NetNews における「なりすまし投稿」の抑制

94H080 田北陽一

目 次

1 はじめに **2**

2 NetNews **3**

2.1 記事の形式 4

2.1.1 From:フィールド 4

2.1.2 Date:フィールド 4

2.1.3 NewsGroup:フィールド 4

2.1.4 Subject:フィールド 5

2.1.5 Message-ID:フィールド 5

2.1.6 Path:フィールド 5

2.1.7 Mime-Version:フィールド 5

2.1.8 Reply-to:フィールド 5

2.1.9 Sender:フィールド 5

2.1.10 Followup-to:フィールド 6

2.1.11 Reference:フィールド 6

2.1.12 Organization:フィールド 6

2.1.13 Keywords:フィールド 6

2.1.14 Summary:フィールド 6

2.1.15 Lines:フィールド 6

2.1.16 Xref:フィールド 6

3 なりすまし投稿 **8**

3.1 なりすましの定義 8

3.2 なりすます方法 8

3.3 抑制対象としている環境 9

3.3.1 NAPT 9

4 なりすまし投稿の抑制方法 **10**

4.1 ユーザー認証の方法 11

4.2 中継用プログラム 15

4.2.1 stone 15

4.2.2 estone 15

5 まとめ **16**

1 はじめに

近年インターネットは利用人口が急増しており、主に WEB コンテンツの閲覧やメイルの送受信といった用途で利用されている。この他にも、ファイル転送の FTP[1]、チャットの IRC[2]、電子掲示板としての NetNews [1] といったサービスもあり、現在も活用されている。ここでは特に、インターネット黎明期から重要なサービスの 1 つとして位置付けられている NetNews に着目した。NetNews では記事の投稿の際、投稿者のメイルアドレスを記述する事が RFC[3] によって義務づけられている。NetNews ではこのメイルアドレスを架空の電子メイルアドレスや他人の電子メイルアドレスを用いて News を投稿できてしまう。これらの実装の為、誰もが容易に送信者を偽ることができる可能性がある。特に Gateway に NAPT を導入し、クライアントマシンにプライベート IP アドレス[4] を割り当てている本学の演習室の環境では、News サーバから各クライアントマシンの IP アドレスを特定するはできない。一つ一つのマシンを一人一人のユーザに専用で割り当てている環境の場合、なりすまし投稿を行なったマシンの IP アドレスがわからないと、投稿者もわからなくなってしまう。また、複数のマシンを複数人に割り当てている環境の場合、IP アドレスとマシンの使用時刻の対応からユーザ名、つまり投稿者を特定する事が環境によって可能である。しかし、いずれの場合でも IP アドレスを特定できない場合、送信元電子メイルアドレスを偽った送信者を特定する事はできない。

本研究ではこれらの問題を解決するために、NetNews 投稿者のなりすましを抑制する事を目的とする。また抑制対象としては、Gateway に NAPT を導入している環境を想定した。

[1] File Transfer Protocol ネットワーク上のクライアントとホストコンピュータとの間でファイルの転送を行うためのプロトコル。RFC959 に詳細な説明がある。

[2] Internet Relay Chat , インターネットを利用したリアルタイムなチャットシステム。RFC1459 に詳細な説明がある。

[3] Request for Comments の略:インターネットに関する技術情報や仕様、運用規則などを定める文章。(付録参照)

[4] 組織内部のネットワークアドレスとしてインターネット上に存在しない事を保証されている IP アドレス。

2 NetNews

NetNews とはインターネット上で運営されている電子掲示板システムの事。テーマ別に掲示板がわかれおり、特定の話題について議論等を行う。それぞれのテーマは NewsGroup といった名前でツリー構造[5] にまとめられている。特にコンピュータ関連の NewsGroup では、コンピュータに関する障害を自身で解決できない人などが、解決策を知っているかもしれない他者のアドバイスを求める時などにおいて使用される。その他にはプログラムの共同開発での利用、連絡用掲示板としての利用などもある。NewsGroup において回答者はボランティアで回答している。日本における代表的な NewsGreoup には fj や japan などがある。ユーザーは News リーダ[6] をセットアップし、News サーバにアクセスする事で記事を取得できる。ユーザーから見た場合、下記の点においてメーリングリスト[7] と非常によく似ている。

1. ある特定のテーマに基づいて議論等が行われる事。
2. 参加者はサーバに対して記事またはメイルを要求する事[8]

NetNews とメーリングリストにおける違いとしては、管理者が参加可能な個人を限定できるかどうかという違いがある。メーリングリストの場合、管理者が参加者の限定する事が可能である。これに対して、NetNews の場合は News サーバを公開した集団においてのみ、NewsGroup への参加が可能である。NetNews とメーリングリストにおける違いとしては、管理者が参加可能な個人を限定できるかどうかという違いがある。メーリングリストの場合、管理者が参加者の限定する事が可能である。これに対して、NetNews の場合は News サーバを公開した集団においてのみ、NewsGroup への参加が可能である。News サーバの管理者は集団を選択するという意味においては限定が可能であるが、その集団を構成する個人個人を限定する事は不可能になっている。

[5] 枝分かれをした階層構造の事。(付録参照)
[6] NetNews において記事の閲覧や投稿などを行うソフトウェア。クライアントマシンにセットアップして使用する。
[7] インターネット上で特定のメンバに一斉同報の電子メイルを送るシステム。特定のテーマについて議論を行ったりする。
[8] 昨今のメーリングリストでは WEB サイトと連携しているものがある。この連携によって、WEB 上から投稿内容の確認、発言、転送などの設定が可能である。

