コンピュータセキュリティ　18−12
(2002. 7. 18)

SPAMメール対策システムの提案と実装

齋藤　孝道† 森井　章夫†† 古森　貞††† 鬼頭　利之†††

† 東京工科大学　〒192-0982 東京都八王子市片倉町 1404-1
†† 株式会社インテック
††† 東京理科大学　〒278-8510 千葉県野田市山崎 2641
E-mail: †saito@cc.teu.ac.jp, †††{komori2000,Toshiyuki.Kito}@jcom.home.ne.jp

あらまし　これまでの SPAM メール対策は，その受信を拒否，または削除する方式が広く知られている．しかし，SMTP (Simple Mail Transfer Protocol) に基づいた電子メールシステムは，特定，または，不特定のユーザにそのサービスを提供することを目的としているため，これらの SPAM 対策方式において，SPAM メールの判定を誤ると，対策にならないばかりか，正規のメールが全く配送されなくなる問題がある．そこで，本論文では，このような判定を誤ると配送されなくなるような問題を解決しつつ，SPAM メールの抑制を狙う対策方式を提案する．また，本論文では，実現方法を示し，その評価実験に関しても説明を行う．

キーワード　システムセキュリティ，SPAM メール

The active SPAM Buckler: Preventing the SPAM

Takamichi SAITO†, Akio MORII††, Tadashi KOMORI†††, and Toshiyuki KITO†††

† Tokyo University of Technology　Katakura-machi 1404-1, Hachioji, Tokyo, 192-0982, Japan
†† INTEC Inc.
††† Tokyo University of Science　Yamazaki 2641, Noda, Chiba, 278-8510, Japan
E-mail: †saito@cc.teu.ac.jp, †††{komori2000,Toshiyuki.Kito}@jcom.home.ne.jp

Abstract　In recent years, while E-mail over an internet has achieved popularity, there is a great trouble, i.e. the SPAM mail. Although some countermeasures against the SPAM mail is proposed, the SPAM mail is coming persistently. On the other, an oversensitive way of countermeasure can refuse and eliminate legitimate E-mails. Hence, we propose a countermeasure that guarantees legitimate E-mails must be delivered. In this paper, we will explain the proposed system and show some experiments on it.

Key words　System Security, SPAM mail

1. はじめに

現在，SPAM メールは，社会問題の域にあり，様々な対策方式が提案されている．本論文では，新たな SPAM メール対策の方式を提案し，実装を行いその有効性について考察する．

SPAM メールの定義は，一般的には，「配送されることを望んでいないのに送られてくる電子メール」である [1]．この定義はユーザの主観も含まれるので，SPAM メールを送信する行為自体や，個別のユーザに届くすべての SPAM メールを排除することは現実的には不可能である．

上の定義は，ユーザの観点にあるので，ここで，電子メールシステムの観点から，SPAM メールにおけるある事例をもとに考察してみる．例えば，ある携帯電話会社のユーザの電子メールのアドレスは，デフォルトで，090 で始まる 11 文字の数字から構成されているとする．このため，スクリプトなどを用いて，様々な組み合わせを生成するなどして，様々なアドレスにメールを送信することが行われてしまう．それにより，存在するアドレスを発見する試行を繰り返し，一旦，有効なアドレスと判明した場合，永続的に SPAM が送信される．その携帯電話会社は，その対策として，アドレスとして簡単に類推できないアドレスを利用することを推奨したとしても，SPAM メール送信者が一般的な単語を組み合わせて，様々なアドレスを生成し送信することにより，同様の行為が実現できることは容易に考えられる．

上の事実を電子メールのユーザを多数抱えるサーバの観点から鑑みると，「SPAM メール送信行為」は，SPAM メールを出す主体は複数あるが，各主体が上述の試行を含めて大量の電子メールを送信する行為と想定できる．したがって，本論文では，ISP (Internet Service Provider) や携帯電話会社などの多数のユーザを抱えている電子メールサービスを提供するシステムを対象とし，上述の「SPAM メール送信行為」を抑制する技術方式を提案する．

ところで，これまでの SPAM 対策の方式における本質的な操作は，

SPAM メールと判断された全ての電子メールの受信を拒否するか，削除されるかのいずれかであった．しかしながら，これらの方式では，正規の電子メールが，誤って SPAM メールと判断された場合，受信者の元に届かなくなるという問題点がある．元来，電子メールサーバは，様々なクライアントからの接続を許す，すなわち，オープンシステムであるため，特定の電子メールとはいえ，受け取りの拒否は好ましくないばかりでなく，誤って正規の電子メールを受け取りを拒否してしまう可能性がある．したがって，このような方式を組み込むことは，電子メールのシステムとして不備であろう．

