2H−02

発信者詐称SPAMメールによるサービス不能攻撃の早期検出手法

田中 清[1]　山井 成良[2]　岡山 聖彦[3]　中村 素典[4]　丸山 伸[4]　宮下 卓也[2]

1 岡山大学自然科学研究科　2 岡山大学総合情報処理センター
3 岡山大学工学部　4 京都大学総合情報メディアセンター

1 はじめに

近年，電子メールはWWWと並んでインターネットにおいて最も普及しているサービスの1つである一方で，セキュリティ上の問題の多いサービスの1つでもある．特に，SPAMメールの蔓延は大きな問題になっており，その対策は重要である．

SPAMメールによる被害のうち最も深刻なものは，発信者アドレスの詐称による自組織メールサーバへのエラーメールの集中である．現状の電子メールの仕組みでは発信者のアドレスの詐称が容易であるため，事実上全てのSPAMメールでは発信者を特定されないように発信者アドレスが詐称されている．

詐称アドレスとして実在のアドレスが使用されると，そのアドレス宛に全てのエラーメールが短時間に集中して送られ，過負荷によるMTAの停止や，SPAMではない通常メールの配送遅延が発生するなどの問題が生じる．

これに対して我々は，発信者詐称SPAMへの対策手法を提案している[1]が，本手法ではいかに早い段階でSPAMメールの兆候を検出できるかが重要になる．そこで本稿では発信者詐称SPAMに起因するエラーメールによるサービス不能攻撃の早期検出手法について述べる．

2 サービス不能攻撃検出手法

2.1 発信者詐称SPAM対策手法の概要

発信者詐称SPAMに起因するエラーメールが発生すると，大量のエラーメールが短時間に集中して送信されMTAの過負荷が生じる．この時MTAが1台しかないと，どんな方法を用いたとしても全ての処理がこのMTAに集中するため過負荷は避けられない．

そこで我々は，発信者詐称SPAMへの対応策として従来用いて来たMTA(プライマリMTA)以外にもう1台のMTA（セカンダリMTA)を用意し，SPAM発生時にはエラーメールの処理を主としてセカンダリMTAで処理する方法を提案している(構成は図1)．このようにMTAの負荷分散をすることにより，通常メールの配送処理に影響を与えないようにすることができる．

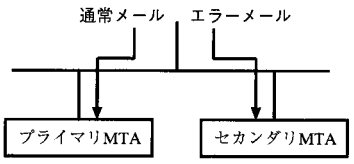

図1: SPAM発生時の配送処理

2.2 検出手法の提案

この発信者詐称SPAM対策手法の効果を十分に発揮するには，エラーメールを大量に受け取る前に，エラーメールの処理をセカンダリMTAで行えるようにする必要がある．そこで本研究では，SPAMによるエラーメールの配送過程に着目して，エラーメール受信回数とDNS問合せ回数に基づいた検出手法を提案する．以下ではそれぞれについて説明する．

2.2.1 エラーメール受信回数による検出

SPAMメールはほとんどの場合，1つの詐称アドレスを利用し1通のメールを多数の宛先に対して送信している．またその宛先についても実在するものだけでなく，SPAM発信者によって適当に作られたものも多い．場合によってはSPAMメールのほとんどが宛先誤りなどの理由によってエラーメールとして返信されることもある．当然このエラーメールは詐称アドレスに対して短時間に集中して送信される．

このことから，エラーメール受信回数を調べ，特定のアドレスに対して通常よりはるかに多くのエラーメールを受信していれば，これをSPAMによる不能攻撃の兆候であると見なすことができる．

2.2.2 DNS問合せ回数による検出

SPAMに起因するエラーメールの送信は2つの場合に分類できる．

1つは，図2に示すようにSPAMメールを発信するMTA(SPAM発信MTA)自身がエラーメールを送信する場合である．SPAM発信MTAが宛先アドレスに対応するMTA(宛先アドレスMTA)へ直接SPAMメールを送信しようとした時にエラーとなると，SPAM発信MTAは詐称アドレスに対応するMTA(詐称アドレスMTA)に直接エラーメールを送信する．

もう1つは，図3に示すようにSPAM発信MTAからSPAMメールを受信した別のMTA(SPAM中継MTA)がエラーメールを送信する場合である．例え

An early detection method of Denial of Service attack by sender-spoofed SPAM mail.