2.1 記事の形式

記事の形式は記事に示すようになっている。記事は正規表現[9]による空行 (^$) を境にして記事の送信者名や投稿時刻などの情報を含む header 部分と、本文である body 部分にわかれる。記事のフォーマットは RFC1036 [2][10]で詳細に定義されており、header 部分には次の項目を含ませる事が義務づけられている。特に From:フィールドには投稿を行なう人が保持するメイルアドレスを記述しなければならない事に留意されたい。

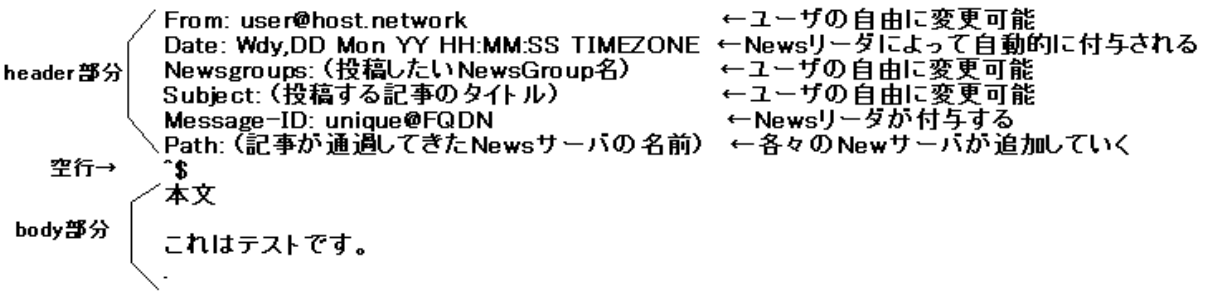

図 1: 記事の一般形

2.1.1 From:フィールド

必須のヘッダ。ユーザの保持するメイルアドレスを記述する。記事の方法は以下に示すように三通りある。メイルアドレスのフォーマットは RFC2822[11] に準拠しなければならない。

- From: takita@h-ps011.ise.osaka-sandai.ac.jp
- From: takita@h-ps011.ise.osaka-sandai.ac.jp (Yoichi TAKITA)
- From: Yoichi TAKITA<takita@h-ps011.ise.osaka-sandai.ac.jp>

2.1.2 Date:フィールド

必須のヘッダ。インターネットに投稿された日時が記述されなければならない。通常は News リーダが自動的にヘッダに記述する場合が多い。RFC822 に準拠した以下のフォーマットでなければならない。

- Date: Wdy, DD Mon YY HH:MM:SS TIMEZONE

2.1.3 NewsGroup:フィールド

必須のヘッダ。投稿を行いたい NewsGroup 名を記述する。ユーザの任意に記述が可能である。複数ある場合は、カンマ (,) で区切る。

- Newsgroup: (投稿を行いたい NewsGroup 名)

[9]文字列の一部を一般化して表現する為の手法。(付録参照)
[10]Standard for Interchange of USENET Messages:NetNews におけるメッセージフォーマットの内容について定義している文書。
[11]Standard For The Format Of Arpa Internet Text Messages: コンピュータ利用者間で送られるテキストメッセージの構文を規定した文書。

2.1.4 Subject:フィールド

記事のタイトル名を記述する。ユーザの任意に記述可能である。タイトル名は記事内容の全体像を表現しているものとする事が推奨されている。

- Subject: (記事のタイトル名)

2.1.5 Message-ID:フィールド

必須のヘッダ。ユニーク[12] な識別子。多くの場合、News リーダによってヘッダに追加される。ヘッダには空白または">" を含めてはならない。ヘッダを追加した News リーダは向こう二年間は Message-ID がユニークである事を保証する必要がある。またフォーマットは RFC822 に準拠したものでなければならない。

- Message-ID: (unique)@(FQDN[13])

2.1.6 Path:フィールド

必須のヘッダ。投稿者から購読者まで、記事がコピーされた経路。右端が投稿者側、左端が購読者側になる。マシン名とマシン名の間は、感嘆符 (!) で区切られている。

- Path: A!B!C!D!E!F

2.1.7 Mime-Version:フィールド

非 US-ASCII 文字を扱う場合にヘッダに付与しなければならない文字列。RFC2049[14] に MIME は定義されている。

- Mime-Version:1.0

2.1.8 Reply-to:フィールド

オプションのヘッダ。記事のフォーマットは From:フィールドと同じである。記事の返信を特定のメイルアドレスに指定したい場合に記述する。

- From: takita@h-ps011.ise.osaka-sandai.ac.jp
- From: takita@h-ps011.ise.osaka-sandai.ac.jp (Yoichi TAKITA)
- From: Yoichi TAKITA<takita@h-ps011.ise.osaka-sandai.ac.jp>

2.1.9 Sender:フィールド

オプションのヘッダ。記事のフォーマットは From:フィールドと同じである。記事の投稿者のメイルアドレスが From:と異なる場合に記述する。

- Sender: takita@h-ps011.ise.osaka-sandai.ac.jp

[12]世界に一つしかないという意味
[13]Fully Qualified Domain Name: ホスト名に続けて、ドメイン名まで省略せずにすべて指定した記述形式の事。(hostnema).(subdomainname).(domainname) で表現される。
[14]Multipurpose Internet Mail Extensions の略:非 US-ASCII 文字を使って、漢字やひらがな、その他様々な形態のデータを取り扱う為のプロトコルを定義したもの。

