情報処理学会論文誌 Vol.64 No.1 13–23 (Jan. 2023)

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

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 2022年4月11日, 採録日 2022年10月4日

概要：迷惑メール対策を目的として，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とフィードバックループについて提案する．送信者レピュテーションは，メールの送信元情報を用いて受け取りを判断するための情報であるが，その中で受け取るべき正規のメール送信元を収集することは簡単ではない．本論文では，転送メールの送信サーバが正規のメール送信元と考え，転送メールをメール受信時に送信ドメイン認証の結果を用いて判断する手法を示す．この転送メールの判断手法には課題が残っており，メール転送時に送信元情報を書き換える転送メールについては判断できない．本論文では，送信ドメイン認証の結果を用いて，メール転送時に送信元情報を書き換える転送メールについても判断できる手法を追加した，送信者レピュテーションの構築手法について示す．また送信者レピュテーションは，正規のメール送信元から送信される迷惑メールに対応できないという課題がある．この課題を改善するためには，迷惑メールの受信側からメールの送信元へ通知を行うフィードバックループが有効である．本論文では，通知の信頼性を向上させるために送信ドメイン認証を利用する手法を示す．送信者レピュテーションの構築手法の有効性を評価するために，実際のメールサービスでの受信記録情報を用いて適用し，より多くの受け取るべきメールを判定できることを示した．これらの手法により，迷惑メール対策において必要なメールがより確実に届き，送信者レピュテーションを悪用する正規のメールサーバの不正利用を改善することが可能となる．

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，フィードバックループ

Sender Reputation Construction Method And Feedback Loop Using Sender Authentication

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

Received: April 11, 2022, Accepted: October 4, 2022

Abstract: We propose a sender reputation construction method and feedback loop using sender authentication technology for the purpose of preventing unsolicited emails. Sender reputation is information for judging receipt by using the sender information of mail, but it is not easy to collect the legitimate mail sender to be received in it. In this paper, the sender of the forwarded email is considered to be the legitimate email sender. We show a method to judge forwarded mail by using the result of sender authentication when receiving mail. There are still issues with this method of determining forwarded mail, and it is not possible to judge forwarded mail that rewrites the sender information when forwarding mail. In this paper, we show a method of constructing sender reputation by adding a method that can judge forwarded mail that rewrites the sender information at the time of mail forwarding by using the result of sender authentication. In addition, sender reputation has the problem that it cannot handle unsolicited emails sent from legitimate email sources. In order to improve this problem, a feedback loop that notifies the sender of the email from the receiver of the junk email is effective. In this paper, we show a method that uses sender authentication to improve the reliability of notifications. In order to evaluate the effectiveness of the sender reputation construction method, we applied it using the reception record information of the actual mail service, and showed that more mails to be received can be determined. With these methods, it is possible to more reliably receive the emails necessary for anti-spam measures, and to improve the unauthorized use of legitimate mail servers that abuse sender reputation.

Keywords: email, anti-spam measure, sender authentication technology, SPF, DKIM, feedback loop

1. はじめに

社会的な情勢の変化もありリモート環境での各種作業が行われるようになり，インターネット上のコミュニケーションツールの利用が進んでいる．コミュニケーションツールには，各種チャットツールやSNS（Social Networking Service）のメッセンジャーなどのアプリケーションが利用されているが，異なった組織間などで共通して利用できるツールとして，電子メールが依然として広く使われている．電子メールでは，宛先メールアドレスが分かれば誰でも送信することができるため，広告宣伝メールやフィッシング，セキュリティ上の問題を引き起こす不正プログラム（マルウェア）に感染させようとする悪意あるメールなどが送られる．そのため，これら迷惑メールの対策は解決すべき重要な課題の1つとなっている．

迷惑メールによる被害を防ぐためにメール受信側では，メールの内容などから迷惑メールであるかを判断したり，添付されているファイルがウイルスやマルウェアであるかを確認したりするなどの，各種メールフィルタを利用する．迷惑メールの送信者やマルウェアの作成者は，これらメールフィルタで検知されないために様々な工夫をしてきており，そうした行為に対抗するためにさらに様々な検知手法が研究されてきている [1]．こうした攻防が続く原因には，メール送信のコストが低いことがあげられるが，受信側で送信者を正しく認識できないことにより，メール内容から受け取るべきかを判断しなければならない点にある．こうした背景から，メールの送信者をドメイン名単位で認証する，送信ドメイン認証技術の仕様が開発されてきた．

送信ドメイン認証技術は，メールの送信側がDNSと連携して送信元を明らかにすることで，受信側で送信者情報がなりすまされていないかを検証できる技術である．送信者情報が詐称できなくなれば，送信者情報によって受け取るべきかどうかを判断することができるようになる．このような送信元やドメイン名などに対する評価は送信者レピュテーションと呼ばれるが，送信元のIPアドレスを利用したDNSBL（DNS Block List）以外はあまり利用されていない．また受け取るべき許可リスト（Allow List）については，登録する基準やそのリスト管理者に対する信頼性の課題などがあり，これまであまり利用されてこなかった．またメールの利用者は，不要な迷惑メールの情報提供はできるが，受け取るべき必要なメールには重要な情報が含まれる場合も多いことから，許可リストの管理者など第三者への情報提供が難しいという課題もある．これらのことから，許可リスト構築のための情報は集めにくく，結果として利用も進まない状況となっていることが推測される．そのため，送信者レピュテーションを利用するメール受信側が，自ら受信するメールの情報から送信者レピュテーションを構築することができれば，送信者レピュテーションに対する基準や信頼性は明らかであり，受け取るべきメールを明確に判断できるようになる．

