール内容や添付ファイルの巧妙化とともに高度化しており，判定のための処理負荷も増加傾向にある．メールフィルタの負担を軽減するためには，メール送信元の情報による判定方法を利用し，メールフィルタで判定するメール量を減らすことが望ましい．つまり，送信者情報を利用し，明らかに迷惑メール送信者からのメールであれば受け取らず，正規のメール送信者からのメールであれば迷惑メールフィルタを介さず直接受信者に届けるようにする．そのためには，送信者情報を利用したメール受信の判断基準となる，拒否リスト（Block List）と許可リスト（Allow List）による送信者レピュテーションの構築が必要となる．特に，防ぐことが完全には難しいメールフィルタの誤判定（False Positive）によって必要なメールが届かなくなることを防ぐためにも，許可リストは重要である．許可リストには，メールフィルタによる検査を必要としないメールの送信元をできる限り多く登録する必要がある．そうした送信元を判断する方法はいくつかあるが，ここでは転送メールに着目する．

本論文では，送信者レピュテーションの構築手法について提案する．構築手法は 2 つのアプローチからなり，1 つは転送メールの送信元が正規のメール送信元であるとして，送信ドメイン認証技術を利用することで転送メールの送信元を検知し，正規のメール送信者を抽出する手法である．この正規のメール送信者から許可リストを構築する．2 つ目は，メールフィルタの判定結果を利用した拒否リストと許可リストを構築する手法である．この手法により，自動的に独自管理できる送信者レピュテーションを構築する．

送信者レピュテーションの構築手法を評価するために，実際に受信した約 3 億 4 千万件のメールの記録を利用して送信者レピュテーションを構築した．構築した送信者レピュテーションを，約 8 千万件の新たな受信メールに適用させ，迷惑メールでない受けとるべきメールの大部分を判定することができた．受信メールのデータは，筆者の 1 人が所属する ISP のメールサービスの受信ログ情報を利用した．

本論文では，2 章で研究の背景となる迷惑メール対策の状況と，利用する送信ドメイン認証について説明し，3 章で関連する研究を示し本研究のアプローチを示す．4 章で送信者レピュテーションの構築手法を述べ，5 章で実際の受信データ情報を利用して送信者レピュテーションを構築する．6 章で構築した送信者レピュテーションのデータを実際の受信メールに適用し，構築した各レピュテーションデータを評価する．7 章で送信者レピュテーションの構築手法について考察する．

2. 背景

メールの内容に基づく迷惑メールの判定方法として，これまで様々な技術が開発されてきた [2], [3]．また，いわゆる添付ファイルが不正なプログラムかを検査するアンチウイルスフィルタは，これまでのパターン適合による方式だけでなく，動的解析 [4] によって未知のウイルス検出も可能とするなど，新たな技術が開発されてきている．しかし対策技術が開発されれば，それを回避する新たな迷惑メール送信手法が現れるといったことが繰り返されており，その間に迷惑メール判定のために費やされる計算機資源は増加してきている．

送信元情報を利用した迷惑メール対策には，IP アドレスを利用したブロックリストが利用されている．特に，DNS の名前解決の仕組みを利用した DNSBL（DNS Block List）[5], [6] が，DNS と同様にインターネットから利用できる点と，キャッシュの仕組みによるアクセス負荷の軽減など，利用側と提供側の双方に利点のある仕組みとして利用されてきた．これら DNSBL への登録のポリシは，管理元の判断で運営されている．そのため，急激な迷惑メールの大量送信が発生した場合や，ブロックリストに登録されて届かなくった送信元から受け取りたい場合など，リスト管理が自由にできないといった課題がある．

また，受け取るべき送信元 IP アドレスを参照できる DNSWL [7] も運営されているが，登録されれば受信者に確実に届いてしまうために，リストへの登録についてはより厳格さが要求されるべきで，迷惑メール送信元が登録されてしまった場合の影響の大きさもあり，DNSBL ほど一般的に利用されていない．

メールの送信元を示す情報としては，送信者を示すメールアドレスも利用できる．送信者のメールアドレスは，送信ドメイン認証技術の普及とともにドメイン単位で詐称を検知できるようになり，送信元を判断する情報として利用できる環境が整ってきた．これにより，送信ドメイン認証技術で認証されたドメイン名に対して，受け取るべきかどうかを評価するドメインレピュテーションの利用が期待されているが，まだ DNSBL のように広く一般に利用できるような環境は整備されていない．

2.1 送信ドメイン認証技術

メールの送信者をドメイン単位で認証する送信ドメイン認証技術には，Sender Policy Framework（SPF）[8],

表 1 送信ドメイン認証技術の概要
Table 1 Overview of sender authentication technologies.

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

DomainKeys Identified Mail（DKIM）[9]，Domain-based Message Authentication, Reporting, and Conformance（DMARC）[10] がある．それぞれの認証技術の特徴を**表 1** に示す．このうち DMARC については，SPF または DKIM の認証結果を利用するため，送信ドメインを認証するための仕組みとしては SPF と DKIM の 2 通りとなる．

SPF は，受信メールサーバがメール受信時に送信元の IP アドレスと，配送上の送信ドメイン（envelope from のドメイン）名の SPF レコードによって認証を行う．送信ドメインの管理者は，DNS 上の SPF レコード（そのドメイン名に対する TXT 資源レコード）にメールの送信元を記述する．メール受信側は，送信ドメイン名（envelope from）から SPF レコードを取得し，受信時の送信元 IP が SPF レコードに含まれているかを評価することで，送信ドメインの認証を行う．

DKIM は，メールヘッダと本文から秘密鍵を用いて電子署名を作成し，DKIM-Signature メールヘッダとして関連情報も含めてメールに記載する．電子署名を検証するための公開鍵は，DNS 上の DKIM 鍵レコードとして記述する．メール受信側は，DKIM-Signature メールヘッダから署名ドメイン名とセレクタ名を取り出し，DNS へ問い合わせるドメイン名を構成し，DNS から DKIM 鍵レコードを取得することで，メールヘッダと本文から電子署名を検証する．