2.1.10 Followup-to:フィールド

オプションのヘッダ。記事のフォーマットは Newsgroups:フィールドと同じである。ユーザが記事の返信を行った際に、記事が投稿される Newsgroup 名。このフィールドに記述がない場合は、Newsgroups:フィールドに記述されている Newsgroup に投稿される。

- Followup-to: (NewsGroup 名)

2.1.11 Reference:フィールド

オプションのヘッダ。オプションのヘッダではあるが、投稿する記事が、返信としてのものであるのであれば、この返信元の記事の Message-ID を News リーダは付与する必要がある。

- Reference: Message-ID

2.1.12 Organization:フィールド

オプションのヘッダ。投稿者の所属組織名をユーザの任意に記述する事ができる。

- Organization: (投稿者の所属組織名)

2.1.13 Keywords:フィールド

オプションのヘッダ。記事のキーワードをユーザに任意につける事ができる。他のユーザは自分自身にとって興味深い記事かどうかを決定する基準にする事ができる。

- Keywords: (キーワード)

2.1.14 Summary:フィールド

オプションのヘッダ。記事の要約をユーザが任意につける事ができる。他のユーザが記事を読むかどうかを決定するのに、非常に役に立つ。

- Summary: (要約)

2.1.15 Lines:フィールド

オプションのヘッダ。body 部分の行数を表す。

- Line: (行数)

2.1.16 Xref:フィールド

オプションのヘッダ。複数の Newsgroup に投稿するマルチポストが行われた場合に、News サーバが Newsgroup 名と記事番号をヘッダに追加する。これは、HDD[15] の容量を節約するためである。

- Xref: (News サーバ名) (Newsgroup 名):(記事番号) (Newsgroup 名):(記事番号) .....

下記にサンプル記事を示す。

[15] Hard Disk Drive の略。ハードディスクの事。記憶デバイスの一つ。

```
Xref: news.osaka-sandai.ac.jp sandai.test:5
Path: news.osaka-sandai.ac.jp!not-for-mail
From: Yoichi TAKITA <takita@h-ps011.ise.osaka-sandai.ac.jp>
Newsgroups: sandai.test
Subject: Re: Test
Date: Wed, 12 Sep 2001 09:10:24 +0000 (UTC)
Organization: Osaka-Sangyo Univ.
Lines: 5
Message-ID: <9nn8q0$ftd$1@news.osaka-sandai.ac.jp>
References: <9nn1fp$e57$1@news.osaka-sandai.ac.jp>
NNTP-Posting-Host: h-ps011.ise.osaka-sandai.ac.jp
Mime-Version: 1.0
Content-Type: text/plain; charset=iso-2022-jp
NNTP-Posting-Date: Wed, 12 Sep 2001 09:10:24 +0000 (UTC)
^$
test

Yoichi TAKITA
```

図 2: サンプル記事

3　なりすまし投稿

3.1　なりすましの定義

なりすましとは、組織において正式に発行されたメイルアドレス以外のメイルアドレスを使用して、電子メイルの送信または NetNews への投稿を行うことをここでのなりすましとして定義する。

3.2　なりすます方法

MS-Windows や MacOS などで使用されている一般的な News リーダを使って、NetNews 投稿者が他者になりすますことは容易である。電子メイルアドレスを架空のものや他者のものを記述したのち NetNews 投稿を行う場合、多くの News サーバでは認証機能を使用しておらず、その為なんの問題もなく投稿できる。

以下に、本学の演習室で使用されている News リーダである Wintama[16] を用いて例をあげる。ユーザはユーザが所有していない `foo@osaka-sandai.ac.jp` という電子メイルアドレスで、NetNews 投稿を行う方法である。

1. 図 3に示すように From:行の送信者名と電子メイルアドレスを書き換える。
2. NetNews の記事を新規作成する。
3. 記事を投稿する。

図 3: クライアントソフトの設定例

上記の結果、送信者を foo@osaka-sandai.ac.jp とした記事が投稿される。

[16] MS-Windows95 と MS-WindowsNT4.0/3.51 の環境下で動作を保証している News リーダ。株式会社 Orangesoft が開発を行っている。http://www.orangesoft.co.jp/products.html

3.3 抑制対象としている環境

本研究が NetNews 投稿のなりすましを抑制する対象としているのは、本学の演習室のようなゲイトウェイマシンに NAPT が施されている環境である。

3.3.1 NAPT

NAPT(Network Address Port Translation) は、2 つのネットワークセグメント[17] がゲイトウェイマシン[18] 等を介して接続している環境で、一方のネットワークセグメントに属しているマシンがゲイトウェイの IP アドレスを用いて、もう一方のネットワークセグメントに属するマシンと通信するための機能である。特に NAPT が使用される例としては、プライベート IP アドレスしかもたない複数のクライアントマシンがゲイトウェイマシンのもつ 1 つの IP アドレスを利用してインターネットに接続させる場合が多い。この場合異なるネットワークセグメントに属している News サーバからはクライアントマシンの IP アドレスが特定できない。

