報告番号	※甲　　第　　号

主　論　文　の　要　旨

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

氏　　名　　北川 直哉

論　文　内　容　の　要　旨

世界中でインターネットが普及し，我々の社会生活において欠かすことのできない存在となっている．一方で，spam メール送信や DoS 攻撃，機密情報の漏洩等のインシデントが日常的に発生しており，セキュリティ対策の重要性が叫ばれている．

インターネットサービスの中で，電子メールは長年にわたり世界中の人々の間で最も広く利用されているサービスの一つである．しかし，大量の spam メールに起因する膨大な量のトラフィックは電子メールサービスのみならず，インターネット全体に対する重大な脅威である．

長年にわたって spam メールによる被害を軽減するための研究が広く行われており，様々な技術が提案されている．メール送信側と受信側の双方で様々な対策手法が存在するが，受信サーバにおける spam メール対策手法は，メール本体を受信した後，メールのコンテンツを解析して判定する手法と，メール本体を受信する前の段階で，送信ホストの通信挙動によって判定する手法の 2 つに大別できる．前者のコンテンツフィルタリングは判定精度が高いものの，メールデータを全て受信した後で判定処理を実施するため，spam メール送信に起因するトラフィック量の軽減には一切貢献しない．本論文では，spam メールに起因するトラフィック量を減少させる手法の提案を目的とし，メール本体を受信する前の段階で，ホストの通信挙動の特異性を様々な観点から見出すことにより，spam メール送信ホストを識別する手法に注目する．

メール受信前の通信挙動の特徴によって spam メール送信ホストを識別する代表的な従来手法に，Tempfailing や 5-Way Handshake と呼ばれる手法が存在する．Tempfailing は SMTP セッション中に一時拒否エラーを示す 400 番台の応答を行い，SMTP 接続に失敗した送信ホストが一定時間経過後に再送を行った場合には正当な送信ホストであると判断して受信する手法である．しかし，spam 送信ホストは

メール配送の信頼性よりも配送効率を優先するため，一時的エラーを受信しても再送処理を行わないことが多い．Tempfailing はこのような spam メール送信ホスト特有の動作に注目した手法であり，spam メール送信ホストによる接続を排除する効果は高いものの，受信までに長時間の遅延が発生する欠点がある．RFC5321 によれば，送信ホストは一時的エラーを受信後，少なくとも 30 分以上経過後に再送を行うよう推奨されているため，30 分以上の配送遅延が予想される．

Tempfailing の遅延問題を解決するために，5-Way Handshake と呼ばれる TCP 接続時の通信挙動に注目した手法が提案されている．RFC5321 により，送信ホストは配送先ドメインの MX レコードを問い合わせた後，その優先度順に接続を試みることが定められている．5-Way Handshake は，MX レコードにプリファレンス値の異なる 2 つの受信ホストを用意し，送信ホストから最も優先度の高いプライマリ MX に対して送られる SYN パケットに対し，プライマリ MX は SYN+ACK パケットの代わりに RST パケットで応答する．これにより，MX フォールバックを促し，セカンダリ MX への再送を受信する手法である．

5-Way Handshake の代表的な実装法として，Nolisting と Unlisting がある．Nolisting は，固定的にプライマリ MX への TCP 接続を拒否し，セカンダリ MX では常に接続を許可するものである．しかし，多くの spam メール送信ホストは MX レコードの優先度を無視するため，1 度目の配送でプライマリ MX とセカンダリ MX を区別すること無く配送を試みる．その結果，多くの False Negative が発生することになる．

Unlisting は Nolisting を強化した手法であり，MX フォールバック後の配送のみをセカンダリ MX で受信するものである．送信ホストはプライマリ MX からの RST パケットを受信すると，即座にセカンダリ MX への再送を試みる．従って，送信ホストからの 1 回目の SYN パケットに対し，プライマリ MX が即座に RST パケットを返してしまうと，プライマリ MX から通知される送信ホストに関する情報の処理がセカンダリ MX で完了する前に再送が始まってしまい，セカンダリ MX では受信の可否を判断することができなくなる．さらに，高負荷時にパケットフィルタリングの処理が遅延した場合の対応が困難になるなど，実用性に問題がある．

本論文では，5-Way Handshake が spam メール送信ホストを識別するために有効な手段であることを確認するため，MX フォールバックまでの挙動や時間について調査し，正当な送信ホストの通信挙動の特徴から “正当な送信ホストと見なす条件” を独自に定めた．この条件と spam メール送信ホストによの通信挙動を比較したところ，大多数の spam メール送信ホストによる配送ではこの条件を満たさず，両者が判別可能であることを確認した．

この知見に基づき，主要な OS が複数回にわたって SYN パケットの再送を行う機構を有することに注目した MX フォールバック検出手法について述べる．この

手法は，プライマリ MX およびセカンダリ MX のどちらにおいても全ての送信ホストからの接続を拒否する状態で待機させる．プライマリ MX に 1 度目の SYN パケットが到着するとこれを棄却し，同時に当該送信ホストを一時ホワイトリストに登録する．この登録は，プライマリ MX への SYN パケットの再送が繰り返される間に完了すれば良く，また，調査した全ての OS の中で最短のものでも再送は 9 秒間繰り返されることが観測された．このため，高負荷等の理由で一時ホワイトリストの処理が遅延した場合でも，9 秒以内であれば MX フォールバック検査を確実に実施できる．

送信ホストが一時ホワイトリストに登録されると，プライマリ MX は当該送信ホストからの SYN パケットに対し RST パケットで応答し，セカンダリ MX は接続を許可するよう一時的に対応が変化する．その結果，当該送信ホストにおいて MX フォールバックが誘導され，セカンダリ MX に SYN パケットが再送される．その後，セカンダリ MX と送信ホストの間で TCP コネクションが確立し，SMTP セッションが開始される．この手法は，調査を行った全ての OS が最初の SYN パケットの送信から 3 秒以内に 2 度目の SYN パケットの送信を行うことから，Tempfailing で発生する配送の遅延の問題を解決した．この手法により，Nolisting の判別精度の低さや Unlisting の非柔軟性等，従来の手法の様々な弱点を克服できる．さらに，システム実装の要となる一時ホワイトリストの保持時間の変化による spam メール送信ホスト判別精度の評価を行い，5 秒から 20 秒程度の設定が判別精度と負荷耐性の確保のいずれの観点からも適切であるという知見を得た．

さらに，今後精巧な spam メール送信プログラムが増加することが懸念されるため，前述の MX フォールバック検査に加え，メール送信時の挙動を様々な視点から監視することにより，spam メール検出精度を向上させることが望まれている．前述の一時ホワイトリストを用いた MX フォールバック検査の spam メール送信ホスト識別精度をさらに向上させるため，応答する MX レコードのリストを定期的に変更する特殊な DNS コンテンツサーバを用いた検査を提案する．この検査は，MX フォールバック検査の前段として，送信ホストによって参照される DNS キャッシュサーバが MX レコードの TTL を遵守し，かつ，送信ホストが正しい MX サーバを選択する機構を有するかを検査する．

このシステムを実際に spam メール収集ドメインに導入し，spam メール送信ホスト識別精度の評価を行ったところ，spam メール送信に起因する SMTP セッション数が導入前後で約 96.7%削減された．本手法は，高速かつ低負荷に spam メール送信ホストの識別が行え，また他手法と容易に組み合わせて運用することができる柔軟性や拡張性が高い MX フォールバック検出手法の長所を維持しつつ，機能拡張により判定性能をさらに高められることを確認した．