SPF と DKIM ともに，受信したメールから送信者のドメイン名を取得し，このドメイン名を利用して DNS から認証のための情報を取得することで認証を行う．

2.2 SPF と DKIM の特徴

送信ドメイン認証技術 SPF は，メール送信元の IP アドレスを認証に用いる．そのため，最初のメール送信者と異なる送信元からのメール，たとえば転送メールは SPF では正しく認証ができない．しかしながら，SPF は DNS 上に SPF レコードを設定することで導入できるため，メール送信側での普及率が高いという特徴がある．今回の調査対象としたメールサービスでは，2020 年 4 月に受信したメールのうち，87.9%が SPF に対応している [11]．

DKIM は，メールの配送経路によらない方式で認証を行うため，SPF のようなメール転送の問題は発生しない．しかし，送信するメールについてそれぞれ電子署名を作成しメールに追加する処理が必要なため，DKIM を導入するためには，送信メールサーバに対して追加機能が必要となる．そのため，DKIM は SPF に比べて送信側の普及率が低い傾向がある．2020 年 4 月に受信したメールでは，DKIM の普及率は 48.3%であった [11]．

このように，SPF と DKIM では，特に送信側での導入コストに大きな違いがあり，それに関連して普及率にも差がある．また，SPF はメール転送時に正しく認証できないといった課題もある．

3. 関連研究

3.1 送信者レピュテーション

メールの受け取り判定に利用する送信者情報の 1 つとして，送信元の IP アドレスが利用されてきた．迷惑メール（spam）の送信元 IP アドレスを集める方法には，メール受信者からの spam 報告を受け付ける DNSBL [6] がある．しかしながら，報告された spam がかならずしも正しい情報とは限らないため，内容が spam であることの確認やそれが確かに送信されたメールであるかを報告を受ける側が判断する必要がある．こうした作業を軽減させるため，各報告者に信用度を割り当てる手法がある [15]．新規の spam 報告者は，すでに高い信用度の報告者の spam 報告を利用し，同じ spam を報告していくごとに信用度を獲得していく．しかしながら，こうした spam 報告者のネットワークを構築することは簡単ではなく，また基準となる高い信用度の報告者を獲得すること自体も容易ではない．そのため，広く使われている DNSBL の Spamhaus [5] では，spam 報告を受け付けておらず，各国に存在する調査員が収集した spam 情報を利用するが，この手法では多くの情報を集めるためにはコストが必要となる．送信元 IP アドレスを区別する方法として，ヒューリスティックに判断する手法がある [12]．この手法では，よく知られたメールサービス提供者のドメインの SPF レコードに指定される IP アドレスや，インターネットの一般利用者に割り当てられる動的 IP アドレス，既知のボットネットからの通信の特徴などからその送信元 IP などを収集する．この手法では，ネットワークの利用構成が変更されたり，新しいボットネットなど送信側の特徴が変わった場合に，新たに spam 送信元であることの特徴や正規のメールサービスの送信元の情報を収集してレピュテーションを再構築する必要がある．ほかにも複数の宛先ドメインへの送信パターンから判断する手法 [13] や，SPF レコードの設定内容を統計的に判断し，そのドメイン名をレピュテーションとして利用する手法 [14] など様々提案されている．いずれも，すでに spam と判断したメールに対する特徴を抽出することで，同じ特徴を持つメールの送信元や SPF 認証されたドメインを特定する手法といえる．そのため，対象とするメールが spam であるかの判断が人手によって行われていたり，spam 送信側の技術的な変化などによって特徴が変化した場合，これら送信者レピュテーションが有効に機能しなくなったり，新た

な特徴を抽出するための人的負担が新たに生じることになる．たとえば，中規模のメールサービスで，2020 年 10 月に受信したメールのうち，メールフィルタによって検知された spam は 550 万通以上あり，その割合は約 25%であった．これらのメールを人手によって判断し，集めること自体が簡単な作業ではないし，より大規模のメールサービスであればさらに多くの spam を判断する必要がある．

本論文では，迷惑メール（spam）の判断にメールフィルタの結果を利用し，メール送信元として技術的に詐称が難しい送信元 IP アドレスや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用いて送信者レピュテーションを構築する．これらの送信者レピュテーションの構築には，spam の判断に人手を必要とせず，メール受信時に利用できる信頼できる情報のみを蓄積し利用するため，状況の変更によって変化する可能性の高い spam の特徴を探すなどの負担が生じない．また，受信するメールをレピュテーション構築に利用するため，別途 spam 報告者や報告者からの spam を必要としないという特徴があり，送信者レピュテーション構築の負荷の軽減が期待できる．

3.2 転送メールの抽出

転送メールの検知手法には，DMARC レポートを利用する手法 [16], [17] が提案されている．この手法は，メール受信側がメール送信側に対して，SPF，DKIM，DMARC の送信ドメイン認証結果やメールの送信元 IP アドレスなどの統計情報をレポートする DMARC レポートを利用し，送信ドメイン認証結果とヘッダ From との一致の有無の情報から，X-means によって送信元をクラスタリングし，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．しかしながら，現時点ではメール受信時に DMARC 認証を行うメール受信側自体が少なく，DMARC レポートを送信する受信側はさらに少ないという課題がある．たとえば，中規模のメールサービスで，2020 年 10 月に送信したメールの宛先ドメイン数 17,635 の中で，DMARC レポートを送信してきたドメイン数は 27 であり，0.15%の送信先しか DMARC レポートに対応していなかった．そのため，DMARC レポートを利用して転送メールを抽出する手法は，DMARC レポートの送信が普及していない現在のような状況ではデータが多く集まらず，DMARC レポートの解析を代行するような事業者以外では，転送メールの抽出が難しいといえる．