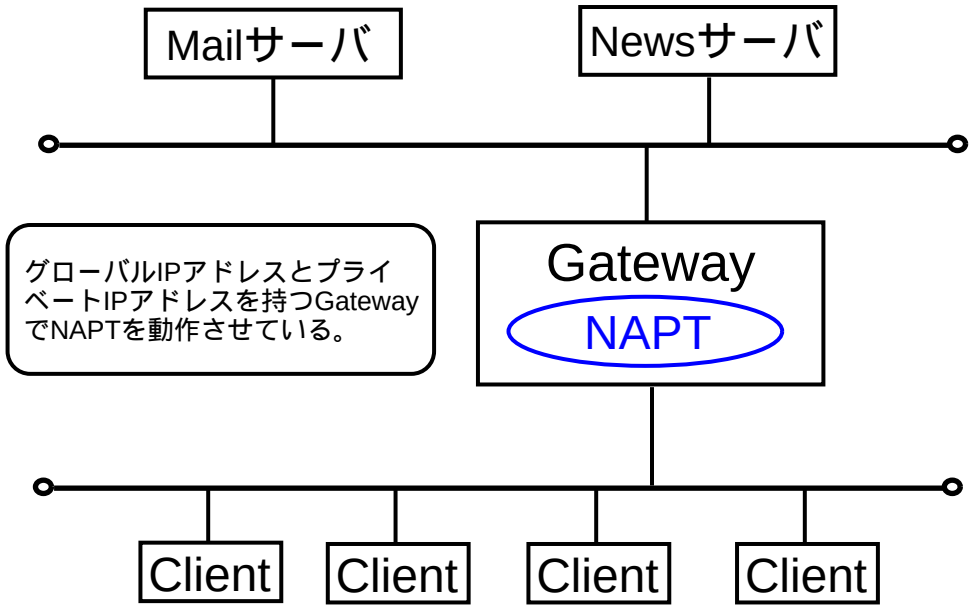

図 4: 認証の切替え

[17]ネットワークにおける論理的な解釈の 1 つ。ブロードキャストパケットが到達可能なノードの集まりを言う。
[18]2 つ以上のネットワークセグメントを介してルーティングなどのサービスを提供する機器。またはサービスの総称。

4　なりすまし投稿の抑制方法

なりすまし抑制は POP サーバ [3] がユーザ認証を受け付けている状態で、tstone を gateway 上で動作させるだけでよい。つまり、News サーバ、POP サーバ、News リーダは実装上または設定上の変更をする必要がない。tstone は News リーダに対して News サーバのように振舞う。また、tstone は POP サーバに対して POP の認証情報を提供しているため、MUA[19] のように振舞う。さらに、tstone は News サーバに対して、News リーダのように振舞う。以下に、その関係を図示する。

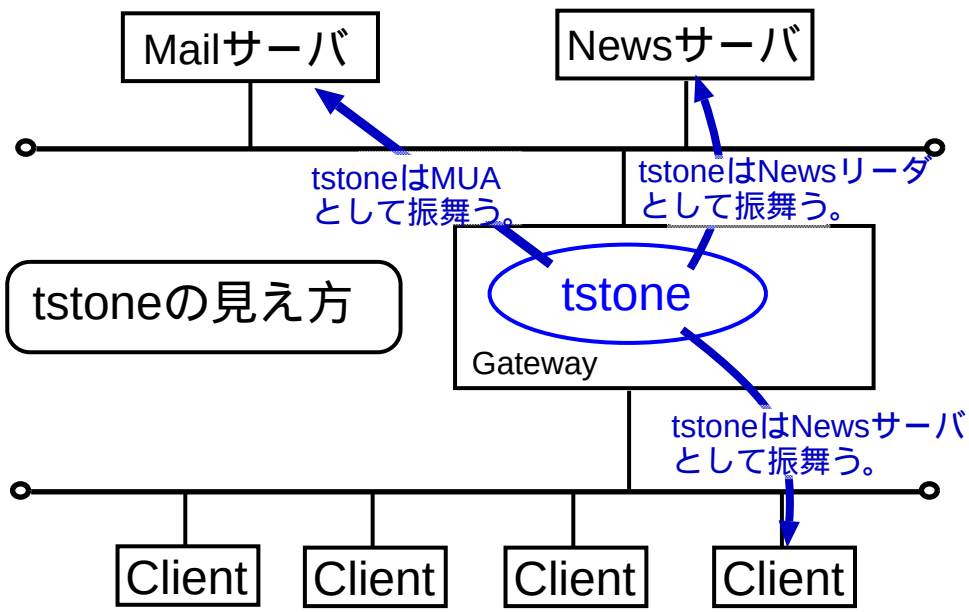

図 5: tstone との関係

またなりすまし投稿の抑制には、次の二つの手法を用いる。

1. ユーザ認証を行う事
   (a) tstone によって、認証を POP [3] サーバに依頼する
   (b) 認証の結果を News リーダへ返す。
   (c) 認証成功後に POP のユーザ名に対応するメイルアドレスを認証ファイルに記録する。
   (d) 認証成功後に tstone は投稿以外の処理を中継する。
2. メイルアドレスのチェックを行う事
   (a) News リーダが投稿を行おうとしたときのメイルアドレスが記録されたものと同じであるかチェックする。
   (b) チェックが成功すると tstone は投稿を中継する。

[19] Mail User Agent の略:電子メイルを送受信するためのクライアントソフト。ユーザーインターフェイスの部分を担当している。メイラーとも呼ばれる。

4.1 ユーザー認証の方法

1. New リーダは News サーバへ接続を行う。しかし実際にはゲイトウェイマシンにインストールされデーモンとして起動している tstone が通信を中継している。最初この tstone は、New リーダに認証情報の提供を要求する。この要求を受け、News リーダは News サーバに対して認証情報を送る。しかし中継を行っている tstone によって、POP のアカウントを用いた形で Mail サーバで認証が行われる。