我々は，送信ドメイン認証技術を利用して，受け取るべきメールの判断手法や送信者レピュテーションの構築手法の研究を行っている．送信者レピュテーションには，受け取るべきと判断した正規のメールサーバから，いわゆる踏み台送信によって迷惑メールが送信された場合に受け取ってしまうという課題がある．こうした事象により，送信者レピュテーションの信頼性が下がってしまうことへの対策も必要と考えている．迷惑メールの踏み台送信は，送信側では迷惑メールが送信されたかどうかを判断できない場合が多く，受信側からの苦情などの連絡がなければ送信側でも気がつかない．そのため，迷惑メールの踏み台送信は，メールの送受信側双方にとって対策すべき共通の課題である．

本論文では，必要なメールが確実に受信者に届くようなメール環境の実現を目指して，送信ドメイン認証技術を利用した以下の2つの手法について提案する．まず，転送メールに着目し，転送メールの送信サーバを受け取るべき正規の送信元として送信者レピュテーションを構築する．メールの転送方法には，送信者情報を書き換える場合とそのまま設定する場合の2つの転送方法があり，これまでは送信者情報を書き換える転送メールを判断できなかった．この課題を解決するため，送信ドメイン認証の結果を用いて，送信者情報を書き換える転送メールを判断する手法を示す．これによって得られた送信者レピュテーションを，実際の受信メールに適用させることで評価を行う．次に，構築した送信者レピュテーションを利用した場合，受け取るべきと判断したメールに迷惑メールが含まれている事例を，実際のメール受信記録を用いて示す．こうした迷惑メール送信を止めるために，信頼性を向上させた新たなフィードバックループの仕組みを提案する．フィードバックループは，迷惑メールの受信側がその送信側に受信したことを通知する仕組みの1つであり，この仕組みを運用するためには，メールの送信者を正しく認識できることが求められる．これらメールの送信者を認識するために，送信ドメイン認証技術を利用する．

本論文では，2章で研究の背景となる送信ドメイン認証技術の概要について述べ，それを用いたこれまでの送信者レピュテーションの構築手法について述べる．また，フィー

[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

ドバックループを構成するうえで検討すべき課題について整理する．3 章では，送信ドメイン認証技術を利用して転送メールを判断する新たな手法について述べ，これらが受け取るべき正規のメール送信元であることを，実際のメールの受信記録情報（ログ）を利用して検証する．4 章では，正規のメールサーバから迷惑メールが送信されていることを抽出する手法について述べ，こうした踏み台送信をなくすため，送信ドメイン認証技術を利用したフィードバックループの仕組みついて提案する．5 章では，これら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利用と，フィードバックループについて考察する．

2. 背景と関連研究

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，その認証の対象となる送信者情報と仕組みの違いにより，Sender Policy Framework（SPF）[2]，DomainKeys Identified Mail（DKIM）[3]，Domain-based Message Authentication, Reporting, and Conformance（DMARC）[4] 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，送信ドメイン名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．いずれも，メール送信側での設定が必要であり，メール受信側ではメール受信時にそれぞれの仕組みで認証処理を行う．認証結果については，メール受信者も参照できるように新たなメールヘッダ `Authentication-Results` に記載することが仕様化された．

SPF は，メール受信時に送信メールサーバの IP アドレスと，配送プロトコル上の送信者情報（envelope from）のドメイン名から，DNS 上の SPF レコードを取得する．この送信者情報は，この配送プロトコルの仕様番号（RFC5321）から RFC5321.From とも示される．SPF は，送信元の IP アドレスが SPF レコードに含まれているかどうかで認証を行う．つまり SPF は，メールの送信側が送信者情報としてのドメイン名が，どのメールサーバから送信するかをあらかじめ規定しておく仕組みといえる．SPF は，送信側の導入手順として送信ドメイン名の DNS に対して SPF レコードを設定するだけなので，普及率が高いという特徴がある．総務省の電気通信事業者らの統計データ [5] によれば，2021 年 9 月時点で 94.51%の受信メールで送信側が SPF に対応しており，88.17%が SPF の認証を pass している．

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	認証ドメイン名	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	From ヘッダ	SPF and/or DKIM

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，署名ドメイン名や関連情報を含めてメールヘッダ（`DKIM-Signature`）とし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` ヘッダから署名ドメイン名や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，DKIM 鍵レコードを取得する．取得した公開鍵を用いて，メールヘッダと本文から電子署名を検証する．認証されるドメイン名は，署名ドメイン名（SDID: Signing Domain Identifier）となる．メールの送信側で DKIM を導入するためには，送信メールサーバなどで送信するメールに対して電子署名を作成し，ヘッダとして挿入する機能を追加する必要がある．最近のフィッシングなどの増加もあり DKIM の導入も増えてきたが，SPF に比べて普及率は低い．総務省の統計データでは，2021 年 9 月時点で 70.77%が対応しており，69.52%が DKIM の認証を pass している．

