

論文の内容の要旨

| | |
|-----------|--|
| 論文題目 | 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 |
| 学 位 申 請 者 | 櫻庭 秀次 |

第1章 序論

電子メールは、インターネット上の重要なコミュニケーション手段の一つであるが、迷惑メールによって様々なセキュリティ侵害をもたらし、その悪用が大きな社会問題になっている。この迷惑メールの対策として、メールサービスプロバイダは、メールの受信側で迷惑メールであるかを判断するメールフィルタを適用することで、メール受信者に届かないような仕組みを提供してきた。メールフィルタでの判定手法の一つには、メールの送信者情報の利用があり、これまでは送信元のIPアドレスが利用されてきた。送信元情報として、送信ドメイン認証技術の普及に伴い、認証されたドメイン名が利用可能となってきた。このドメイン名を送信者情報として利用するためには、判断基準となる送信者レピュテーションが必要となる。しかしながらその構築に関して、これまで有効な手法は提案されておらず、課題となっている。

第2章 関連研究

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技術であり、メールサービスプロバイダの間でも普及してきている。この認証されたドメイン名を送信者情報として、メールの受け取り判断に利用することが期待されており、そのための判断基準である送信者のレピュテーションの構築手法や、より性能を高めるための手法が求められている。IPブロックリストの構築では、送信された迷惑メールを収集し、その送信元のIPアドレスを収集する手法が一般的である。しかしながら許可リストの場合、必要なメールを第三者に提供することは困難であり、受け取るべきメールをどの様に判断するか、構築の元となる情報をどう集めるか、といった課題がある。

第3章 送信者レピュテーションの構築手法

本章では、まずメールフィルタの判定結果を利用して送信者レピュテーション

の構築を試みた。実際に受信したメール3億4千万通を利用し、受け取るべきメールの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の送信者レピュテーションを構築し適用した。受け取るべき送信元については、ある程度受け取るべき送信者レピュテーションとして利用できることがわかった。

次に転送メールに着目し、転送メールの送信元が受け取るべきメールの送信元と考え、それを送信ドメイン認証の結果を利用して判断する手法を提案した。さらに、転送メールの送信元を管理する送信元からのメールも受け取るべきメールとし、その送信ドメイン名を抽出する手法を示した。これらの判断手法は、送信ドメイン認証の結果が含まれる受信メールログ情報から、受け取るべきメール送信ドメイン名を抽出することができる。そのため、メール本文を必要とせず、送信者レピュテーションを構築できるという利点がある。これを同様に実際の受信メールに適用させることで送信者レピュテーションを構築し、その後受信した約8千万通のメールに適用し、受け取るべきメールの半分以上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て構築した送信者レピュテーションを併合することで、受け取るべきメールの大部分を判断することができた。これらの適用結果から、提案する新しい送信者レピュテーションの構築手法が有効であること、さらにその性能の高さを示すことができた。

第4章 フィードバックループの提案

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送信は、メール送信のセキュリティにも関わる解決すべき問題であり、送信者レピュテーションにとっても対策すべき課題である。この踏み台送信に対しては、メール受信側から送信側へ通知を行うフィードバックループが有効であるが、フィードバックを機能させるためには、送信されたメールが確かにフィードバックの受信者から送信されたものであることの確認など、フィードバック送受信間での信頼性や確認手段が課題となる。これらの確認手段に送信ドメイン認証技術を組み込み、フィードバック相互の信頼性のために認証ドメイン名のリストを利用する、フィードバックループの仕組みを提案した。

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

迷惑メール対策とメール疎通の向上を目的として、送信者レピュテーションの構築とその適用、それらを悪用する送信者対策としてのフィードバックループを備えたメールシステムを示した。

第6章 結論

本研究では、送信者レピュテーション構築の課題である、1)受け取るべきメールの判定手法と2)レピュテーションデータの元となる情報の収集方法を明らかにし、特に受け取るべきメールの送信者レピュテーションの構築手法を提案した。これを実際に受信したメール情報を利用して構築および適用し、有効な手法であることを確認することができた。さらにメール送信側にとっても脅威となりうる3)送信メールサーバの踏み台利用、に対する対策として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仕組みを提案した。