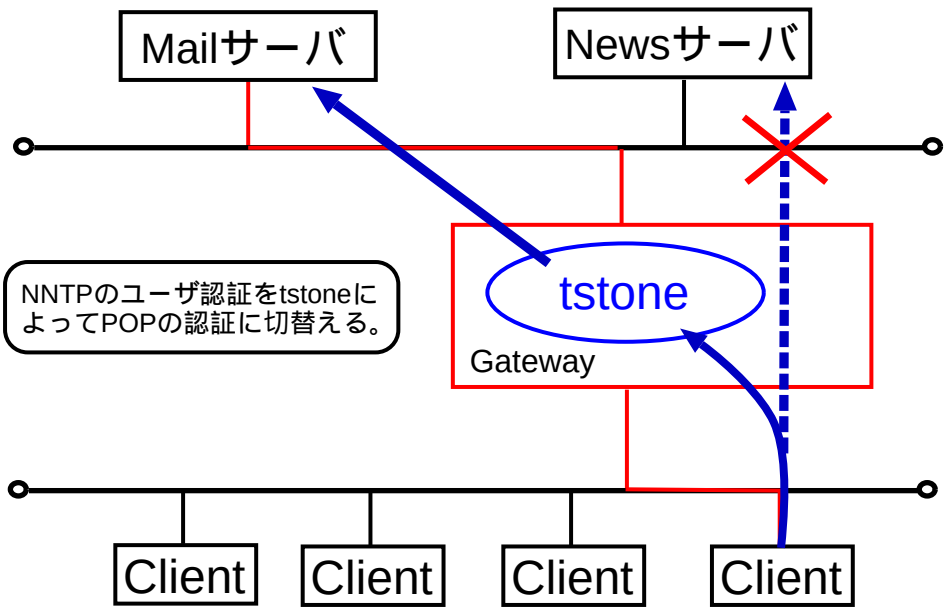

図 6: 認証の切替え

2. 認証の結果が Mail サーバからゲイトウェイマシン上の tstone に返る。また、tstone は認証の結果をクライアントマシンへ返す。さらに、認証に成功した場合は、認証ファイルへクライアントの IP アドレス、認証が成功した時刻、POP のユーザ名に対応するメイルアドレスを記述する。

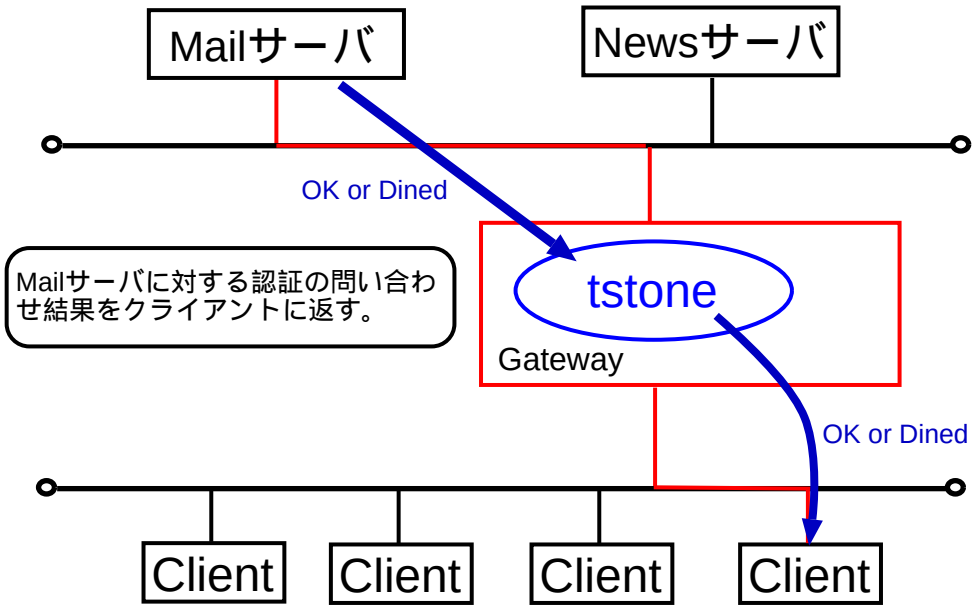

図 7: 認証結果の返答

3. 認証が成功した場合、クライアントは記事の投稿を News サーバに対して行う。この時、tstone は通信を中継しているが、認証が成功しているため投稿をそのまま許可する。