DMARC は，SPF あるいは DKIM で認証されたドメイン名と，メールヘッダ上の送信者（From ヘッダ）が一致するかどうかで認証を行う．DMARC では，認証に失敗したメールの取扱いを送信側のドメイン名の管理側でポリシとして DMARC レコードに設定する．また，メール受信側から送信側のドメイン名の管理側へ，認証結果の統計情報などのレポートを送信する仕組みがある．DMARC では，ドメイン名を登録した管理側で一括して DMARC レコードを設定したり DMARC レポートが受け取れたりするように，組織ドメイン名という設定方法がある．組織ドメイン名は，登録可能な最上位のドメイン名で，この組織ドメイン名に DMARC レコードを設定すれば，同じ内容がそのサブドメイン名それぞれに設定した場合と同等となる．DMARC の仕様は，SPF と DKIM の仕様が作成された後に作られたため，特に日本での普及率は低い．筆者の調査 [6] では，2020 年 4 月に受信したメールでは 24.6%が対応しており，20.6%が DMARC の認証を pass している．登録されている jp ドメイン名全体では，2020 年 5 月時点の調査では，DMARC レコードの設定割合は 1.19%であった．

2.2 転送メールと送信ドメイン認証技術

現在のインターネット上のメール配送では，宛先のメールアドレスから受信メールサーバに直接接続しメール配送を行う．そのため，メールの受信側にとって接続元の IP アドレスは，最初のメール送信者である場合が多い．メールでは，受信したメールをあらかじめ設定した他のメールアドレス宛に自動的に送信する転送メールが利用されてきた．転送メールは，転送先では最初のメール送信者の送信元とは異なってしまう．また多くの転送メールでは，転送

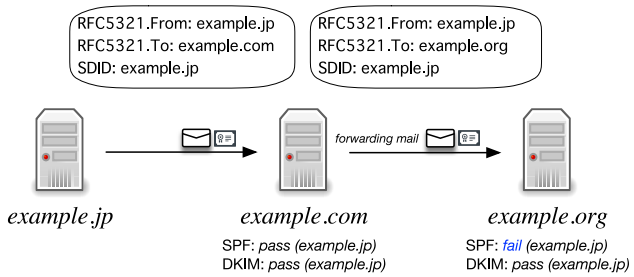

図 1 転送メールの SPF と DKIM 認証
Fig. 1 SPF and DKIM authentication for forwarding mail.

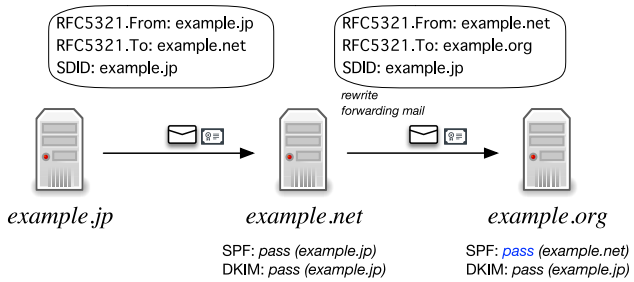

図 2 RFC5321.From を書き換える転送メールの SPF と DKIM 認証
Fig. 2 SPF and DKIM authentication for forwarding mail that rewrites RFC5321.From.

時に転送先のメールサーバに対して，配送上の送信者情報のメールアドレスとして，元のメールアドレスをそのまま利用する．そのため，転送先のメールサーバでは，送信元の IP アドレスが配送上の送信者情報のドメイン名に設定された SPF レコードに含まれないことから，SPF 認証が失敗する（**図 1**）．一方 DKIM では，メールの配送経路によらない電子署名による認証を行うため，転送メールは一般的に転送先でも DKIM 認証は pass する．

転送メールが，転送先で SPF 認証が失敗するという課題は，SPF の仕様が作成された時点からすでに明らかであった．そのため，メールの転送時に SPF の認証ドメイン名である RFC5321.From を，転送元のドメイン名に書き換える（**図 2** の example.net）といった手法が示された [7]．メールの転送時に RFC5321.From を書き換える手法は，転送先で SPF は pass するものの，SPF の認証結果を利用する DMARC では，ヘッダ From と SPF の RFC5321.From のドメイン名が異なるため，DMARC としては SPF では認証が失敗する．DKIM では，書き換える RFC5321.From は電子署名に利用するメールヘッダや本文とは異なる情報のため，DKIM 認証結果には影響しない．

2.3 転送メールと正規メールサーバ

転送メールを利用する目的としては，元のメールアドレスを継続して利用したい場合や，届いたメールを 1 カ所で参照したい場合などが考えられる．つまり多くの場合，転送メールの設定をしたメール利用者は，その転送メールを受け取るメール受信者ということになる．そのため，転送メールの受信者は，転送メールを送信するメールサーバからのメールは受け取りたいはずであり，転送メールサーバは正規のメールサーバとすべきと考える．

受信したメールが転送メールであるかを判断する手法として，DMARC レポートを利用する方法がある [8]．DMARC は，特に国内での普及率がまだそれほど高くなく，しかも DMARC レポートを送信するメール受信側もまだ少ないという課題がある．これに対して筆者らは，送信ドメイン認証技術の SPF と DKIM の認証結果の組合せを利用して，転送メールを抽出する手法を示した [9]．この手法により抽出した転送メールの送信サーバを，メールフィルタの結果を利用して，正規のメールサーバであるかを検証した．さらに正規のメールサーバを抽出する過程において，不正な SPF レコードなどを持つ迷惑メール送信元を除外するために，SPF のドメインレピュテーション（ブロックリスト）を適用する手法を示した [10]．これにより，送信者レピュテーションの判定精度を向上させることができた．これらの手法は，メールの転送時に SPF の認証ドメイン名である RFC5321.From を書き換えない転送元を対象にしたものであり，図 2 のように転送時に RFC5321.From を書き換える転送元を抽出できていない．また，送信ドメイン認証技術の SPF と DKIM の認証結果はいずれも pass であるため，転送メールでない通常のメールとは区別がつきにくいという課題がある．