本論文では，以上の既存システムの問題点を解決しつつ，「SPAM メール送信行為」を抑制するために，SPAM メールと判断された電子メールを拒否，または削除するのではなく，ある任意の時間内に受信する SPAM メールの量を制限する方式を提案する．この方式により，SPAM メールの大量送信を妨害しつつ，最終的には宛て先に指定されたユーザに配送されることを保証する枠組みをシステムに提供する．

2. 準　　備

2.1 用　　語

SPAM メール ：ユーザが送信されることを望んでいないのに送られてくる電子メールであり，電子メールシステムの観点では，ある特定の一つ以上の主体により大量のユーザに送信される電子メール．

正規の電子メール ：SPAM メール以外の電子メール．

SMTP クライアント ： 電子メールを送信する側の MTA (Mail Transfer Agent)．もしくは，電子メールを送信するユーザの MUA (Mail User Agent)．

SMTP サーバ ：電子メールを受信する側の MTA．

電子メールのユーザ ：SMTP サーバから電子メールの送受信サービスを享受している主体．

管理ドメイン ：SMTP サーバの管理者が，管理下におくドメイン．

2.2 電子メールシステムの概要

SMTP は，TCP/IP 上で動作する通信の主体間の通報交換の手順と制御通報を規定したプロトコルである [2]．ヘッダやサブジェクトの形式なども，定められている [3]．本論文では，この SMTP を用いた電子メールシステムを対象とする．

SMTP における電子メール送信の手順は，大きく分けて，以下の 4 つの手順から構成される．

a. セッションの開始
b. 電子メールの送信者，受信者の確認
c. 電子メール本文データの送信
d. セッションの終了

以下に典型的な SMTP セッションの例を示す．ここで，SMTP クライアントを C，SMTP サーバを S とする．

1)	$C \rightarrow S$:	(接続要求)
2)	$S \rightarrow C$:	220
3)	$C \rightarrow S$:	HELO ⟨ ドメイン名 ⟩⟨ 改行 ⟩
4)	$S \rightarrow C$:	250 ⟨ ドメイン名 ⟩
5)	$C \rightarrow S$:	MAIL FROM :⟨ 発信元アドレス ⟩⟨ 改行 ⟩
6)	$S \rightarrow C$:	250 ok
7)	$C \rightarrow S$:	RCPT TO :⟨ 送信先アドレス ⟩⟨ 改行 ⟩
8)	$S \rightarrow C$:	250 ok
9)	$C \rightarrow S$:	DATA ⟨ 改行 ⟩
10)	$S \rightarrow C$:	354 go ahead
11)	$C \rightarrow S$:	(メール本文)
	⋮	
N)	$C \rightarrow S$:	.⟨ 改行 ⟩
$N+1$)	$S \rightarrow C$:	250 ok 1008252493 qp 24575
$N+2$)	$C \rightarrow S$:	QUIT⟨ 改行 ⟩
$N+3$)	$S \rightarrow C$:	221

以上のように，クライアントがある通報を送信し，サーバからの返答を待って，次の通報を出す通信形態としている．このため，クライアントが一方的に電子メールを送信することが出来ないことに注意されたい．

また，「b. 送信者，受信者の確認」と「c. メール本文データの送信」は SMTP のセッションの制御とは別であるため，一つのセッションで，複数の電子メールを送信することができる．すなわち，上のセッションの例で，クライアントが $N+1$ 以降で，更に，5〜N のようなやり取りを繰り返すことにより，複数の電子メールの送信をすることが出来る．

クライアントの接続要求から，サーバのコネクション終了確認 (**221**) までを，本論文では，**SMTP セッション**と呼ぶ．また，SMTP セッションにおいて，**MAIL FROM**:からピリオド（上の例の 5〜N）までで送信されるデータを**メール本体**と呼ぶ．また，メール本体の **DATA** より後で，行頭が改行コードの直前の行までを**（メールの）ヘッダ**と呼び，行頭が改行コードの直後からピリオドの前までを**メール本文**と呼ぶ．