本論文では，メール受信時の送信ドメイン認証結果の組合せを利用することで，転送メールを抽出する手法を提案する．実際に，同じ中規模のメールサービスで同時期に受信したメールについて調査したところ，送信ドメイン（ヘッダ From）による分類では，受信した送信ドメイン数 62,206 に対して，SPF あるいは DKIM で認証できた送信ドメイン数は 40,752 あり，65.51%の送信ドメインを調査対象にできることが分かった．メールの送信側と受信側という違いはあるが，この結果からは DMARC レポートを利用する手法に比べて，本論文の手法では，調査対象にできる送信ドメインの割合が 400 倍以上高い結果であることが分かった．本論文の手法では，実用上の観点からより多くのメールを転送メールの抽出対象にできるといえる．さらに，転送メールの送信元からのメールは受け取るべきメールであることを示し，送信ドメイン認証技術を利用することで，転送メールの送信元をより広く集める手法を示す．これらの送信元を，正規のメール送信元として送信者レピュテーションを構築する手法を提案する．

3.3 フィードバックループの利用

筆者らは，メール受信側からの spam などの報告のためにフィードバックループの仕組みを構築し，フィードバックされたメール情報からレピュテーションを構築する手法を提案した [18]．この手法では，フィードバックのメール形式に標準的な仕様を用いて統一し，その中で最初の受信時の送信ドメイン認証による認証情報と，フィードバックループそれ自体のメールをそれぞれ送信ドメイン認証することで，最初のメール送信者とフィードバックの報告者をそれぞれ特定できる，信頼性の高いレピュテーションデータを構築できることを特徴としている．しかしながらこのフィードバックループの仕組みは，メール受信側とフィードバックを受け付けてレピュテーションデータを構築する側，最初のメール送信側と，三者の協力関係があってはじめて有効に機能する．そのため，現時点ではこうした三者による協力関係やフィードバックループの実用レベルの仕組みが運用されていない．

本論文では，他者の協力者を必要とせず，メール受信側だけで送信者レピュテーションを構築できる手法を提案している．これにより，送信者レピュテーションをより容易に構築運用できると考えている．

4. 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

送信者レピュテーションとして利用する送信者情報として，メール受信時の送信元 IP アドレス，送信ドメイン認証技術 SPF と DKIM による認証ドメインを利用する．いずれの送信者情報も，メール受信時あるいは受信後の一定の処理時間で得られるため，受信判定のための処理負荷も比較的軽い．

送信者レピュテーションの構築手法としては，2 つの手法を用いる．1 つは，転送メールの送信元を送信ドメイン認証技術を利用して抽出し，その送信元からのメールを正規メールとして許可リストを構築する手法である．送信ドメイン認証技術の SPF と DKIM では，それぞれ認証の仕組みが異なっており，メールの配送経路の違いでそれぞれ

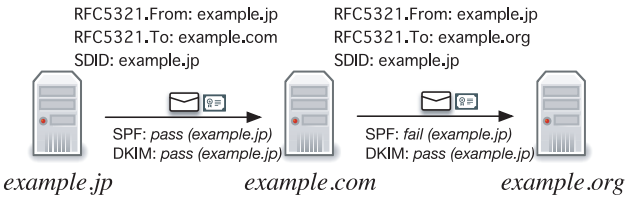

図 1 転送メールの SPF と DKIM 認証
Fig. 1 SPF and DKIM authentication of forwarded maiil.

の認証結果が異なる場合がある．この認証結果の違いを利用することで転送メールであるかを判断する．もう 1 つは，メールフィルタの判定結果を用いて，迷惑メールのみを送信する送信元情報と拒否リストとして構築し，迷惑メールと判定されないメールを送信する送信元情報を許可リストとして構築する．

4.1 転送メールの送信元の抽出

転送メールは，受信したメールサーバが転送設定やエイリアス機能などにより，受信したメール本体を改変することなく，別のメールアドレスへ配送するメールである．転送時のメール送信者のメールアドレスは，最初のメール送信者のまま利用されることが一般的であるため，転送先で SPF 認証すると，送信元の IP アドレスは最初のメール送信者とは関係のない転送元となるため，通常は SPF 認証が失敗する．転送メールでは，署名対象のメール本文が改変されることはないため，最初のメール送信者が DKIM に対応していれば，転送先でも DKIM が認証できる（図 1）．

これらの SPF と DKIM の認証の特徴を利用すれば，受信メールに対して 1) SPF の認証が失敗し，2) DKIM の認証が成功するメール送信元は，転送メールの送信元である可能性が高いと推測できる．また，こうした転送メールの送信元については，すべてが上記の条件を満たしている必要はなく，そうした条件のメールが 1 通でもあれば推測することができる．これにより，DKIM の普及率がそれほど高くない現在のような状況でも，転送メールの送信元の抽出が可能である．

4.2 正規メール送信元の抽出

転送メールの受信者（図 1 では example.org のメール受信者）は，転送メール元（図 1 では example.com）のメール受信者と同じであるか同じ管理者である．転送メールは，転送元が受信するメールを転送先（図 1 では example.org）へ送信するといった，何らかの転送設定をしたことで，転送先に送信されているのであり，そうした設定ができるのは利用元が同じ管理者の場合である．つまり，転送メール先（example.org）の利用者からみれば，メール転送元（example.com）はメールが送信されることを望んでいる正規のメール送信元であると考えることができる．

また，転送メールの送信元は，転送メールだけを送信する送信元とは考えにくく，通常のメールも送信するメールサーバと一般的に考えることができる．SPF の普及率を考えれば，この転送メールの送信元も通常のメールサーバとして何らかのドメイン名の SPF レコードに含まれていると予想できる．これらのことから，1) 転送メールの送信元からのメールであって，2) SPF 認証できた送信ドメイン名は，正規のメール送信ドメイン名と考えることができる．これら正規の SPF ドメイン名の認証ができる送信元は，正規のメール送信元と考えることができる．

正規のメール送信元を抽出する手法は，転送メールの送信元と同じ送信元から送信されて，SPF 認証が成功（pass）する SPF 認証ドメイン名を正規の（SPF）送信ドメイン名として集める．この送信ドメイン名を送信元として設定し，SPF 認証できるメールが正規のメール送信元となる．