2.4 正規メールサーバからの踏み台送信

送信者レピュテーションとして，評価の高い受け取るべき送信元を踏み台にして迷惑メールが送られる場合がある．オンラインなどで契約できる個人向けメールサービスなどを利用して，正規のメールサーバから迷惑メールを送信する場合や，マルウェアに感染するなどによって，送信のための認証情報を窃用されたり，感染した PC から正規のメールサーバを経由して送信する場合などである．さらに送信側のメール利用者がマルウェアに感染していれば，その被害は迷惑メール送信だけにとどまらず，より多くの情報が摂取されていたり，ランサムウェアなどによってより深刻な被害をもたらしたりする可能性がある．送信者レピュテーションだけでは，こうした正規のメールサーバからの迷惑メールを防ぐことができず，マルウェアに感染した送信者の対策もできないという課題がある．

メールサービス事業者では，メール送信時には送信者認証（SMTP-AUTH）を行い，送信されたメールの情報をログなどに記録している．そのため，迷惑メールが送信された場合そのメールに関する情報があれば，メールの送信時に利用された認証情報（送信者）を特定することができる．これにより，一時的に送信時の認証を停止することで迷惑メールの送信を停めたり，その間に利用者の PC の状態を

確認したりするなどの対策を行うことができる．そのためには，正規のメールサーバから送信された迷惑メールに関する情報を得ることが必要であり，そのための仕組みの構築が必要となる．

2.5 フィードバックループ

迷惑メールの受信側がその送信側に受信したことを通知する仕組みは，メール業界で検討が行われ [11]，元の迷惑メールを MIME（Multipurpose Internet Mail Extensions）形式で取り込む形式が ARF（Abuse Reporting Format）として規格化された [12]．この ARF 形式のメールで通知する仕組みがフィードバックループである．

フィードバックループを機能させるためには，メールの送信者を正しく認識できることが求められる．迷惑メールが送信され，その送信元が正しく認識できなければ，フィードバック先を判断することができない．またなりすましメールなどによって，誤った通知先にフィードバックしてしまうことがないような仕組みも必要である．フィードバックを受ける側としては，受信したフィードバックに含まれるメールが，実際に送信したメールであるかが確認できなければならない．

筆者の 1 人は，メール受信側からの迷惑メールの報告に ARF と送信ドメイン認証技術を用いるフィードバックループの仕組みと，フィードバックされたメール情報から送信者レピュテーションを構築することを提案した [13]．この仕組みを，迷惑メールの踏み台送信の対策に利用することを検討する．

3. 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構築手法

送信者レピュテーションの構築のために，正規メールの送信元としての転送メールの送信サーバを抽出する手法について述べる．通常の転送メールの送信者を抽出する手法については，SPF の認証が失敗し DKIM の認証が成功するメール送信者を抽出する手法として述べた [9]．ここでは，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を抽出する手法について述べ，従来の手法とあわせて送信ドメイン認証技術の認証結果を利用し，転送メールの送信サーバを判断する手法について述べる．

3.1 送信者情報を書き換えるメール転送

SPF の認証失敗を防ぐ目的で，メール転送時に RFC5321.From を書き換える送信元は，転送先での認証結果だけでは転送元と判断できない．DKIM では，メールの配送経路によらない電子署名を用いた送信ドメイン認証技術のため，最初のメール送信者が DKIM に対応していれば，転送先に届いたメールで DKIM 認証できる（図 2）．

しかし，転送されていない通常のメール送信であれば，SPF および DKIM の認証ドメイン名は同じか関連の高いドメイン名となるはずである．SPF と DKIM の認証結果を用いる DMARC 認証も，比較するドメイン名は異なるが，少なくとも 2 種類の送信ドメイン名が同じか同じ組織ドメイン名であることを認証の仕組みとしている．つまり関連のない複数の送信ドメイン名を用いる送信元は，一般的な送信元ではないといえる．これらのことから，SPF 認証が pass するメール送信元から，DKIM 認証が pass するドメイン名（署名ドメイン名）が複数ある場合は，RFC5321.From を書き換えて転送する送信元である可能性が高いと考えた．送信者レピュテーションの構築手法として，これらのメール送信元も転送メール送信元として抽出し，正規のメール送信元とする手法を提案する．

3.2 正規メール送信元の抽出手順

転送メールの送信サーバを正規メール送信元として，メールの転送時に SPF の認証情報である RFC5321.From をそのまま転送するメール転送元と，RFC5321.From を書き換えるメール転送元の両方を抽出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（$1 \leq i \leq |M|$）とした場合の，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．$srcip(m_i)$

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

	判定分類	SPF pass %	DKIM pass %
ham	88.3%	68.8%	37.7%
spam	11.7%	2.3%	0.3%
total	100.0%	71.1%	38.1%

表 3 送信者レピュテーションの抽出
Table 3 Collection of sender reputation.