2.3 SPAM メールの配送方式

一般の電子メール，特に，SPAM メールの配送には，主に以下の 2 つのタイプがある．

（1） 送信者が，配送先の SMTP サーバ に直接接続して，SPAM メールを送信する方式．これをここでは直接接続方式と呼ぶ．

（2） 送信者が，インターネット上の一個以上の MTA を中継して，配送先の SMTP サーバに配送する方式．これをここでは間接接続方式と呼ぶ．

直接接続方式では，ある一つの IP アドレスからの SPAM メールを送信する SMTP クライアントからの SPAM メールを受け取ることになる．受信者が特定したあるアドレスからのメールを拒否することも可能であるが，ダイヤルアップ環境下など，接続ごとに IP アドレスが異なるときは，その SMTP クライアントの IP アドレスを特定することは困難である．

間接接続方式では，外部からのメールの中継を許可しているか，中継の制限が掛けられていない MTA を中継して，SPAM メールを配送する．この方式は，一般に，送信元の隠蔽を目的に使用される．つまり，メールを中継した MTA を SPAM メールを配送する MTA と見せかけることができる．

2.3.1 既存の SPAM メールの対策方式

一般的な SPAM メール対策として，SMTP サーバにメールアドレス，ドメイン名，SMTP クライアントの IP アドレスなどをあらかじめ登録しておき，それらによってメールを受信するかどうかを判定する方式がある．これは，sendmail を始めとする多くの MTA で実装されている．また，ORDB (Open Relay Database) [4]，MAPS (Mail Abuse Prevention System) [5] といった，不正中継を行う MTA の

データベースを参照して，登録されている SMTP クライアントからのメールの受信を拒否する方式もある．

SPAM メールが送信元を隠蔽することが多いことから，送信元を特定するために，以下のような対策が提案，実装されている．

Anti-Spam Recommendations for SMTP MTAs

MTA で SPAM メールを防止する手法を提唱している [6]．しかし，SMTP に送信者を認証する確実な方法はないため，利用できる環境が限定される．

SMTP Authentication

SMTP に対して認証を行う AUTH 要求の拡張を定義している [7]．認証には SASL (Simple Authentication and Security Layer) を用いる．この拡張は，qmail，sendmail 8.10/8.11 などで実装されており，MUA は Outlook 4.0/5.0 などで対応されている．

Secure SMTP over TLS

TLS (Transport Layer Security) を用いる方式で，証明書によってサーバやクライアントを確認し，通信路を暗号化する [8]．

POP before SMTP

POP3 (Post Office Protocol, version 3) の認証を利用して，ユーザの確認を行う．POP3 によるユーザの認証が終ったあと，一定時間内で SMTP によるメール送信が可能になる．

以上は，いずれも，クライアントとサーバとの認証により，発信者を特定しようという方式である．しかしながら，発信者を特定することは直接の SPAM 抑制ではない．

このほかに，送信者アドレスと SMTP クライアントのドメインの比較方式を用いた対策が提案されている [9]．すなわち，配送された電子メールの送信者のメールアドレスと，その電子メールを配送した SMTP クライアントのドメイン名を比較し，一致しないものを SPAM メールとみなす．しかしながら，この方式では，正規な中継を経て配送される電子メールは，すべて SPAM メールと判断されてしまい，配送されなくなる．また，SMTP クライアントのドメイン名や，送信者のメールアドレスを，別の実在する SMTP クライアントのドメイン名やメールアドレスに詐称した場合，この方式では，SPAM メールを排除できない．

最近では，大量の到達不可能メールによる受信拒否するという方式も提案されている．すなわち，多くのユーザーに一斉に送られ，到達不可能のアドレスが多く含まれているメール群を SPAM メールとみなす方式である．当然，この方式では，大量の到達不可能メールが現れない限り，SPAM メールの受信を拒否することはできない．例えば，到達不可能メールが発生する確率を適当に低くして，SPAM メールの配送を行う場合，SMTP サーバが設定した到達不可能メール数の閾値を下まわるので検知できない．また，到達不可能メールを多く含むメーリングリストは，SPAM メールとして排除されてしまう可能性もある．

3. 提案システム

3.1 システムの利用環境とその要件

ここでは，既存の方式の問題点を解決するために，前述のとおり，受信 MTA が受け取りを拒否せずに「SPAM メール送信行為」を抑制するシステムの要件とその利用前提を述べる．

3.1.1 利用前提

まず，提案システムを利用する前提について述べる．ここでの，管理ドメインは提案システムである Proxy サーバ（後述）の保護下にあるドメインとする．

（1） SMTP サーバがある当該管理ドメインは大規模とする．

（2） 管理ドメイン宛てのメールはすべて Proxy サーバを経由する．

1 により，管理ドメインには，SPAM メールの受信対象となるユーザが多数存在し，ある任意の単位時間以内に大量の SPAM メールが送られてくるものとするとする．

