別紙１－１

論文審査の結果の要旨および担当者

報告番号	※　甲　第　　号

氏　　名　　北川　直哉

論　文　題　目　　プロトコル検証に基づく不正通信ホスト識別手法の研究

論文審査担当者

主　査　　名古屋大学教授　　高倉　弘喜

名古屋大学教授　　結縁　祥治

名古屋大学教授　　石井　克哉

名古屋大学准教授　　嶋田　創

紙１－２

論 文 審 査 の 結 果 の 要 旨

北川直哉君提出の論文「プロトコル検証に基づく不正通信ホスト識別手法の研究」は、インターネットに多大な悪影響を及ぼし社会問題となっている迷惑メール(spam メール)の送信元ホストに対し、それらが複数のプロトコル違反によって引き起こす不正な通信に注目することにより、正規のメール送信ホストと高精度に識別できる軽量な手法とその実装法に関する一連の研究をまとめたものであり、全体は 6 章から構成される。

第 1 章は序論であり、spam メールによって生じる社会問題の現状として、spam メール送信が行われる背景とその手法について説明し、これによって生じている被害の実態について述べている。また、spam メール対策として求められる技術的要件を挙げ、現在の対策技術の問題点について概要を述べている。さらに、これらの技術的課題を受けて、解決手法の方向性について述べている。

第 2 章は、メール配送プロトコルとして、DNS による名前解決、3-way handshake、SMTP セッション中の手続の概要について解説している。それぞれに関して、spam 送信ホストが起こすプロトコル違反を、既存研究による対策で対応できているもの、既存対策では考慮されていないものに分類している。また、本論文では対象としていないが、提案方式と併用できるメール受信後の対策と送信ドメイン認証による対策についても述べている。

第 3 章では、spam メール送信元ホストを識別するために、メール配送プロトコルの仕様に正当な送信ホストが対応しているか否か、および、その挙動の差異について主要 OS 毎に調査し、かつ、複数のプロバイダ等を用いてその挙動を検証している。また、spam メール送信元ホストがどのような違反を行なっているか、かつ、その違反をせざるを得ない背景について調査している。その調査結果に対する考察に基づき、異なる優先度を与えたメール受信ホストを設定し、一度目の配送試行を拒否し MX フォールバックによる再送動作を誘発させ、RFC に定義されたプロトコルに従って再送を行なうか否かを確認することで、正当な送信ホストと spam 送信ホストを識別する手法について提案している。また、提案手法によって、正当なホストが影響を受けないことを確認する実験についても述べている。

第 4 章では、第 3 章で提案した手法を、実環境で実装するための設計について述べている。本手法を軽量に実装するため、OS に標準装備されているアクセス制御コマンドを応用すること、および、単一 OS 上に複数の SMTP 機能を実装することで同期ズレや通信不能による動作不良を回避している。さらに、この実装に基づいた、一時ホ

別紙１－２

論文審査の結果の要旨

ワイトリストの構築法、および、これによる正当な送信ホストによる配送試行の処理手順について述べている。また、spam 送信ホストと識別した場合の一時ブラックリストへの登録、および、一時ブラックリストの管理手順についても述べている。厳密にはメール配送プロトコルに違反しているものの、提案手法と親和性が低い SMTP プログラムの存在に対し、問題回避策についても述べている。

第 5 章では、DNS の MX レコードを周期的に更新し、MX フォールバックの動作を動的に変化させることで、MX フォールバックの手順に偶然一致する spam 送信ホストを識別する手法について述べている。また、本手法を実環境で検証するためのシステム設計についても詳細な解説を行なっている。さらに、開発したシステムを、実際に存在するドメインを用いて実験を行っている。当該ドメインは、数百人規模のメールアドレスが存在し、日々2 万から 4 万通の spam メールを受信していたが、本手法により、その 95%以上を排除することに成功している。また、実験の結果、正当なメール送信ホストを誤認識していないことも確認している。また、提案システム導入前後の spam メール送信ホストの国別の分類、送信メールの傾向について分析を行い、言語環境や送信ホストの所属国による特徴の違いについて述べている。

第 6 章は結論であり、本論文の成果を纏めると共に、今後の課題について述べている。

以上のように、本論文は、インターネットにおける深刻な課題の一つである迷惑メール対策に対して、迷惑メールの送信元について綿密な調査を行い、それに基づく高精度かつ軽量な送信元の識別手法という有効性の高い技術と知見を提示している。また、実環境での実証実験を行い、新規性の高い手法でありながら、既存手法との親和性も十分であるという実用的な手法を実現したものであり、情報科学の学術上・技術上の寄与が大きい。よって、本論文提出者である北川直哉君は博士(情報科学)の学位を受けるに十分な資格があるものと判定した。