送信者レピュテーション	抽出数
転送 IPs（fwIPs）	15,169
legit SPF domains（old）	744,660
legit SPF domains（rewite）	11,164
SPF block list	155,088

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．本アルゴリズムでは，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 以上である場合とした．

この手順を適用して抽出した正規メールについて，3.4 節で概要を説明する．

3.3 送信者レピュテーションの抽出

実際に運用しているメールサービスで受信したメールの記録（ログ）を利用し，転送メールの送信サーバの抽出と，受信時に実施した送信ドメイン認証の結果を利用して SPF 認証ドメイン名を抽出する．対象とした受信メールは，2019 年 9 月の 1 カ月間に受信した約 3 億 4 千万通とした．受信メールは，すべて迷惑メールフィルタおよび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，受信時に SPF，DKIM，DMARC の送信ドメイン認証を実施している．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．受信したメールの概要を**表 2** に示す．表で示した割合は，全受信メールに対する割合を示している．

この受信ログから，Algorithm 1 を用いて，正規 SPF 認証ドメイン名を抽出する．抽出した結果を**表 3** に示す．まず，メール転送時に送信者情報（RFC5321.From）を書き換えないメール転送元と思われる送信元の IP アドレス（fwIPs）を抽出する．次に同じ受信ログから，メール転送元と思われる送信元の IP アドレス（fwIPs）から送信され，SPF 認証が pass した SPF 認証ドメイン名（legit SPF domains(old)）を抽出した．以前の研究では，送信元の IP アドレスを送信者レピュテーションとして利用するため，この SPF 認証ドメイン名が pass するメール送信元 IP アドレスをさらに抽出して検証に利用したが，IP アドレスはメールサーバの変更などにより変わる可能性があるデータであるため，今回は Algorithm 1 どおりにドメイン名（SPF 認証ドメイン名）を送信者レピュテーションとして利用した．

同様に，送信者情報（RFC5321.From）を書き換える転送元と思われる SPF 認証ドメイン名（legit SPF domains(rewrite)）を抽出した．抽出に際し，同じ SPF 認証ドメイン名の送信元から送信された DKIM 認証ドメイン名の数は 2 以上とした．

さらに，不正な SPF レコードを設定したドメイン名を除外するために，受信メールがすべて迷惑メール（spam）と判定された SPF 認証ドメイン名を抽出して SPF ブロックリスト（SPF block list）とした．

表 4 送信者レピュテーションの適用結果
Table 4 Sender reputation adaptation result.

送信者レピュテーション	ham（%）	spam（%）
legit SPF(old)+fwIPs	47.45	3.01
legit SPF(old+rewite)+fwIPs	58.01	3.26
legit SPF(old+rewrite-BL)+fwIPs	58.01	3.25

3.4 送信者レピュテーションの検証

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に適用することで検証を行う．対象とした受信メールは，送信者レピュテーションの抽出期間後の翌週，2019 年 10 月 1 日から 1 週間に受信した約 3 千 6 百万通である．この期間，メールフィルタによる迷惑メールの判定割合は約 9%であった．適用した結果を**表 4** に示す．

まず，メール転送時に送信者情報（RFC5321.From）を書き換えない送信元を送信者レピュテーションとして適用する．この従来の手法による適用結果を legit SPF(old)+fwIPs として示した．メールフィルタにより迷惑メールでない（ham）と判定されたメールのうち，47.45%の受信メールがこの従来の送信者レピュテーションに適合した．その一方で，迷惑メール（spam）と判定されたメールのうち，3.01%が適合した．

次に同じ受信メールに対して，メール転送時に送信者情報（RFC5321.From）を書き換える送信元を含めた送信者レピュテーションを適用した結果を legit SPF(old+rewrite)+fwIPs として示した．同様に ham に対しては 10.56 pt 増え 58.01%となった．spam に対しての増加は 0.25 pt で 3.26%となった．受信メールのいずれの分類でも適合割合が増えたが，迷惑メールでない（ham）メールに対する増加割合がより大きかったことから，受信許可リストとしての送信者レピュテーションとしては，受け取るべきメールをより多く判断できたといえる．さらに，この送信者レピュテーションから，SPF のブロックリストを除いた送信者レピュテーションを適用した結果を

legit SPF(old+rewrite-BL)+fwIPs として示した．ブロックリストを適用することで，ham の受信メールに対する割合はほぼ変わらず，spam の受信メールに対しては 0.01 pt とわずかであるが減少した．この結果から，SPF のブロックリストを適用したことにより，迷惑メール（spam）を受け取るべきと判断する，いわゆる誤判定の割合が改善されたといえる．

4. 踏み台送信対策としてのフィードバックループ

送信者レピュテーションを適用した結果から，受け取るべき正規のメール送信元から迷惑メール（spam）が送信されていることが分かった．正規のメール送信元から spam が送信される理由の 1 つとして，メールサーバが踏み台に利用されている可能性が考えられる．これを検証するため，spam が転送メールではなく正規のメールサーバから直接踏み台送信されていることについて検討する．

次に，こうした正規のメールサーバから送信される spam の対策として，メール送信元に通知するフィードバックループの仕組みを提案する．

4.1 踏み台送信メール

正規のメールサーバから踏み台送信された迷惑メールは，表 4 の spam 割合部分に含まれると考えられる．これらの spam メールについて，メールサーバから直接送信されたメールを抽出する．