また，2 により，SPAM サーバも含めた SMTP クライアントから送信される電子メールは，Proxy サーバを中継して，SMTP サーバに転送されるとする．ただし，SMTP サーバが電子メールの送信側となる場合は Proxy サーバを中継する必要は無い．

3.1.2 システムの要件

（1） 単位時間当たりに管理ドメインへ送信される SPAM メールの数を減らす．

（2） 正規のメールを SPAM メールと誤認した場合でも，ユーザに配送させることを保証する．

（3） 既存の SMTP，つまり，プロトコルを変更しない．

（4） 既存の電子メールのシステム構成に付加する形で実現する．

（5） SPAM 送信者に対する予備的な情報を利用しない．

ここで，1 と 2 の要件は前述の提案のとおりであるが，3，4 については，実際に，SPAM 対策システムを既存の電子メールシステムに導入するためには必要であると考えられるため，要件として含める．また，ORDB，MAPS などの SPAM 送信者に対する予備的な情報などに依存するシステムであると，その情報が現状と比べて正しくないときや古いとき，SPAM メール送信行為を抑制できないため，本提案では要件 5 を含める．

3.2 システムの構成

ここでは，既存の電子メールのシステム構成に，上述の 3.1.2 の要件を満たすために，新たに，Proxy サーバを導入した提案システムが想定する主体構成について説明する．

（1） **悪意ある SMTP クライアント**

SPAM メールを送信する SMTP クライアント．以降，**SPAM サーバ**と呼ぶ．

（2） **正規の SMTP クライアント**

SPAM メールではなく，正規の電子メールを送信する SMTP クライアント．本論文では，SPAM サーバとは区別する．しかし，当然，正規の SMTP クライアントが「SPAM 送信行為」するときには，SPAM サーバとみなす．

（3） **Proxy サーバ**

SPAM メール抑制のためのプロクシサーバで，今回，C 言語を用いて実装した．

（4） **SMTP サーバ**

電子メールの受信者のメールボックスが存在する SMTP サーバ．

ここで，SPAM サーバも含めて SMTP クライアントを C として，SMTP サーバを S とする．Proxy サーバを P とし，ある x 番目の任意のメッセージを Msg_x とする．このとき，SMTP クライアント C が送信する全ての SMTP の通信プロトコルにおける通報は，以下のように，必ず Proxy P を経由するものとする．

$$
\begin{array}{lll}
1) & C \rightarrow P: & Msg_1 \\
1') & P \rightarrow S: & Msg_1 \\
2) & S \rightarrow P: & Msg_2 \\
2') & P \rightarrow C: & Msg_2 \\
3) & C \rightarrow P: & Msg_3 \\
3') & P \rightarrow S: & Msg_3 \\
 & \vdots &
\end{array}
$$

3.3 Proxy サーバの仕様

提案システムは，主に，SPAM メール検知機構部と SPAM 抑制処理部から構成される．ここでは，まず概要を述べ，そのあと，それぞれについての説明をする．

3.3.1 システムの概要

Proxy サーバは，SMTP クライアントからの接続要求を受け入れ，

SMTP クライアントと Proxy サーバとの間のコネクションを確立し，そのコネクションを子プロセスに譲渡する．その後，当該子プロセスは，SMTP サーバに接続要求を出し，SMTP サーバと Proxy サーバとの間のコネクションを確立する．

また，Proxy サーバの子プロセスにおいて電子メールのデータを中継する際，SPAM メール検知機構部を用いて，当該電子メールが SPAM メールであるかどうかの判定を，適宜，行う．SPAM でないとき，通常の転送を行う．また，SPAM メール検知機構部が当該電子メールを SPAM と判定した場合，SPAM メールを抑制転送する．

3.3.2 SPAM メール検知機構部について

提案システムにおける SPAM メール検知は，接続してきた SMTP クライアントの「IP アドレス」,「当該 SMTP セッションにおける各ヘッダ」,「当該 SMTP セッションにおける各メール本文」を用いて行う．