Kiyoshi Tanaka[1], Nariyoshi Yamai[2], Kiyohiko Okayama[3], Motonori Nakamura[4], Shin Maruyama[4], Takuya Miyashita[2]

[1] Graduate School of natural science and Technology, Okayama University
[2] Computer Center, Okayama University
[3] Faculty of Engineering, Okayama University
[4] Center for Information and Multimedia Studies, Kyoto University

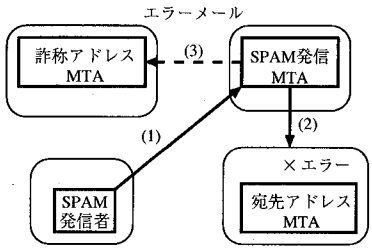

図 2: SPAM 発信 MTA によるエラーメール送信

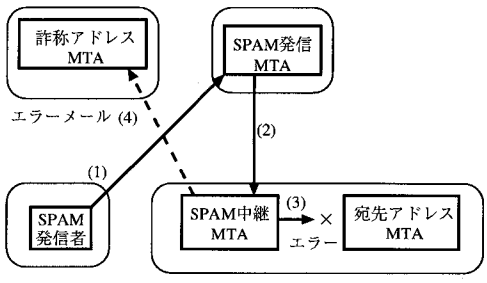

図 3: SPAM 中継 MTA によるエラーメール送信

ば，ある組織において組織外から組織内へのメール配送を中継するような MTA を設置している場合がこれに相当する．

ここで後者について考えると，SPAM メールは極めて広範囲に配布されるため，SPAM 中継 MTA の多くは通常は詐称アドレスに対応する MTA とは通信を行っていないと考えられる．このような MTA がエラーメールを送信する際には，メールの送信先アドレスに関する情報である MX レコードのキャッシュが無いので，自組織内の DNS はエラーメールの送信先の DNS に対して MX レコードの問合せを行うことになる．この問合せは多数の SPAM 中継 MTA でほぼ同時に発生するため，特定のドメインに対する MX レコードの問合せが短時間に集中して発生すると考えられる．

そこで，本研究ではこの点に着目し DNS 問合せ回数を調べ，特定のドメインに対する MX レコードの問合せが通常よりはるかに多ければ，SPAM メールによる攻撃の兆候であると見なすことができる．

3 検出手法の評価

SPAM 発生時に，どれくらいの間にどれだけの量のエラーメールを受信するのか，また，DNS への問合せはどれだけ集中するのかなど，実際に SPAM メールの被害にあわない限り SPAM 判断基準を確立することは難しい．

そこで，前節で説明した方法を評価するために，実際に別々のドメインに対し宛先誤りのエラーが発生するようなメール (以下 EX メール) を約 40 通同時に送信し，その時のエラーメールの受信状況と DNS への問合せ状況の解析結果と通常の場合の解析結果を比較し，SPAM 判断基準を検討した．

3.1 エラーメール受信回数による検出の評価

まず通常の場合のエラーメール受信ログを約 2ヵ月分解析した．その結果約 1800 のアドレス宛に約 29000 件のエラーメールが届いていることが分かった．そのうち受信件数の多い上位 4 つのアドレスと 1 分間あたりの最高受信件数を表 1 に示す．

表 1: 1 分間あたりのエラーメールの受信件数

root	addr1	addr2	addr3
81 件	20 件	10 件	4 件

EX メールのエラーメールも同様の解析をしたところ送信直後に 1 分間あたり 8 件のエラーメールを受信し，通常の場合の 4 位に相当することが分かった．実際の SPAM メールでは膨大な量のエラーメールが発生することからこれ以上の頻度でエラーメールを受信することが予想される．

このことから，エラーメールの受信ログを監視し，各アドレスの 1 分間あたりの受信件数を判断基準にすることが有効であると言える．

3.2 DNS 問合せ回数による検出の評価

次に，通常の場合の DNS の受信ログにおいて，EX メール送信と同一時間帯に 10 分間あたり何回の問合せがあるかを調査した．その結果を表 2 に示す．

表 2: 10 分間あたりの DNS 問合せ回数

平均	標準偏差
5.5 回	2.1 回

また EX メール送信直後の DNS の問合せログを見ると 10 分間に最高 11 回の問合せがあることが分かった．問合せ回数が正規分布に従うと仮定したとき，11 回以上の問合せが発生する確立は 1% 以下であることから，EX メール送信直後の DNS 問合せ回数は通常に比べて十分多いと言える．

このことから，DNS 内の各ドメインに対する問合せログを監視し，10 分間の問合せ回数を判断基準にすれば，実際の SPAM メールが発生した場合にはほぼ確実にその兆候を検出できると言える．

4 まとめ

本稿では発信者詐称 SPAM メールによる不能攻撃の早期検出手法として，エラーメールの受信回数，及び，DNS サーバへの問合せ回数を判断基準とする方法について検討し，いずれも十分に SPAM メールの兆候を検出できそうであることを示した．今後の課題としては，実際に運用して本手法の有効性を確認することが挙げられる．

参考文献

[1] 山井 成良, 山外 芳伸, 宮下 卓也, 大隅 淑弘 『発信者詐称 SPAM メールに対する対策手法』 情報処理学会分散システム/インターネット運用技術研究会研究報告 2201-DSM-22-9 pp.51-56, 2001.