4.3 正規メール送信元の抽出手順

受信したメールの情報（ログなど）から，正規メールの送信元を抽出する手順を示す．受信メールの情報には，メールの送信元 IP アドレスと SPF および DKIM の認証結果が含まれているものとする．

Algorithm 1 Collect Legitimate Email Domains
Require: M: received mail information data
Ensure: L: Legitimate Domains
1: $FW = \{\}, SPF = \{\}, L = \{\}$
2: **for all** $m_i \in M$ **do**
3: **if** spf(m_i) is fail **and** dkim(m_i) is pass **then**
4: $FW = FW \cup \{srcip(m_i)\}$
5: **else if** spf(m_i) is pass **then**
6: $SPF = SPF \cup \{(spfdom(m_i), srcip(m_i))\}$
7: **end if**
8: **end for**
9: **for all** $(dom_i, ip_i) \in SPF$ **do**
10: **if** $ip_i \in FW$ **then**
11: $L = L \cup \{dom_i\}$
12: **end if**
13: **end for**

受信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 $m_i (0 \leq i \leq |M|)$ とした場合の，正規のメール送信元（ドメイン名）の集合 L を抽出するアルゴリズムの概要を Algorithm 1 に示す．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，$spf(m_i)$ ではすべて 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る．

この手順を適用して抽出した正規メールについて，5 章で概要を説明する．

4.4 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

迷惑メール（spam）フィルタや添付ファイル部分を検査するアンチウイルスフィルタなど，メールフィルタで判定された結果ごとに送信者情報を蓄積することで，送信者レピュテーションを構築する．迷惑メールと判定されない送信者情報を蓄積することで，転送メールを利用した正規メール送信元と含めて許可リストを構成する．以降の受信メールに対して，許可リストに含まれる送信者からのメールをメールフィルタを経由させずに受信者に届けることで，メールフィルタの処理負荷を軽減する．同様に，迷惑メールと判定された送信者情報を蓄積し，同じ送信者からのメールを受け取らないことで，メールフィルタの処理負荷を軽減する．

本手法で利用する送信者情報は，メール受信時に得られるものであり，結果はメールヘッダとして保存される．メールフィルタによる判定結果後に，これら保存されている送信者情報を取り出すことで，自動的に送信者レピュテーションを構築することができる．

これら送信者レピュテーションの有効性については，受信するメールにどれだけ多く適用できるか，メールフィルタでの判断処理を省くことができたかで評価することができる．

5. ログデータからの送信者レピュテーションの構築

ここでは，実際のメールサービスで受信したメールのログデータを利用して，送信者レピュテーションの構築手法を適用し，送信者レピュテーションを構築する．対象としたログデータは，2019 年 9 月の 1 カ月間に受信した約 3 億 4 千万件のメール情報である．ログデータの概要を**表 2** に示す．迷惑メールと判定されなかったメールを ham，迷惑メールと判定されたメールを spam とし，それぞれの送信ドメイン認証技術の対応割合と認証された割合を示す．

このログデータから，送信ドメイン認証の結果を利用して転送メールと正規メールの送信元を抽出し，メールフィルタの判定結果から IP レピュテーションと SPF および DKIM のドメインレピュテーションを抽出する．

5.1 転送メールからの正規メール送信元の抽出

正規メールの送信元抽出のための手順では，送信元情報として抽出するのは SPF 認証されたドメイン名であるが，今回は，受信メール数としての比較を分かりやすくするため，メールログから対象の SPF ドメイン名で認証されたメールの送信元 IP アドレスを抽出した．受信メールの送信元 IP アドレスの種類数（IP#）と，抽出した正規のメール送信元種類数（legit IP#）について，メールフィルタの判定結果ごとに結果を**表 3** に示す．

表 2 メールログデータ概要
Table 2 Mail log data overview.

判定結果	受信メール割合	SPF 対応	SPF 認証	DKIM 対応	DKIM 認証
ham	88.3%	78.4%	68.8%	39.2%	37.7%
spam	11.7%	8.5%	2.3%	0.4%	0.3%
total	100.0%	86.9%	71.1%	39.6%	38.0%

表 3 正規送信元の分類
Table 3 Legitiimate source IPs by spam filter.

判定結果	IP#	legit IP#	受信数割合
ham	547,741	57,806	48.5%
spam	555,239	8,347	0.6%

表 4 IP レピュテーションの抽出
Table 4 Classification of IP reputation by mail filter.

判定結果	IP#	受信量割合	平均送信数
ham	379,465	51.4%	468.6
spam	386,963	0.7%	6.3
both	168,276	47.9%	986.0

受信メールのうち ham は全体の 88.3%なので，legit IP の 48.5%は ham の 54.9%を抽出できたことになる．また spam については，受信メールの割合が 11.7%なので spam の 5.4%を抽出している．本来，正規メールの送信元は許可リストとなる送信元であるので，5.4%の受信メールを誤判定したことになる．迷惑メール判定の誤判定率としては比較的低い割合ではあるが，この誤判定の原因と，さらに誤判定を減らす方法について 7 章で検討する．

5.2 IP レピュテーション

メールフィルタの判定結果から，IP レピュテーションを構築する．具体的には迷惑メールではないメール（ham）のみを送信する送信元の IP アドレスを許可リストとし，迷惑メール（spam）のみを送信する送信元の IP アドレスを拒否リストとする．ham と spam の両方のメールを送信する送信元は，both と示した．IP レピュテーション構築の結果を**表 4** に示す．この調査結果から，ham と spam の両方の送信元である both の割合が半数近くあることが分かった．

次に IP レピュテーションの ham と spam について，構築後にどの程度の割合で受信メールに含まれるかについて調査した．また IP レピュテーションの構築期間を 1 週間と 4 週間とし，構築期間も含めて 1 週間単位で 9 週間の期間に ham および spam それぞれの受信メールに対して，含まれる割合を調査した．調査結果を**図 2** に示す．

図 2 の結果からは，ham の送信元については，2 カ月後の受信メールでも 70%前後が含まれており，送信元の収集期間を長くすることで，より含まれる割合が増える結果と

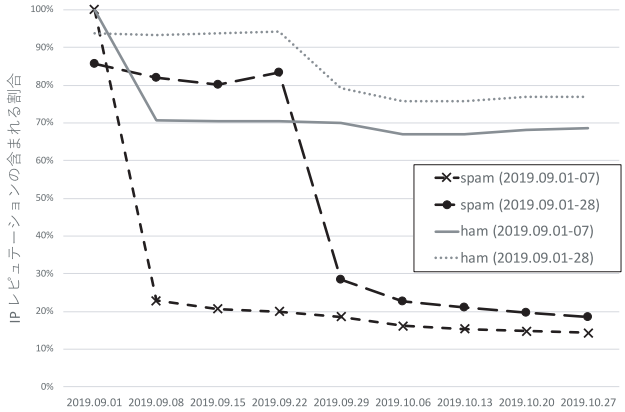

図 2 IP レピュテーションの期間と継続割合
Fig. 2 IP reputation period and duration.