適用した送信者レピュテーションは，転送メールの送信サーバでもあるため，転送された spam メールも含まれると考えられる．転送メールに対する送信ドメイン認証の結果は 2.2 節で述べたとおり，SPF が fail するか，SPF と DKIM が pass する場合はそれぞれの認証ドメイン名が異なる結果となるはずである．つまり，転送メールで SPF が pass するということは，転送元で SPF の認証ドメイン名（RFC5321.From）を書き換えており，そこで DKIM が pass する場合はメール転送元とは異なる最初のメール送信者が DKIM 署名を付加しているということになる（**図 3**）．

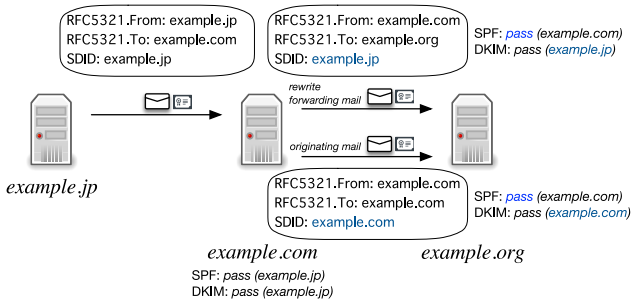

図 3 転送メールと直接送信メールの送信ドメイン認証
Fig. 3 Sender authentication results for forwarding mail and originating mail.

そこで，転送メールではない直接送信しているメールを抽出するために，SPF と DKIM の両方が pass するメールに対して，それぞれの認証ドメイン名が一致するメールを抽出する．実際には，SPF と DKIM の認証ドメイン名がまったく同じでなくても，DMARC の認証と同様に組織ドメイン名が同じ場合には同じ管理元から送信されていると判断し，認証ドメイン名の組織ドメイン名が一致する場合は同じドメイン名として扱った．

表 5 に，メールフィルタで spam 判定されたメールについて，以下の条件でそれぞれメールを抽出し，spam に対する割合で示した．

(1) 送信者レピュテーション（legit SPF(old+rewrite-BL)+fwIPs）に適合
(2) SPF および DKIM の認証が pass
(3) SPF および DKIM の認証が pass で認証ドメイン名が同じ組織ドメイン名
(4) 正規メール送信元 (1) の中で転送ではないメール (3) に適合

正規のメールサーバから直接送信された spam は条件 (4) に適合することになる．

spam の中で，SPF と DKIM の両方の認証が pass するメール自体が 2%台と割合が少ないために，この手法で抽出できた正規メールサーバから直接送信されたと考えられるメールの割合も 0.23%と低い結果となった．しかしながら，0 ではなくある程度の踏み台送信メールがあったということは，送信側に spam 送信を行っている利用者あるいは利用者の認証情報を悪用する者が存在している可能性がきわめて高いといえる．こうした spam 送信者は，今回の調査対象としたメールサービスだけではなく，他の宛先へも spam 送信していると考えられるため，実際にはより多くの spam 送信に関わっている可能性が高い．また，こうした送信者については，単に spam 送信だけにとどまらず他のセキュリティ的な脅威をもたらす可能性もあるため，早急に対策すべき問題でもある．その対策のためには，メール送信側に spam 送信されていることを伝えることが必要である．

4.2 フィードバックループを組み込んだメールシステム

フィードバックループを実現するうえで重要なことは，正しく最初のメール送信元を認識すること，その送信元が

表 5 踏み台送信メールの抽出
Table 5 Extraction of compromised account emails.

メール抽出条件	spam での割合（%）
(1)	3.25
(2)	2.52
(3)	2.32
(4)	0.23

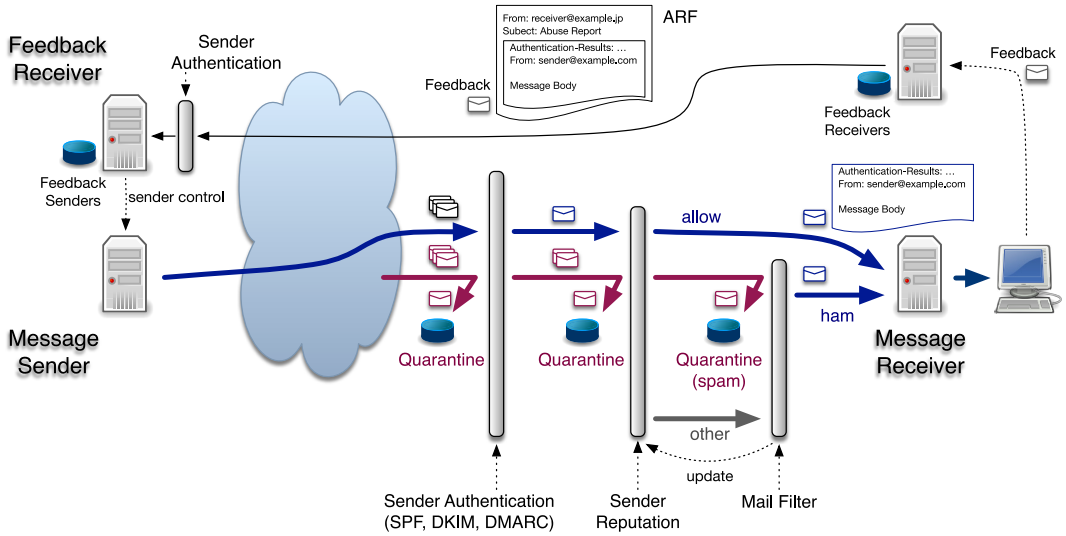

図 4 フィードバックループの構成
Fig. 4 Feedback loop framework.