(a) IP アドレスによる検知機構部

任意のある時間 T_{ip}（これを**サンプリング時間**と呼ぶ）以内に，ある IP アドレス ip を持つ SMTP サーバから，任意のある大きな数 N_{ip} を越える SMTP 接続となるとき，Proxy サーバの当該 SMTP セッションを通常の転送状態（後述）から，抑制状態（後述）に移行させるための判定機構をもつ．すなわち，当該機構部は，SMTP クライアントからの接続があったとき，当該 ip をファイル $file_{ip}$ に保存する．また，$file_{ip}$ を参照して，T_{ip} 以内に，$SPAM_{ip} \geqq N_{ip}$ のとき，SPAM メールと判定をするプログラムを用意する．

(b) メールのヘッダによる検知機構部

任意のある時間 T_{hdr} (サンプリング時間) 以内に，SMTP 接続が行われ，同じであると判定できるヘッダ hdr が任意のある大きな数 N_{hdr} を越えたとき，Proxy サーバの当該 SMTP セッションを通常の転送状態から，抑制状態に移行させるための判定機構をもつ．すなわち，当該機構部は，SMTP クライアントからの接続があったとき，当該ヘッダに関する情報をファイル $file_{hdr}$ に保存する．また，$file_{hdr}$ を参照して，T_{hdr} 以内に，$SPAM_{hdr} \geqq N_{hdr}$ のとき，SPAM メールと判定をするプログラムを用意する．

今回の実装では，当該電子メールのヘッダにおける `subject` が完全一致するとき，もしくは，そうでないときには，ヘッダにおいて，3 種類のある任意の文字がいくつあるかを数え上げ，それが一致するかによって，ヘッダの同定を行っている．

(c) メールの本文部による検知機構部

任意のある時間 T_{bdy} (サンプリング時間) 以内に，SMTP 接続が行われ，同じであると判定できるメール本文 bdy が任意のある大きな数 N_{bdy} を越えたとき，Proxy サーバの当該 SMTP セッションを通常の転送状態から，抑制状態に移行させるための判定機構をもつ．すなわち，当該機構部は，SMTP クライアントからの接続があったとき，当該メール本文に関する情報をファイル $file_{bdy}$ に保存する．また，$file_{bdy}$ を参照して，T_{bdy} 以内に，$SPAM_{bdy} \geqq N_{bdy}$ のとき，SPAM メールと判定をするプログラムを用意する．

今回の実装では，当該電子メールのメール本文において，3 種類のある任意の文字がいくつあるかを数え上げ，それが一致するかによって，メール本文の同定を行っている．

3.3.3 SPAM 抑制処理部について

Proxy サーバは，SMTP クライアントから接続要求があったとき，プロセスを生成し，当該セッションが終了するまで，その子プロセスに，その後の当該 SMTP セッションを引き継がせる．生成される時点で，IP アドレスによる SPAM 判定を行う．また，その後の当該セッションで一つのメール本体におけるヘッダを取得した際，ヘッダによる SPAM 判定を行い，更に，当該メール本体のメール本文を取得の際，メール本文部による SPAM 判定を行う．各々，SPAM と判定した場合，その時点で，当該プロセスは **SPAM 抑制状態**に変化する．それ以外のときには，**通常の転送状態**となる．また，今回の実装では，抑制状態にあるときには，更なる SPAM の判定は行わない．

(a) 通常の転送状態

Proxy サーバは，SMTP クライアントから受信した通報を最小時間で SMTP サーバに送信し，また，SMTP サーバから受信した通報を最小時間で SMTP クライアントに送信する．

(b) SPAM 抑制状態

SPAM 抑制状態は，**セッションサボタージュ方式**と**セッションドロップ方式**によって実現される．

(b-1) セッションサボタージュ方式

この方式は，Proxy サーバにおける SMTP セッションの各通報の中継を，ある任意の時間遅延させることにより，SPAM 抑制状態を実現する．すなわち，Proxy サーバは，例えば，当該セッションの IP アドレス ip により SPAM と判断したとき，SMTP クライアントから受信した通報をある任意の時間 TD_{ip} 経過後に，SMTP サーバに送信する．この TD_{ip} を IP による**基準遅延時間**と呼ぶ．今回の実装では，SMTP サーバから受信した通報の転送に対しては遅延を行わない．

また，メールヘッダによる基準遅延時間を TD_{hdr} ，メール本文による基準遅延時間を TD_{bdy} とそれぞれする．

(b-2) セッションドロップ方式

セッションサボタージュの場合，大量の SPAM メールが送信されているとき，SMTP クライアントとの SMTP セッションを処理しているプロセスの数が増加するため，Proxy サーバと SMTP サーバの負荷が増大する．