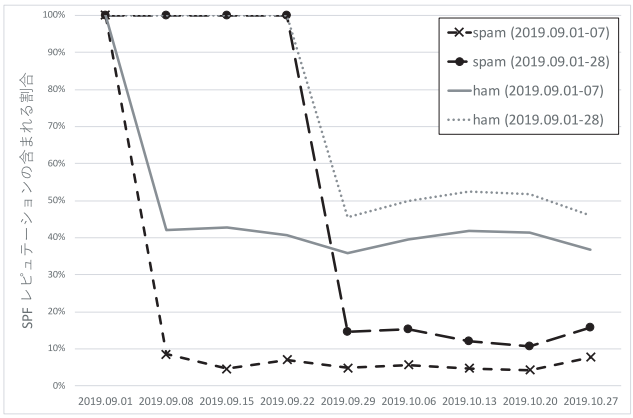

図 3 SPF レピュテーションの期間と継続割合
Fig. 3 SPF reputation period and duration.

表 5 SPF ドメインレピュテーションの抽出
Table 5 Classification of SPF domains by spam filter.

判定結果	ドメイン#	受信量割合	平均送信数
ham	1,473,326	68.9%	115.1
spam	155,088	0.3%	4.4
both	14,804	30.8%	5,125.4

表 6 DKIM ドメインレピュテーションの抽出
Table 6 Classification of DKIM domains by spam filter.

判定結果	ドメイン#	受信量割合	平均送信数
ham	201,369	61.8%	404.1
spam	21,703	0.2%	10.5
both	8,946	38.0%	5,603.7

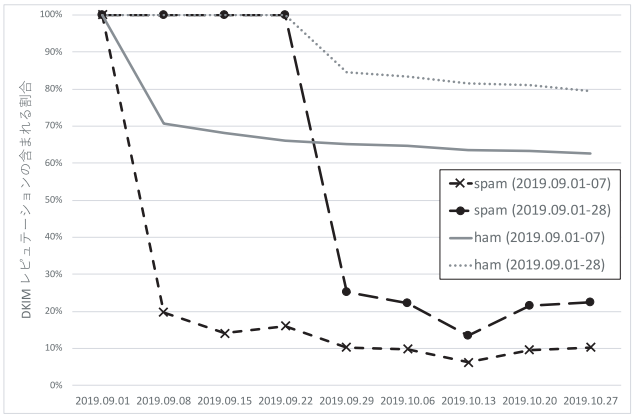

図 4 DKIM レピュテーションの期間と継続割合
Fig. 4 DKIM reputation period and duration.

なった．一方で spam の送信元については，収集期間の翌週には含まれている割合が 20%から 30%程度に低下し，その後も含まれる割合が少しずつ減少していく結果となった．

5.3 ドメインレピュテーション

IP レピュテーションと同様に，SPF と DKIM で認証されたドメイン名に対して，メールフィルタによる判定結果を利用してドメインレピュテーションを構築する．メールフィルタの判定結果を利用し，認証されたドメイン名を ham，spam，both に分類し，ham と spam をドメインレピュテーションとして利用する．ドメインレピュテーション構築の結果を**表 5**，**表 6** に示す．

次に，SPF と DKIM のドメインレピュテーションについて，構築期間を 1 週間と 4 週間に変えて，以後 9 週間に受信するメールに含まれる割合を調査した．調査結果を**図 3**，**図 4** に示す．

IP レピュテーションと同様に，SPF と DKIM いずれのドメインレピュテーションも，構築後に含まれる割合が大きく減少することが分かった．また，IP レピュテーションや SPF のドメインレピュテーションの ham では，構築期間の長さの違いによる割合の差は 10%程度だったが，DKIM の ham については 15%以上高い結果となり，また ham の構築後に含まれる割合も高い結果となった．

6. 送信者レピュテーションの評価

5 章で構築した，2019 年 9 月の 1 カ月間に受信したメールによる送信者レピュテーションについて，その翌週の 2019 年 10 月 1 日から 7 日までの 1 週間に受信したメールが，どの程度含まれるかを調査した．送信者レピュテーションは，受信したメールの送信者情報を利用して随時更新していくことを想定しているため，送信者レピュテーションの構築直後の一定期間に送信者情報がどの程度含まれるかを調べることで，その後の期間も含めた送信者レピュテーションの効果を推測することができると考えている．

この 1 週間で受信したメールの迷惑メール割合は 9.0%であった．メールフィルタの判定結果から，受信メールを ham（迷惑メールではない），spam（迷惑メール），all spam（迷惑メール判定された送信元すべて），both（両方の送信元）の送信元からの受信メール，の 4 種類に分類した．送信者レピュテーションの種類は，正規メールの送信元（legit），IP レピュテーション（allow IP，block IP），SPF の認証ドメイン（allow SPF，block SPF），DKIM の認証

表 7 送信者レピュテーションの適合割合
Table 7 Sender reputation comformance.