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．そのためには，まずメール受信時に送信ドメイン認証によってメール送信元を認証し，転送メールでないことも確認できることが必要である．**図 4** に，送信ドメイン認証技術を利用したフィードバックループの構成例を示す．図 4 を用いて，フィードバックに関わる送信者を認証するフィードバックループの仕組みを以下のように提案する．

メール受信側が，フィードバック対象のメールであるかを，メール受信時に認証したドメイン名を用いて確認する．具体的には，あらかじめドメイン名単位でフィードバック受け取り先をリストなどで管理する（図 4 の Feedback Receivers）．利用する送信ドメイン認証技術については，配送経路によらない DKIM での認証が望ましい．SPF による認証では，pass したとしてもメール転送元からの転送メールである可能性もあるため，3.2 節で示した転送メールの確認手順を利用する．具体的には，(1) SPF 認証が pass し，(2) DKIM 認証が pass したドメイン名が SPF 認証ドメイン名が同じ組織ドメイン名である，場合がフィードバック先となる条件となる．メール送信者が DMARC に対応していれば，DMARC が pass したドメイン名でフィードバック受け取り先であるかを確認することもできる．フィードバックすべきメール送信元であることを判断できない場合は，フィードバックしない．

フィードバックを受け取るメールの送信側では，不要なフィードバックを受け取らないために，受け取るべき送信者であるかどうかを正しく認識できる必要がある．そのためには，フィードバック受信時に送信ドメイン認証を行い，認証された送信ドメイン名が受け取るべき送信者であるかを認識できる仕組み（図 4 の Feedback Senders リスト）が必要となる．このリストには，認証されたドメイン名とその認証に用いた送信ドメイン認証技術の仕組み（SPF, DKIM, DMARC）をあわせてリスト化する．フィードバックのメールは，メール転送のように再配送などされて届くとは考えにくいので，受け取ったメールをいずれかの送信ドメイン認証技術を利用して判断することができる．受け取ったフィードバックのメールから，ARF 形式の元の送信メールを抽出し，その受信時の送信ドメイン認証結果から，実際に送信したメールかであるかを確認する．実際に送信したメールである場合，そのメールの送信ログなどから送信時の認証情報を確認し，一時的にメール送信を停止（認証停止）するなどによって，spam 送信を抑制するといった対策を行う．

フィードバックを送信する相手（メール送信者）や，フィードバックを受け取る相手（メール受信者）は，あらかじめ相互登録制によってそれぞれドメイン名をリストとして組み込んだり，契約などによって登録したりするなどの方法が考えられる．

図 4 では，受信側での送信者レピュテーションの利用例も含めた．メール受信時の送信ドメイン認証およびその認証結果を用いた送信者レピュテーションの適用，送信者レピュテーションで判断できなかった場合のメールフィルタ適用によって，メール受信者には spam がほぼ届かなくなるはずである．受信したメールが明らかに spam であると判断できれば受信拒否することもできるが，誤判定などを考慮すれば，spam 判定されたメールを一定期間隔離（quarantine）するといった受信対応も考えられる．送信メールサーバを踏み台利用などされ正規のメールサーバからの spam がメール受信者に届いてしまった場合は，メール受信者からウェブメールなどの [spam] ボタンなどにより，フィードバックメールを作成し送信することで，フィードバックループを実現する．

5. 考察

メール転送時に，SPF の認証対象である RFC5321.From を書き換える送信元を抽出する手法を示し，これを正規メールの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示した．この手法を用いて，実際のメールサービスで受信したメールの受信記録を用いて送信者レピュテーションを抽出し，送信者レピュテーションの抽出期間以外に受信したメールに対して，メールフィルタの判定結果を用いて分類した．その結果，本論文で提案した手法を含めて構築した送信者レピュテーションでは，迷惑メールでない（ham）と判定されたメールに含まれる割合が増加し，迷惑メール（spam）と判定されたメールに含まれる割合がわずかに増加するという結果となった．これらのことから本論文の手法により，正規のメール送信元をより多く抽出できるようになり，送信者レピュテーションの構築手法を改善することができた．

送信ドメイン認証の結果と認証したドメイン名との関係を調べることで，正規のメール送信元を踏み台利用して送信される迷惑メール（spam）の存在を示した．こうした踏み台送信される spam を改善していくための手法として，spam 送信元に通知行うフィードバックループの利用を提案した．フィードバックの信頼性を高めるための手法として，送信ドメイン認証技術と認証されたドメイン名リストを利用するフィードバックループを提案した．また，正規のメール送信元からの spam 送信は，踏み台送信だけではなく転送されたメールも含まれている．これら転送された spam については，送信者レピュテーションの構築での本論文の手法により，転送メールであることがある程度判断できるため，転送メールと判断したメールをメールフィルタに適用させることで，受信者に spam を直接届けないといった利用の方法も考えられる．さらに，転送メールかどうかを判断できることは，最初のメール送信元（作成者）ではない直近の送信元（転送元）へのフィードバックはしない，といった運用にも利用できる．