したがって，この方式は，Proxy サーバにおける SMTP セッションの各通報を，中継せずに，そのまま破棄することにより，SPAM 抑制状態を実現する．ただし，今回の実装において，この方式は，セッションサボタージュ方式の補佐として適用する．すなわち，Proxy サーバにおける SPAM メールを含む SMTP セッションの中継の起動プロセスが，ある任意の数 N_{proc} を越えているときには接続要求に応じない．また，その送信元 SMTP サーバからの接続要求を，その起動プロセスが N_{proc} を下回った後でも，ある任意の時間 T_{proc} 経過するまで応じない．このため，SMTP クライアントは再送をするためには，否が応でも，任意時間後に再接続しなければならない．

4. システムの評価実験

4.1 実験環境

(1) SMTP クライアント 1

MTA は sendmail (ver.8.11.4) を，DynaBook (CPU: Intel Mobile Celeron (600MHz)，メモリ: 192MB) に，OS は Turbolinux Workstation 7.0 を用いている．

(2) SMTP クライアント 2

MTA は sendmail (version 8.12.1) を，Libretto (CPU: Transmeta Crusoe (600MHz)，メモリ: 256MB) に，OS は Vine Linux 2.1.5 を用いている．

(3) SMTP クライアント 3

MTA は sendmail (ver.8.11.4) を，DynaBook (CPU: Intel Mobile Celeron (600MHz)，メモリ: 64MB) に，OS は Turbolinux Workstation 7.0 を用いている．

(4) SMTP クライアント 4

MTA は sendmail (ver.8.11.4) を，LaVie (CPU: Intel Mobile PentiumIII (600MHz)，メモリ: 128MB) に，OS は，Turbolinux Workstation 7.0 を用いている．

(5) Proxy サーバ

C 言語を用いて，提案システムを実現するためにプロトタイプを実装した．計算機環境としては，LaVie (CPU: Intel Mobile PentiumIII (600MHz), メモリ: 128MB) に，Vine Linux 2.1.5 を OS として用いている．

(6) SMTP サーバ

受信用の MTA として，qmail (version 1.03) を用いた．しかしながら，多くの実験ではエラーとならない SMTP の制御を行うので，4.2 の実験では，SMTP サーバとして SMTP サーバのダミーサーバを用いた．このダミーサーバは理想的な SMTP セッションを想定して，電子メール受信の必要最低限の処理を行う．

計算機環境としては，VAIO (CPU: Intel Mobile PentiumIII (750MHz), メモリ: 128MB) に Turbolinux Workstation 7.0 を OS として用いている．また，この計算機上に，DNS (Domain Name System) として，bind (ver.9.1.2-4) を準備した．

4.2 いくつかの実験

ここで，Proxy システムの評価をするためにいくつかの実験を行う．以下の実験において，SPAM 検知機構部におけるサンプリング時間 T_{ip}，T_{hdr}，T_{bdy} をすべて 180 秒とする．さらに，セッションサボタージュにおける基準遅延時間 TD_{ip}，TD_{hdr}，TD_{bdy} を，10 秒，30 秒，60 秒とそれぞれする．また，この実験では特に扱わないので，セッションドロップの T_{proc} は 0 秒とする．

今回の実装において，セッションサボタージュにおける一つの通報の転送における遅延時間は以下の通りとしている:

IP アドレス検知機構部	$TD_{ip} + (SPAM_{ip} - N_{ip})$
メールヘッダ検知機構部	$TD_{hdr} + (SPAM_{hdr} - N_{hdr})$
メール本文検知機構部	$TD_{bdy} + (SPAM_{bdy} - N_{bdy})$

表 1 **遅延時間**

また，以降，評価のために SMTP クライアントがメールの転送に掛かる参考時間を**転送時間**と呼ぶ．これは，SMTP サーバにおいて，SMTP 接続が開始されてから，すべての電子メールの受信を終了するまでの平均の経過時間とする．

4.2.1 電子メールの生成方法

正規の電子メールは，Subject は 64 文字，メール本文は 512 文字とし，ランダムに文字列をそれぞれ生成している．

また，ヘッダやメール本文にランダムな文字列を埋め込むなどの対抗策は容易に考えられるが，今回の実験では，同一主体からの SPAM メールはすべて同じ内容であるという仮定に基づいて，SPAM メールの内容はすべて同一としている．すなわち，Subject を `test subject` とし，メール本文を `test body` とする．