	ham	spam	all spam	both
受信割合	62.1%	0.8%	9.0%	37.1%
legit	45.3%	1.4%	5.9%	64.3%
allow IP	84.5%	0.8%	0.6%	2.9%
block IP	0.0%	29.0%	4.5%	0.7%
allow SPF	81.0%	0.2%	0.1%	1.8%
block SPF	0.0%	7.3%	0.8%	0.0%
allow DKIM	37.8%	0.2%	1.2%	1.6%
block DKIM	0.0%	2.7%	0.0%	1.5%

ドメイン（allow DKIM，block DKIM）の 4 種類 7 パターンで，ham，spam，all spam，both に対する割合は，それぞれの分類全体の場合に 100 として含まれる割合を示した．

この結果から，ham に最も高い割合で含まれてたのは allow IP で，spam は block IP，both は legit であることが分かった．

both は，迷惑メールと迷惑メールではないメールの両方の送信元であるため，含まれる割合が高いことが，どのメールを抽出したのかがこの数値だけでは判断できない．受信メールで迷惑メール判定されたすべての送信元に対する割合（all spam）が 5.9%なので，legit が both に適合した 64.3%の大部分は，ham を含んでいると考えられる．

次にこれら送信者レピュテーションを適用した場合に，どの程度メールフィルタの処理を減らすことができるかを調査した．送信者レピュテーションの適用の方法は，メール送信元の IP アドレスに対して，次に SPF，DKIM の認証ドメインに対して，それぞれ許可（allow）あるいは拒否（block）リストに含まれているメールを，メールフィルタを介さずに直接届けるあるいは迷惑メールと判断する処理を行うと仮定した．調査の結果，送信者レピュテーションの IP アドレスによってメールフィルタの判定処理を行わずに済むメールは，受信メール全体の 84.3%となり，その中で 83.8%は許可リストに含まれるものだった．同様に，SPF および DKIM で認証されたドメイン名では 2.0%であり，ほぼすべてが許可リストに含まれるメールだった．これらの調査結果から，送信者レピュテーションを適用することで，受信メールすべてをメールフィルタに適用させる場合に比べて，メールフィルタの判定処理を 86.3%軽減できることが分かった．この送信者レピュテーションの結果を，メールフィルタによる判定結果と比較した場合，受信メール全体の 0.6%が異なる結果となった．このうち，メール利用の観点からより重要と考えられる受け取るべきメールを迷惑メールと判断してしまう偽陽性については，受信メール全体の 0.06%であった．

これらの結果から，送信者レピュテーションを適用することで，メールフィルタの判定処理の大部分を軽減できることが分かり，大幅な処理負荷の軽減が期待できるが，誤判定がまったく生じないわけではないことから，その結果についてメールシステムによっては慎重な取扱いを要する必要があると考える．

7. 考察

送信元情報の IP アドレス，SPF と DKIM で認証されたドメイン名それぞれについて，転送メールを抽出することで許可リストを構築し，メールフィルタの判定結果を利用して，許可リストと拒否リストによる送信者レピュテーションを構築した．構築した送信者レピュテーションを実際の受信メールに対して適用し，どの程度適合するかを調査した．

許可リスト（legit，allow IP，allow SPF，allow DKIM）は，おおむね高い割合で含まれており，割合の差は利用できる割合（普及率）の差の順（IP，SPF，DKIM）となった．legit の 45.3%はこの中では低いが，legit で抽出できた送信元 IP アドレスは，ham の 15.0%であり，少ない IP アドレスのデータで大きな割合を抽出できたことになる．また，誤判定といえる spam に含まれる割合も少なく，allow IP，allow SPF，allow DKIM は 1%以下であった．legit は 1.4%と比較的高いが，この原因としては以下が考えられる．

- メール転送元が受信した迷惑メールも含めて転送している（転送元で迷惑メールフィルタしていない場合）
- 正規のメールサーバ経由で迷惑メールが送信されている（送信のための認証 ID などが悪用されているなど）

迷惑メールを含めて転送している場合は，それらのメールも含めて受信したい場合と，迷惑メールを転送先でフィルタリングしたい場合などが考えられる．いずれにしても，転送メールかどうかは SPF 認証で推定できるので，転送メールはメールフィルタに適用させるという設定をメール受信者に提供することもできる．正規のメールサーバを迷惑メール送信に悪用する踏み台の問題は，近年発生している送信手法の 1 つで，送信者情報からの判断では対応できない．踏み台問題については，メールサービス提供側でメール送信のための認証や仕組みを強化するなどの対策が必要と考えている．

もう 1 つ，legit の誤判定の原因として考えられるのが，不正な SPF レコードを設定したドメイン名である．SPF レコードには，メールの送信元を記述し，それ以外の送信元を示す記法として “all” があり，“all” に該当した場合の認証失敗の強度を記号（–，∼，?）で示すことができる．この記号の中には，認証成功を示す “+”（省略した場合も該当）もあり，“+all” を SPF レコードに含めることですべての送信元を SPF 認証できるようなドメイン名を作ることができる．実際に legit で誤判定された送信メールを分析したところ，この不正 SPF レコードにより誤判定していた場合が見つかった．このようなケースは，SPF レコードの内容を検査するることで legit から除外するなどの対