送信ドメイン認証技術は，SPF ではメール受信時に得られる情報（RFC5321.From と送信元 IP アドレス）と SPF レコードだけを利用し，DKIM ではメール本文を利用した電子署名を利用するためメール本文のハッシュ値計算など，一定の処理時間で結果が得られる手法である．そのため，送信ドメイン認証技術を用いる本論文の手法は，送信元の IP アドレスと認証されたドメイン名から，必要なメールを一定時間で判断できる明確な手法である．また，提案した送信者レピュテーションの構築手法は，有効性の検証のためにメールフィルタの判定結果を利用したが，送信者レピュテーションの構築には送信ドメイン認証の結果のみを利用しており，構築においても送信ドメイン認証技術のみを利用する簡便な手法である．

送信者レピュテーションの構築においても，普及率の高い SPF の認証を中心に利用しており，メール受信時の送信者レピュテーション利用時には，普及がまだ十分進んでいない送信側の DKIM の導入を必要としないなど，実際的な運用の面においても利用可能性の高い手法となっている．

6. おわりに

必要なメールを確実に受け取るためには，信頼性の高い送信者レピュテーションの許可リストが重要である．これまで転送メールに着目し，それが受信者からみれば受け取るべきメール送信元であるとして，その送信元を許可リストとして送信者レピュテーションに組み込む手法を提案した．さらに本論文では，メール転送時に送信者情報を書き換える転送元にも着目し，抽出する手法を提案した．本手法では，これらメールの転送元を正規のメール送信元として追加すべきであることを，実際の受信メールを利用して検証した．この検証結果では，受け取るべきメール（ham）の 58.01%を送信者レピュテーションだけで判断することができた．本手法により構築した送信者レピュテーションを利用すれば，より処理負荷の高いメールフィルタを適用させるメールを大幅に減らすことができる．

また，送信者レピュテーションを適用することで，正規のメール送信元から spam が送信されたことを検知できることが示された．その理由として，正規のメールサーバが迷惑メールの踏み台送信に利用されている場合があると考え，その対策としてフィードバックループの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を提案した．送信側のメールサーバが踏み台利用されていれば，送信時の認証情報が窃用されている可能性が高く，送信側ではセキュリティの観点でより深刻な状況となっている可能性がある．

電子メールのシステムは，メールの送信者とそれを受け取るメール受信者で構成される．メールマガジンなどの配信事業者を除けば，メールの送信者はメールの受信者でもあり，またその逆の立場にもなる．メールシステムの信頼性を維持していくためには，正規のメール送受信者間での信頼性を高める必要がある．そのためには，踏み台送信などの悪用があった場合には，適宜相互で連絡し合うことで対策していくフィードバックループなどのコラボレーションが必要と考えている．たとえば 4.1 節で示した，踏み台送信のメールの割合は，迷惑メール全体の 0.23%という結果であったが，送信ドメイン認証技術の SPF と DKIM に対応した直接送信された迷惑メールに対する割合としては，約 10%という結果である．これらの迷惑メールは，フィードバックループによって対策され，減らすことができる可能性が高い迷惑メールである．さらに，送信ドメイン認証技術を適切に設定するメール送信者が増えれば，この対策できる迷惑メールの割合やメール量を増やすことも期待で

きる．本論文で提案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仕組みが，こうしたメールシステムの信頼性向上に貢献できることを期待している．

謝辞 本研究は JSPS 科研費 JP21H03496，JP22K12157 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 の皆様に感謝いたします．

参考文献

[1] 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).
[2] Kitterman, S.: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1, RFC7208 (2014).
[3] Crocker, D., Hansen, T. and Kucherawy, M.: DomainKeys Identified Mail (DKIM) Signature, STD 76, RFC6376 (2011).
[4] Kucherawy, M. and Zwicky, E.: Domain-based Message Authentication, Reporting, and Conformance (DMARC), RFC7489 (2015).
[5] 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 2021-03-08）.
[6] 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/pdf/iir_vol47_report.pdf⟩（参照 2022-03-05）.
[7] JEAG (Japan Email Anti-Abuse Grouup)：JEAG Recommendation—送信ドメイン認証について，入手先 ⟨https://salt.iajapan.org/wpmu/anti_spam/wp-content/themes/iajapan/docs/senderauth.pdf⟩（参照 2022-03-05）.
[8] Konno, K., Kitagawa, N., 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).
[9] 櫻庭秀次，依田みなみ，清 雄一，田原康之，大須賀昭彦：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，情報処理学会論文誌，Vol.62, No.5, pp.1173–1183 (2021).
[10] Sakuraba, S., Yoda, M., Sei, Y., Tahara, Y. and Ohsuga, A.: Improvement of Legitimate Mail Server Detection Method using Sender Authentication, *18th IEEE/ACIS International Conference on Software Engineering, Management and Applications* (*SERA*), pp.10–14 (2021.6)
[11] Falk, J.D. and Kucherawy, M.S.: Battling Spam: The Evolution of Mail Feedback Loops, *IEEE Internet Computing*, Vol.14, No.6, pp.68–71 (2010).
[12] Falk, J.D. and Kucherawy, M.S.: Creation and Use of Email Feedback Reports: An Applicability Statement for the Abuse Reporting Format (ARF), RFC6650 (2012).
[13] 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 2022-03-05）.

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の研究に従事．2016 年度日本ソフトウェア科学会解説論文賞，2022 年度情報処理学会卓越研究賞（SE 研究会）受賞．電気学会，日本ソフトウェア科学会各会員．

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業．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．2022 年より同大学産学官連携センター長併任．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，2022 年情報処理学会卓越研究賞（SE 研究会）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．