論文審査の結果の要旨

| | |
|---------|--------|
| 学位申請者氏名 | 櫻庭 秀次 |
| 審査委員主査 | 大須賀 昭彦 |
| 委員 | 田中 健次 |
| 委員 | 南 泰浩 |
| 委員 | 大坐 晶 智 |
| 委員 | 清 雄一 |

(*自筆署名の場合に限り、押印省略可)

本論文「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」は、以下に示す全6章から構成されている。

第1章では、本研究の背景、目的と意義が記述されている。背景では、迷惑メールがもたらすセキュリティ的な問題と、これまでの主要な対策手法が迷惑メールかどうかの判定であること、メール受信者が迷惑メールではない受け取るべきメールの送信元を判断できることの利点を述べている。また、受け取るべきメールの送信元を判断する送信者レピュテーションの構築のためには、受け取るべきメールそのものが得られにくいため、受信したメールの記録から判断できる手法が必要であり、その構築手法が目的であることが明確に記述されている。

第2章では、本研究の基盤となる送信ドメイン認証技術、SPF、DKIM、DMARCそれぞれの仕組みと、転送メールに関するSPFの課題とそれに対するDKIMの利点、DMARCの普及度合いについて明確に記述されている。さらに、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、本研究の認証されたドメイン名を用いた送信者レピュテーション、特に受け取るべきドメイン名の構築手法の目的について明確に記述されている。

第3章では、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手法について述べ、実際の受信メールの情報を利用して送信者レピュテーションを構築し、その収集期間と適用できた割合について評価を行った。本研究の目的である受け取るべき送信ドメイン名については、約半数の受信メールを判断することができた。次に、転送メールの送信元を送信ドメイン認証の結果を利用して判定する新しい手法を提案し、それを利用して受け取るべき送信ドメイン名を収集する手法を示した。これを実際の受信メールに適用し、送信者レピュテーションを構築した。さらにこれを次の受信メールに適用することで、受け取るべきメールの半数以上を判定できることを示した。この手法は、メールフィルタ等を

利用しない処理の負担が低い判定手法であり、判定結果も含めその手法の有効性を示すことができたことから、高く評価できる。さらにメールフィルタを利用した送信者レピュテーションと、転送メールの送信元を利用して構築した送信者レピュテーションを併合することで、受け取るべきメールの約74%を判定することができ、それぞれの構築手法と合わせた手法とその検証結果が得られたことは、高く評価できる。

第4章では、特にメール送信側のセキュリティ課題である迷惑メールの踏み台送信について、その受信側での送信ドメイン認証技術を利用した判定手法を示し、実際の受信メールに適用することで、踏み台送信が実際に行われていることを示したことは、高く評価できる。さらに、この踏み台メール送信対策として、フィードバックループを実現することが必要であり、そのためにはフィードバックの信頼性を高めることが重要であることが明確に述べられている。その信頼性を高めるために、メール送受信の双方で、送信ドメイン認証技術を利用して、フィードバックするメール情報と、その送受信者を認証し認可する仕組みを組み込んだことは、高く評価できる。

第5章では、送信者レピュテーションおよびその構築のための仕組みと、信頼性の高いフィードバックループの仕組みを組み込んだ、メールシステムの全体について明確に記述されている。

第6章では、結論として、本論文における提案内容および評価結果、さらには今後の課題が記述されている。

このように、本論文では、迷惑メール対策として、受け取るべきメールを送信ドメイン認証技術を用いて判断するための送信者レピュテーションの新しい構築手法を提案した。さらに、送信者レピュテーションを悪用するような踏み台メール送信の対策手法として、送信ドメイン認証技術を用いた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しており、優れた研究であると評価できる。

以上により、本論文は博士（工学）の学位論文として十分な価値を有するものと認める。