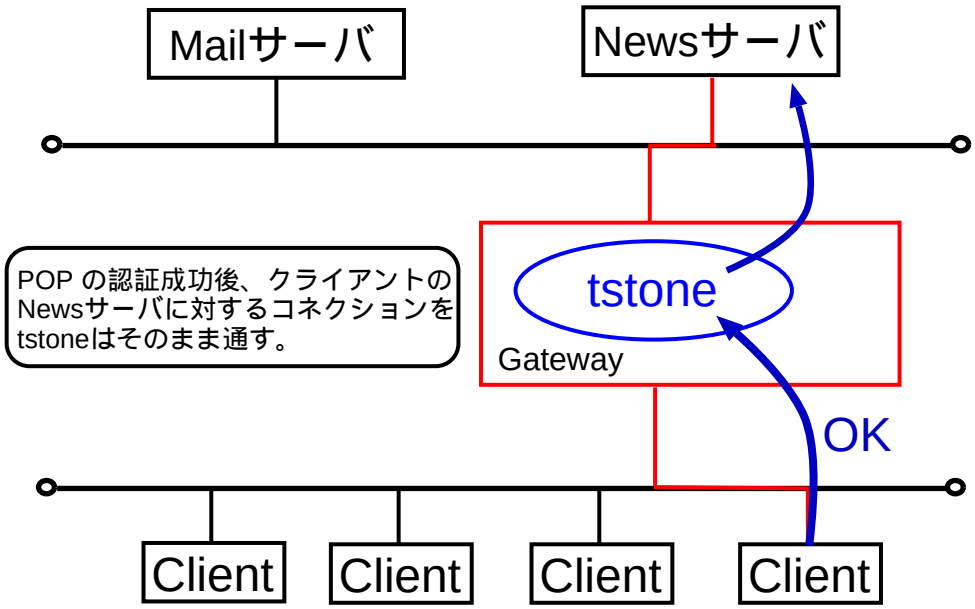

図 8: 認証成功後

4. News リーダが投稿を行おうとしたとき、News リーダが動作しているクライアントマシンの IP アドレスとメイルアドレスが認証ファイルに記載されているものと同じかどうかをチェックする。

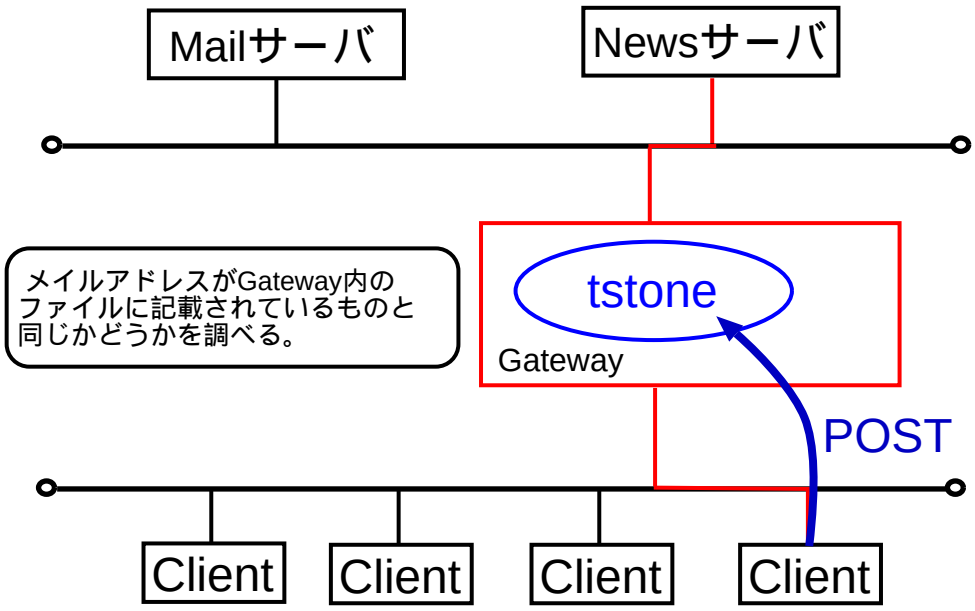

図 9: メイルアドレスのチェック

5. News リーダが投稿の際に提出したメイルアドレスと IP アドレスの組合せが認証ファイルに記述されていない場合、なりすまし投稿を行ったものと判定する。なりすまし投稿が行われた場合、tstone は投稿が終了した時点で News リーダへ-ERR の文字列を返す。News リーダはこれを解釈し、ユーザへエラーメッセージを伝える。