4.2.2 通常転送状態のスループット

ここで，通常転送状態のスループットを見るために，SPAM 検知機構部におけるそれぞれの閾値 N_{ip}，N_{hdr}，N_{bdy} を十分に高く設定し，SPAM と判定されないようにしておく．このとき，各々の SMTP クライアントが 200 通の電子メールを送信し，Proxy サーバが，実際に SPAM メールの判定を行い，通常転送を行った際の転送時間を，以下の通り，それぞれについて計測した．

SMTP クライアント	2 台のとき	3 台のとき	4 台のとき
1	14.2 sec	18.6 sec	29.8 sec
2	16.0 sec	21.8 sec	33.0 sec
3	—	20.6 sec	29.8 sec
4	—	—	31.0 sec

表 2 **通常状態の転送時間**

4.2.3 SPAM サーバが一台のとき

ここでは，SPAM を送信する主体（下の表の主体 4）が，400 通の SPAM メールを，一つの SMTP クライアントによって，送信してくる状況を想定した実験を行う．また，ほぼ同時に，他の SMTP クライアントは正規のものとして，閾値を超えない 200 通送信する．ここで，SPAM 検知機構部における閾値 N_{ip}，N_{hdr}，N_{bdy} をすべて 300 とする．このとき，表中の「遅延した数」は IP アドレスによる判定である．

SMTP クライアント	遅延した数	転送時間（メール数）
1 (正規)	0	38.4 sec (200)
2 (正規)	0	40.6 sec (200)
3 (正規)	0	39.2 sec (200)
4 (SPAM サーバ)	100	1455.6 sec (400)

表 3 **SPAM サーバが一台のとき**

4.2.4 SPAM サーバが分散されているとき

ここでは，SPAM メールを送信する主体が，400 通の SPAM メールを 2〜4 つの SMTP クライアントに分散して送信してくる状況を想定した実験を行う．ここでも，SPAM 検知機構部における閾値 N_{ip}，N_{hdr}，N_{bdy} をすべて 300 とする．

また，表の中の「遅延した数」の項目で，+ より前はヘッダによる判定，後ろはメール本文による判定とする．

SMTP クライアント	遅延した数	転送時間（メール数）
1 (正規)	0	26.5 sec (200)
2 (正規)	0	27.5 sec (200)
3 (SPAM サーバ)	64.0+0.25	279.75 sec (200)
4 (SPAM サーバ)	35.5+0.5	281.25 sec (200)

表 4 **SPAM サーバが 2 台に分散しているとき**

SMTP クライアント	遅延した数	転送時間（メール数）
1 (正規)	0	16.0 sec (200)
2 (SPAM サーバ)	38.2+0	265.8 sec (133)
3 (SPAM サーバ)	39.4+0.25	258.8 sec (133)
4 (SPAM サーバ)	19.6+0.4	179.4 sec (134)

表 5 **SPAM サーバが 3 台に分散しているとき**

SMTP クライアント	遅延した数	転送時間（メール数）
1 (SPAM サーバ)	28.2+0	243.4 sec (100)
2 (SPAM サーバ)	27.2+0	250.8 sec (100)
3 (SPAM サーバ)	28.8+0	258.8 sec (100)
4 (SPAM サーバ)	13.0+0	158.8 sec (100)

表 6 **SPAM サーバが 4 台に分散しているとき**

5. 考　　察

5.1 実験結果の考察

直接転送（表 3）における SPAM メールの遅延は，例えば，2 台に分散しているとき（表 4）のそれらと比べて，長くなっている．これは，IP アドレスによる検知方式だとプロトコルの最初から遅延の決定と遅延を行えるのに対して，ヘッダによる検知方式だと，その決定と遅延がヘッダを受信してからしか行えず，更に，メール本文が，今回の実験では，最少の一行であるためであるため，遅延できる機会が少ないためである．

また，分散して送信する状況を想定した今回の実験では，遅延の時間を少なめに設定したため，おおよそ，10〜16 倍程度の転送時間となっているが，分散の仕方に依存せず，遅延が掛かっていることが分かる．いずれにせよ，転送方法に依存せず，遅延時間は任意に変更できる．

5.2 運用について

まず，メーリングリストについて考察する．今回のSPAM検知機構方式では，SPAMメールと，正規の電子メールであろうメーリングリストを，区別することは困難である．しかしながら，メーリングリストのサーバを管理運営してるSMTPクライアント側では，電子メールのスプールが溢れるなどの傾向が現れるので，予め当該システムを導入した側に知らせて，そのドメイン，もしくは，メールアドレスからの電子メールに対して，遅延を掛けないように要請するなどの運用上の対策を取ることができる．