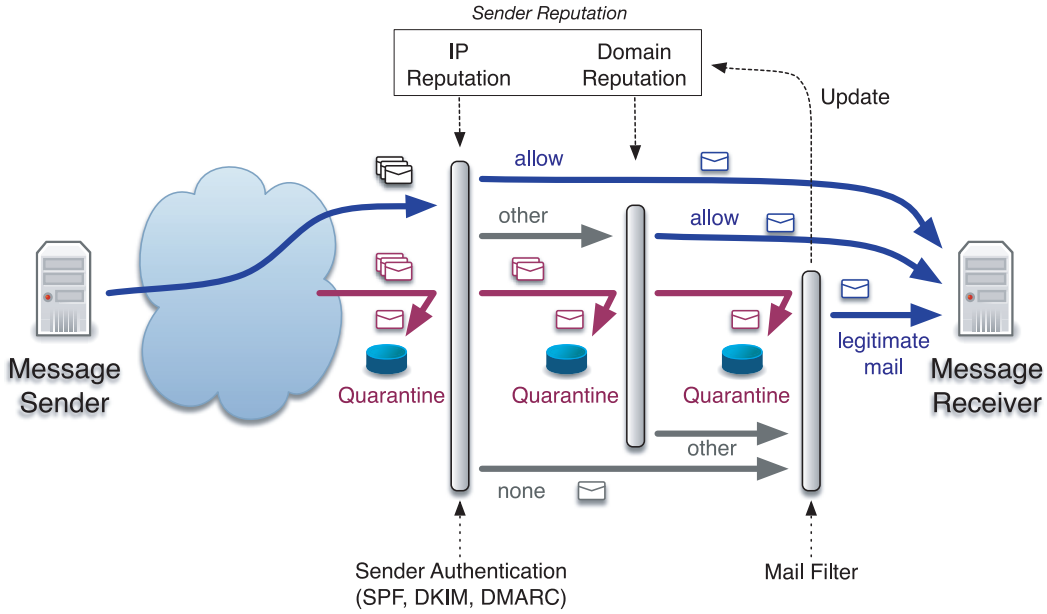

図 5 送信者レピュテーションを利用したメールシステム
Fig. 5 Mail system with sender reputation.

応により，誤判定を減らすことができる．

拒否リストでは，block IP が最も適合割合が高いが 30%以下であり，これまでの評価結果から時間経過によってこの割合が低下していくと予想される．同様の手法として DNSBL などが利用されていることから，迷惑メール送信者が固定的な送信元ではなくボットネットなど広範囲な送信元を利用していることが適合割合が低い原因と考えている．拒否リストについては，判定できなかったメールをメールフィルタに適用していくことで，長期的に迷惑メール送信元を蓄積していく必要がある．

メールフィルタの判定結果を利用した送信レピュテーション（IP，SPF，DKIM）では，迷惑メールと迷惑メールでない両方のメール送信元（both）部分を判別することが難しい．これらの送信元は，2019 年 9 月で受信メール全体の 47.9%，2019 年 10 月の第 1 週で 37.1%と大きな割合であるため，これら both の送信元からさらに許可あるは拒否の判断が必要になる．転送メールを利用した正規メール送信元の抽出による許可リスト（legit）が，この both 部分から正規のメールをうまく判別できていると考えている．この legit を活用することで，より多くの受信メールをメールフィルタを介さずに適切に対応できると考えている．

7.1 送信者レピュテーションの利用例

送信者レピュテーションを利用したメール受信システムの一例を図 5 に示す．メール受信時に送信元の IP アドレスを参照し，その IP アドレスが，送信者レピュテーションの IP アドレスによる許可リストと拒否リストに含まれるかを検査する．許可リストに含まれる送信元からのメールは，その後のフィルタ処理を通さず受信メールサーバに直接送信する．これにより，メールフィルタの判定処理の負荷を軽減することができる．拒否リストに含まれる場合は，迷惑メールであると判断し，そのメールのメール受信者が参照できる隔離領域（Quarantine）に一定期間保存する．また，メール受信時には，SPF，DKIM，DMARC による送信ドメイン認証を行い，それぞれの認証技術による認証ドメイン名を取得する．送信ドメイン認証によって認証できなかったメール（none）は，送信者レピュテーションのドメイン名による判定ができないため，メールフィルタでメール内容から迷惑メールであるかを判断する．メールフィルタで迷惑メールであると判断された場合は，同様に隔離領域に保存される．

送信ドメイン認証技術により SPF，DKIM の認証ドメイン名が得られた場合，二段目の送信者レピュテーションの SPF および DKIM のドメインレピュテーションにより，許可リストあるいは拒否リストに含まれるかを検査する．許可リストに含まれる場合は，メールフィルタを介さずに受信メールサーバに直接送信する．拒否リストに含まれる場合は，隔離領域に保存される．いずれかのドメインレピュテーションに含まれるメールをメールフィルタによる判定処理を行わないことにより，判定処理にかかる負荷を軽減させることができる．メールフィルタ処理では，判定された結果とメールの送信者情報を抽出し，送信者レピュテーションのデータ更新を行う．

このように，送信者レピュテーションを構築し適用させることで，メール内容に基づくメールフィルタの判定処理に適用させるメール量を減らすことができる．これにより，迷惑メールの判定処理により多くの計算資源を割り当てたり，高度な判定技術を導入していくことで，メールフィル

タの判定精度をさらに高めていくことも期待できる．

8. おわりに

本論文では，送信ドメイン認証技術を利用して転送メールを抽出し，この転送元から正規メールの送信元を抽出することで許可リストを構築する手法と，メールフィルタの判定結果と送信ドメイン認証技術を利用して許可リストと拒否リストを構築する手法を提案した．これらの提案手法に基づき実際の受信メールから送信者レピュテーションを構築し，さらに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ことで，それぞれの送信者レピュテーションの特徴を明らかにすることができた．特に転送メールの抽出による正規メールの抽出手法については，これまで課題とされてきたSPFの転送メール問題を逆に活用することで，メールフィルタの判定結果の利用だけでは判別が難しい，迷惑メールと通常メールの両方の送信元に対しての新しい判定手法を提案することができた．

また，これまで送信ドメイン認証技術は，送信ドメイン名の詐称の検知以外の用途が広がらず，送信ドメイン認証技術特にDKIMやDMARCの普及率が低い状況が続いている．本手法により，メール送信側での導入およびメール受信側での認証機能の導入が進むことを期待している．

今後の課題として，不正なSPFレコードの検知とそれを利用した送信者レピュテーションへの組み込み，DKIMおよびDMARCの利用があげられる．また送信ドメイン認証技術は，DNSの信頼性に依存している部分も多いため，DNSSECの利用促進やその利用ドメイン名に対してのレピュテーション，ドメイン管理元に対してのレピュテーションなどを取り入れることを検討している．

謝辞 本研究はJSPS科研費JP17H04705, JP18H03229, JP18H03340, JP18K19835, JP19H04113, JP19K12107の助成を受けたものです．本研究を遂行するにあたり，研究の機会と議論・研鑽の場を提供していただいた（株）インターネットイニシアティブおよび迷惑メール対策推進協議会 技術WGの皆様に感謝致します．