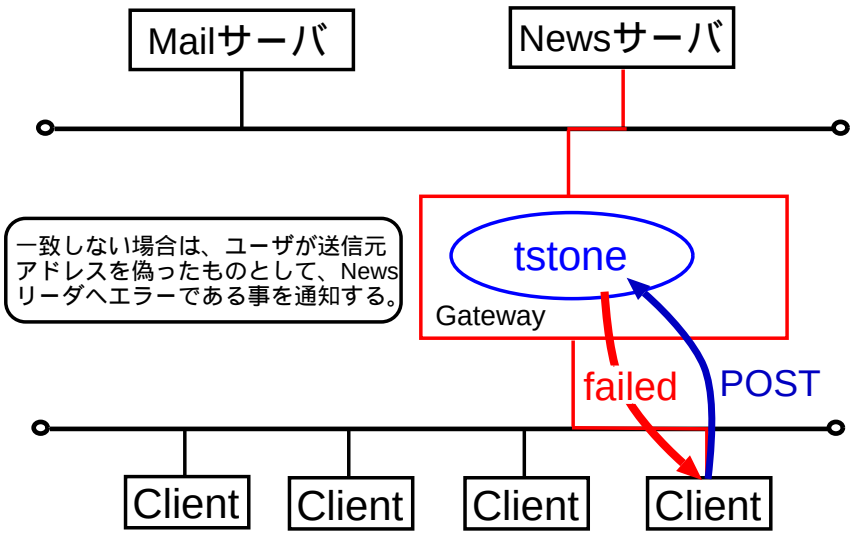

図 10: メイルアドレス不正

6. チェックによって一致と判定された場合は、なりすましを行っていないものとして、tstone は投稿をそのまま中継する。

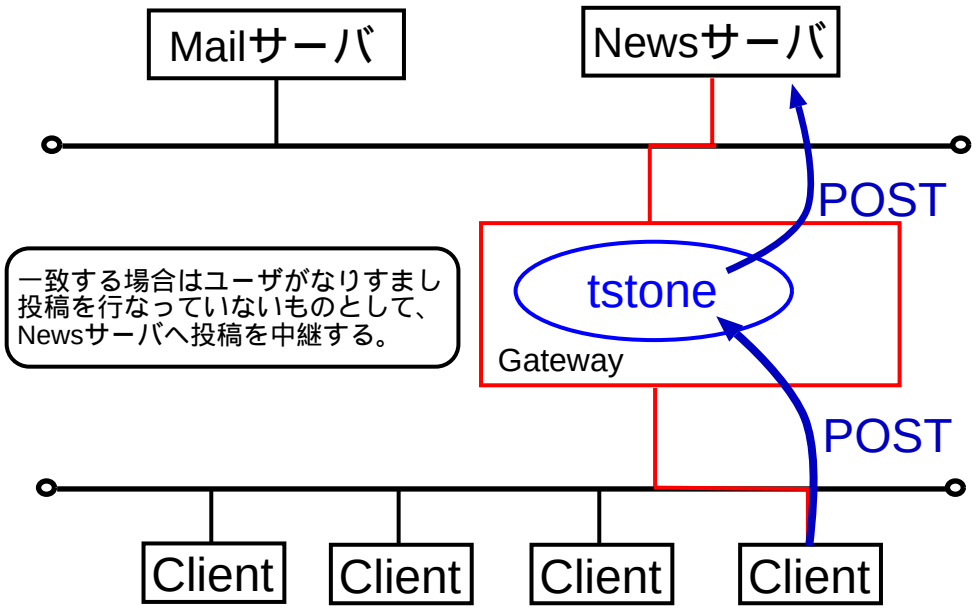

図 11: チェック成功

7. News リーダが News サーバとの接続の中断を要求した時、tstone は、要求を中継する。またこの時、クライアントの IP アドレス、メイルアドレス、認証時刻の組み合わせを認証ファイルから削除する。

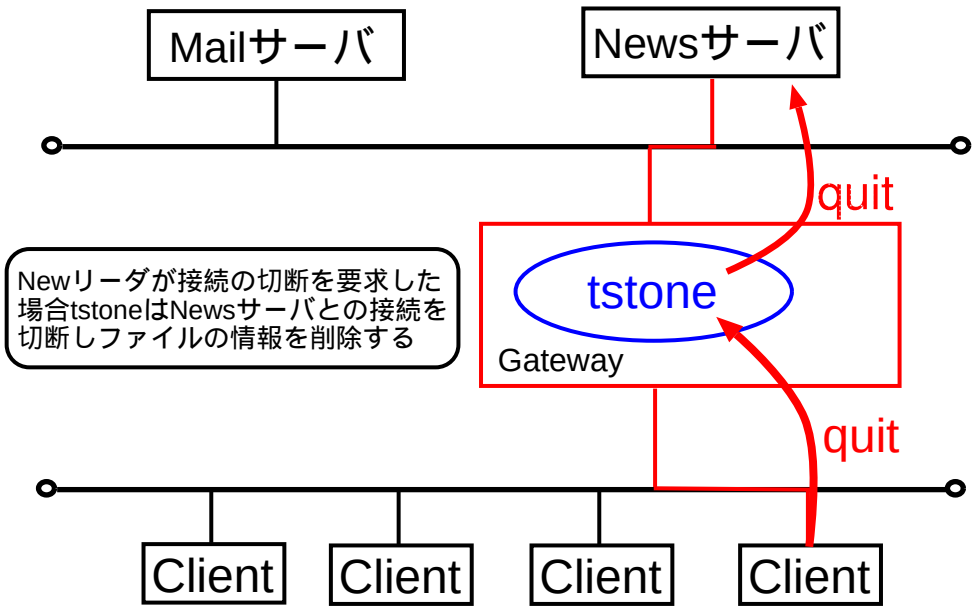

図 12: 接続の切断とクライアント情報の削除

4.2 中継用プログラム

本研究を進める上で、中継プログラムは以下の機能を満たすことが必要である。

1. News サーバとクライアントの間で NNTP を中継する。
2. POP サーバと POP で通信する。
3. POP の認証が成功したクライアントマシンの情報を認証ファイルに記録する
4. POP の認証成功後に News サーバへ投稿以外の通信を中継をする。
5. クライアントマシンの情報を接続の中断と同時に削除する

4.2.1 stone

本研究で使用した中継プログラムは、stone [4] である。stone は、TCP または UDP のパケットを中継する、アプリケーション・レベルのパケット・リピータです。 特定のホストの特定のポートに対する TCP または UDP 接続を、他のホストの特定のポートへ中継できます。

4.2.2 estone

本研究で参考とした中継プログラムは、estone [5] である。estone は、NAPT 環境下でメイルアドレスのなりすまし投稿を抑制したもの。江口裕一[20] によって、提案、作成された。estone は gateway 上にインストールされ、デーモンとして起動される。次に MUA が POP の認証に成功した時に、投稿者の情報を gateway 上にファイルとして記録する。また MUA からの投稿の際は、先のファイルの情報に記録されている IP アドレスと From:が同一であるかをチェックする。一致した場合にのみ、SMTP [6][21] サーバの使用を許可するというもの。本研究では特に From:行のチェックの部分を参考とした。

[20] 大阪産業大学工学部情報システム工学科の卒業生。Estone の作者。
[21] Simple Mail Transfer Protocol の略:電子メイルを送信するためのプロトコル。(付録参照)