また，今回の実験では，主に，セッションサポタージュを扱ったが，大量の接続に対して長時間遅延を掛けるためには，それに応じた数のプロセスが必要である．実際に，遅延が掛っているということは，少なくとも，SPAMメールである可能性が高いので，SPAMサーバ側も相応にシステムのリソースを消費しているのだが，SPAMサーバに，適宜，より一層の負荷を掛けるためにも，プロセス数を節約できるセッションドロップを有効利用する．したがって，プロセスに関する問題も，このように運用する上で，抑制方式をどのように行うかを選択することで解決できる．

また，セッションサポタージュにおける遅延時間の設定において，SMTPクライアント側のタイムアウトついても考察する．この場合も，遅延しているということは，SPAMメールであると判定されている可能性が高く，SMTPクライアントがタイムアウトでセッションを切ったとしても，再送されることを期待すればよい．

5.3 SPAMメールに対する安全性

SSLの認証の際，接続クライアントにパズルを出して，DoSを抑制するという方式が提案されている[10]．これは，*TCP SYN flooding*のように，サーバのリソースを消費させるクライアントからの攻撃を防御するための方式として有効である．しかしながら，特に，電子メールの送信においては，すべてのクライアントに，パズルを解かせる必然性はない．したがって，本方式は，クライアントが一方的に電子メールを送信できないということを利用して，SPAMと判定できたメールについてだけ，遅延させることにより，時間と電子メールのスプールというリソースをクライアントに消費させている．

また，DoSとは直接関係ないが，UNIXマシンにログインする際，ユーザはパスワードを用いた認証を行う．この際，例えば，パスワードを間違えると，ある一定の時間をおいてからプロンプトを出すシステムがある．これは単位時間に総当りの試行回数を減らすのに有効である．本提案システムも，単に，SPAMメールの送信コストを増大させるだけでなく，有効なアドレスを探索する際の妨害になり得るであろう．

以上の事例より，攻撃的なクライアントのリソースを消費させる行為は，その攻撃を抑制するのにある種の効果があると考えられる．本論文では，このような考えに基づいて，**SPAMメールに対する安全性**としている．

5.4 他方式との融合

SPAMメールの検知機構部は，抑制処理部とは完全に独立したものであるので，例えば，広告などの用語を含む電子メールをSPAMと判定したり，存在しないメールアドレスを大量に送りつけてくるサーバからの送信をSPAMメール送信行為と判定する方式を導入してもよいであろう．しかし，いずれの方式も，単に，削除してしまったり，受け取りを拒否してしまう方式だと，正規の電子メールが届かなくなる．例えば，あるISPのユーザ達が結託して，誤操作と主張して，存在しないメールアドレスに送信したとき，そのISPからの電子メールを拒否すべきなのであろうか，という運用上の問題にも，本方式は一つの解決策を示している．

6. おわりに

本論文では，既存のSPAM対策システムの問題点を解決しつつ，「SPAMメール送信行為」を抑制するために，SPAMメールと判断された電子メールを拒否，または削除するのではなく，ある任意の時間内に受信するSPAMメールの量を制限することを行う方式を提案した．また，別の観点でみると，これまで電子メールは，そのシステム上，受け取るか，拒否するかのどちらかであったが，本提案方式の遅延という行為によって，その中間状態を作り出した．さらに，その実装システムとその評価のための簡単な実験を行った．

最後に，今後の課題としては，SPAMサーバ，SMTPサーバとProxyサーバの消費リソースの対応関係などの計測を行い，定量的な「SPAMメール送信行為」に対する安全性の定式化がある．

文　献

[1] ジェフ・モリガン: SPAMの撃退, ピアソンエデュケーション.
[2] Simple Mail Transfer Protocol, RFC821.
[3] Standaed for the Format of ARPA Internet Text Messages, RFC822.
[4] Open Relay Database, **http://www.ordb.org/**
[5] Mail Abuse Prevention System, **http://mail-abuse.org/**
[6] Anti-Spam Recommendations for SMTP MTAs, RFC2505.
[7] SMTP Service Extension for Authentication, RFC2554.
[8] SMTP Service Extension for Secure SMTP over TLS, RFC2487.
[9] 浅野 徹, 菊地 高広, 力武 健次, 永田 宏: 企業網におけるSPAM対策と実現手法, Computer Security Symposium CSS2001, pp.139-144, 2001.
[10] A. Juels and J. Brainard: *Client puzzles: A cryptographic countermeasure against connection depletion attacks*, In 1999 ISOC NDSS.