参考文献

[1] 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，入手先 ⟨https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#toukei⟩（参照2020-07-25）．
[2] Karim, A., Azam, S., Shanmugam, B., Kannoorpatti, K. and Alazab, M.: A Comprehensive Survey for Intelligent Spam Email Detection, *IEEE Access*, Vol.7, pp.168261–168295 (2019).
[3] Godwin, C. and Li, M.: A Survey of Emerging Approaches to Spam Filtering, *ACM Computer Surveys*, Vol.44, No.2 (2012).
[4] 情報処理推進機構：未知ウイルス検出技術に関する調査 調査報告書，入手先 ⟨https://www.ipa.go.jp/security/fy15/reports/uvd/documents/uvd_report.pdf⟩（参照2020-07-25）．
[5] The Spamhaus Project, available from ⟨https://www.spamhaus.org/⟩ (accessed 2020-07-25).
[6] SpamCop, available from ⟨https://www.spamcop.net/⟩ (accessed 2020-07-25).
[7] DNS Whitelist - Protect against false positives, available from ⟨https://www.dnswl.org/⟩ (accessed 2020-07-25).
[8] Kitterman, S.: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1, RFC7208 (2014).
[9] Crocker, D., Hansen, T. and Kucherawy, M.: DomainKeys Identified Mail (DKIM) Signature, STD 76, RFC6376 (2011).
[10] Kucherawy, M. and Zwicky, E.: Domain-based Message Authentication, Reporting, and Conformance (DMARC), RFC7489 (2015).
[11] 櫻庭秀次：メッセージングテクノロジー，*Internet Infrastructure Review*, Vol.47, pp.4–9 (2020), 入手先 ⟨https://www.iij.ad.jp/dev/report/iir/047.html⟩．
[12] Esquivel, H., Akella, A. and Mori, T.: On the effectiveness of IP reputation for spam filtering, *2010 2nd International Conference on COMmunication Systems and NETworks* (*COMSNETS 2010*), pp.1–10 (2010).
[13] Ramachandran, A., Feamster, N. and Vempala, S.: Filtering spam with behavioral blacklisting, *Proc. 14th ACM Conference on Computer and Communications Security*, pp.342–351 (2007).
[14] Sipahi, D., Dalkılıç, G. and Özcanhan, M.H.: Detecting spam through their Sender Policy Framework records, *Security and Communication Networks*, Vol.8, No.18, pp.3555–3563 (2015).
[15] Prakash, V. and O'donnell, A.: Fighting Spam with Reputation System, *ACM Queue*, Vol.9, No.9, pp.36–41 (2005).
[16] Konno, K., Kitagawa, N. and Sakuraba, S., et al.: Legitimate E-mail Forwarding Server Detection Method by X-means Clustering Utilizing DMARC Reports, *11th Internation Conference on Evolving Internet* (*INTERNET 2019*), pp.24–29 (2019).
[17] Konno, K., Kitagawa, N. and Yamai, N.: 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 & 2, pp.35–45 (2020).
[18] 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，入手先 ⟨https://www.dekyo.or.jp/soudan/data/anti_spam/fbl_16101501.pdf⟩（参照2020-07-25）．

櫻庭 秀次 （正会員）

1967年生．1999年電気通信大学電気通信学部情報工学科卒業．現在，電気通信大学情報システム学研究科博士後期課程に在学中．（株）東芝を経て（株）インターネットイニシアティブにて，メッセージング技術に関する研究開発および国内外のメッセージングセキュリティに関する活動に従事．ACM会員．

依田 みなみ

1990 年生．2017 年電気通信大学情報システム学研究科博士前期課程修了．同年（株）トヨタ自動車入社．同社コネクティッド先行開発部に所属．2019 年電気通信大学大学院情報理工学研究科情報学専攻博士後期課程入学．プログラム解析によるバグや脆弱性の検出に興味を持つ．EAJ ジェンダー委員会学生委員．

清 雄一 （正会員）

1981 年生．2009 年東京大学大学院情報理工学系研究科博士後期課程修了．同年（株）三菱総合研究所入社．2013 年電気通信大学．現在，同大学大学院情報理工学研究科准教授．博士（情報理工学）．エージェント，プライバシ保護技術等の研究に従事．2016 年度土木学会水工学論文賞，情報処理学会論文賞受賞．電子情報通信学会，日本ソフトウェア科学会，IEEE Computer Society 各会員．

田原 康之 （正会員）

1966 年生．1991 年東京大学大学院理学系研究科数学専攻修士課程修了．同年（株）東芝入社．1993～1996 年情報処理振興事業協会に出向．1996～1997 年英国 City 大学客員研究員．1997～1998 年英国 Imperial College 客員研究員．2003 年国立情報学研究所着任．2008 年より電気通信大学准教授．博士（情報科学）（早稲田大学）．エージェント技術，およびソフトウェア工学等の研究に従事．日本ソフトウェア科学会会員．

大須賀 昭彦 （正会員）

1958 年生．1981 年上智大学理工学部数学科卒．同年（株）東芝入社．同社研究開発センター，ソフトウェア技術センター等に所属．1985～1989 年（財）新世代コンピュータ技術開発機構（ICOT）出向．2007 年電気通信大学．現在，同大学大学院情報理工学研究科教授．2017 年より同大学大学院情報システム学研究科研究科長併任．2012 年より国立情報学研究所客員教授兼任．工学博士（早稲田大学）．ソフトウェア工学，エージェント，人工知能の研究に従事．1986 年度および 2016 年度情報処理学会論文賞，2013 年度人工知能学会研究会優秀賞，2014 年度同学会功労賞，2018 年度電子情報通信学会 ISS 活動功労賞受賞．IEEE Computer Society Japan Chapter Chair，人工知能学会理事，日本ソフトウェア科学会理事，同学会監事，同学会評議員等を歴任．電子情報通信学会，人工知能学会，日本ソフトウェア科学会，電気学会，IEEE Computer Society 各会員．本会フェロー．