5　まとめ

以前江口裕一により、NAPT 下における電子メイル送信者のなりすまし抑制が考案された。これは本学の演習室において、電子メイルの送信元メイルアドレスを偽称する事が可能である事に着目したものである。本研究では、本学の演習室における NAPT を導入した環境で、NetNews においてなりすまし投稿ができることに着目した。なりすましが行えないような抑制手法としては大きく二つの流れがある。

1. ユーザ認証を行う事
2. ユーザ認証に成功したユーザ名に対応するメイルアドレスで投稿しているかどうかのチェックを行う事

まず最初のユーザ認証において、認証情報を保持していな者の News サーバの利用は阻止できる。また、次のメイルアドレスのチェックによって、ユーザ認証は保持しているが From:を偽称する者の「なりすまし投稿」を阻止できる。

本研究で考案された手法を用いることによって、NetNews 投稿のなりすましを抑制する事が可能である。今後は実際にプログラムの実装と安定性の向上、APOP[22] や IMAP[23] への対応、一般ユーザが使用している環境でのテストなどが課題としてあげられる。

[22]POP におけるユーザ認証のパスワードの部分を暗号化してセキュリティを強化したもの。(付録参照)

[23]Internet Message Access Protocol の略:メイルを読み出したり、送信したりするためのプロトコル。RFC1730 ~ RFC1733 で定義されている。(付録参照)

謝辞

本研究を進めていく上で、御協力及び、御指導頂いた大垣 斉講師、藤井 信夫教授、中村 孝講師そして各研究室の方々に深く感謝の意を表します。

参考文献

[1] RFC977,Network News Transfer Protocol

[2] RFC1036,Standard for Interchange of USENET Messages

[3] RFC1939,Post Office Protocol - Version 3

[4] Stone のページ,[http://www.gcd.org/sengoku/stone/]

[5] 江口裕一 Estone のページ, [http://www-fken.ise.osaka-sandai.ac.jp/fken99g/45/H/]

[6] RFC821,Simple Mail Transfer Protocol

付録

- RFC: Request for Comments の略:インターネットに関する技術情報や仕様、運用規則などを定める文章。現在、IETF(Internet Engineering Task Force) が管理する。また、日本では JPNIC が anonimousFTP で公開している。初期のインターネットはあくまで研究プロジェクトであり、研究と運用が同時に行われる環境であった。この段階で、研究者相互での情報交換や新技術などの提案に使われたのが RFC である。直訳すると「コメント求む」という意味になる名称も、この時期の性格を反映したものである。現在では、インターネットは商業利用もされる全世界規模の巨大なインフラである。通信システムである以上、相互通信を可能にするための互換性や相互運用性の確保、信頼性や安全性のためにも、「標準」の存在は、欠かせないものとなっている。そのため、RFC も徐々に公的な性格を強め、現在ではインターネットに関する公的な文書として認められている。反面、提出から承認、公開に至る厳密な手順が定められ、誰もが簡単に公開できるものではなくなってきている。現在では、「コメント求む」どころではなく、公開された段階では既に十分な議論が尽くされ、標準と認められた仕様となっていることが大半と考えるべきであろう。

- ツリー構造: 枝分かれをした階層構造の事。また、複数の分岐情報を持つセルにより、階層的な構造を持たせたデータ構造。あるセルの分岐先には、同様の構造を持ったセルが連結される。セルの連結状態が木の枝 (もしくは根) のような構造を持つ事からこうよばれる。この際、各セルの分岐が 2 つのものを、特に二分木 (バイナリツリー) と呼ぶ。MS-DOS の FAT ファイルシステムなどが構成するディレクトリ構造も一種のツリー構造である。

- プライベート IP アドレス: これらの IP アドレスについては、インターネット側ではルーティングしないことになっているが、組織外へこのアドレスを持つパケットを送出することも禁止されている。しかし、このアドレスについては、組織内であれば、ネットワーク管理者の任意に割り当てて使うことができる。

- SMTP: Simple Mail Transfer Protocol の略。電子メイルを送信するためのプロトコル。TCP/IP の上位プロトコルである。電子メイル送信システム (MTA) で仕様されているプロトコル。プロトコルの仕様は RFC2821 で定義されている。

- APOP: POP におけるユーザ認証のパスワードの部分を暗号化してセキュリティを強化したもの。POP 認証時のパスワードはネットワーク上を平文で流れる。 これはメイルチェックの間隔が 5 分程度であった場合、非常に危険である。APOP はこの問題において、パスワードを暗号化する事で対応したもの。

- IMAP: Internet Message Access Protocol の略。メイルを読み出したり、送信したりするためのプロトコル。RFC1730 ~ RFC1733 で定義されている。一般によく使われている POP または SMTP のプロトコルと違って送信と受信の両方を併せもつ。メイルはホストマシン上で管理される。POP のようにメイル自体をクライアント側へ取り込まないので、複数のクライアント環境からアクセスしても、メイルを同じように読み書きできる。例えば、会社と自宅の両方からアクセスする場合などでも送信済のメイルや未読のメイルが非同期になる事はない。

- 正規表現 (regular expression): 一定の文字列ではなく、文字列の一部を一般化して表現するための手法。もともとはコンピュータ言語理論の分野において、字句 (変数名や予約語、その他の識別子) を一般化して定義するために考案された表現手法。通常のコンピュータ利用では、ドキュメントからの文字列検索時などに、検索したい文字列すべてを指定するのではなく、文字列の任意の一部を置き換え可能な状態で検索する場合などに用いる。