セッション型通信を用いた次世代メッセージングサービス
Next Generation Messaging Services using SIP.

外山 将司†, 高橋 寛幸†, 市川 裕介†, 水野 修†
Masashi TOYAMA, Hiroyuki TAKAHASHI, Yusuke ICHIKAWA, Osamu MIZUNO

概要

個人サーバ間でセッション管理に基づくメッセージ流通を行うことで，従来の電子メールの課題を解決する次世代メッセージングサービスを提案する．提案方式では，SIP のセッション管理の特性を利用し，さらに送信者サーバにメッセージを格納することにより，送信者によるメッセージの管理を実現した．また，プロトタイプの実装とそれを用いた性能評価実験により提案方式の実現可能性を示した．

1 はじめに

インターネットに代表される IP ネットワークの進展に伴い，様々なコミュニケーション手段が発達してきた．その一つに SMTP (Simple Mail Transfer Protocol)[1] を用いた非リアルタイム型メッセージングサービス，すなわち電子メールがある．電子メールでは，受信者状態の如何にかかわらず送信者の都合でメッセージを送付可能という利便性から，ビジネスの上でも社会生活の上でも不可欠なコミュニケーション手段の一つとなっている．

その一方で，電子メールには，例えばウィルスメール，SPAM メールやフィッシング等の数多くの問題が指摘されている． これらは，正常なコミュニケーションを阻害するだけにとどまらず，犯罪や経済的損失を引き起こす等の社会的な問題へと発展している[2]．

これら電子メールの問題に対し，サーバ側，クライアント側それぞれで SPAM 対策が取られるなど，問題毎に様々な対策が考案されており，安全性の向上が図られている．しかしながら，これらの対策はいずれも SMTP の持つ脆弱性を根本的に解消してない．そもそも SMTP はメールを配達するための手順のみを規定したものであり，ユーザによる誤操作や不正への対策が考慮されていないことに要因がある．

一方，IP ネットワークでのコミュニケーション実現手段の一つとして SIP (Session Initiation Protocol) [3] がある．SIP とは，IP ネットワークにおいてエンドーエンドでの通信をセッション管理下で実現するためのプロトコルであり，IP 電話等の音声通話，プレゼンス通知やインスタントメッセージング等が可能となる．

本論文では， SIP のセッション管理能力に着目し，セッション管理下でメッセージを流通することで，SMTP の持つ問題を根本的に解消する次世代メッセージングサービスを提案する．

以下，第 2 章では電子メールの課題を整理し，実現すべきメッセージングサービスの要件を抽出する．第 3 章では，要件に基づいて SIP を用いたメッセージングサービスの構成方法と詳細シーケンスを検討する．第 4 章では，提案方式のプロトタイプを実装し，実験結果に基づいて評価する．

2 背景

2.1 従来技術と課題

本節では，SMTP による電子メールで発生している問題と，それらを解消するための従来技術について述べる．

問題 1:SPAM メール問題

SMTP が送信者の意図で一方的にメールを送信する仕組みであることから，受信者は意図しない相手からの迷惑メールや宣伝メールを防ぐ事ができない．これに対し，送信者（From）アドレスを用いてフィルタリング（ホワイトリスト，ブラックリスト）する等の対策が考案されている．

問題 2:送信者アドレスの詐称問題

SMTP の持つ脆弱性から，送信者アドレスを詐称したメールを送信することが可能であるため，送信者アドレスによるフィルタの回避や，フィッシングサイトへ誘導

† 日本電信電話株式会社
NTT 情報流通プラットフォーム研究所
NTT Information Sharing Platform Laboratories,
NTT Corporation

するメールの送付ができてしまうなどの問題がある. これらに対し DomainKeys[4] の導入などにより送信者アドレスの保証を行う対策が考案されている.

問題 3:到達確認不可問題

電子メールは, 最終的にメッセージが受信者のメールボックスに格納されてしまうため, 送信者はメール送信後に受信者側への到達や既読状況を確認する事ができない, という問題がある. これに対し, Message Disposition Notification[5] 等開封状況の通知するための手順が検討されている.

問題 4:盗聴による情報漏洩問題

SMTP では, 複数のサーバを経由して配送するバケツリレー方式が採用されており, 配送経路上での盗聴の恐れがある. これに対し, S/MIME[6] 等の暗号化技術により問題を防ぐことが検討されている.

問題 5:誤送信による情報漏洩問題

電子メールは, 最終的にメッセージが受信者のメールボックスに格納されてしまうため, 送信先を誤って送信してしまった場合に, 送信後の取消しができない. これに対して, Web メールと HTTP アクセスを利用した消せるメール[7] が提案されている. 同サービスでは, 消せるメールとしてメールが作成された場合に, 受信者に向けて本文を取得するための URI を送付することで, 受信者が URI にアクセスするまでの期間において, 送信済みメールの削除を可能とするものである. しかしながら, 通常のメールと混在していることなどを考慮すると, ユーザ操作による誤送信の可能性が残り, 問題を根本的に解決するものではないと考えられる.

問題 6:容量問題

電子メールが送信者の都合でメールを送る仕組みであることから, 悪意のある送信者が受信者の意図しない大容量のデータを送信し, 受信者サーバ容量をあふれさせてしまうことが可能である. これに対し, 運用対処として受信側のサーバや中継経路で受信サイズを制限する対策が採られている. しかし, この対策には, 受信できるサイズ上限が一定でない, 送信側が受信できるサイズを確認できない, などの問題があるため, 現状の電子メールでは大規模ファイルの送信が難しくなっている.

2.2 問題解決への課題

前述のように, SMTP を用いた電子メールの問題への対策技術が検討されている. しかしながら, これら技術があるにもかかわらず, SPAM, アドレス詐称によるフィッシング, 盗聴や誤送信による情報漏洩等の問題は解消されておらず, 対策が広まっているとはいえない. 本節では, 従来技術の課題を論ずることで, 次世代メッセージングサービスに必要な要件を抽出する.

課題 1:通信相手の対策状況がわからない

従来技術は, 送信者, 受信者双方が対策を施していることを前提としている. 例えば, Message Disposition Notification や DomainKeys は受信者側での実装を前提としている技術だが, 送信者が受信者側の実装を確認する手段が無い為, 送信者は期待する機能が働くかどうかメッセージ送信時に知る事が難しい. さらに, S/MIME では, 受信者側で正しく設定されていない場合にメッセージを確認できなくなるなど, 電子メールサービスそのものが機能しなくなる可能性がある. これらは, SMTP のメッセージを一方的に送りつける特性により, 通信相手の対策状況を把握できないこと起因するものである. そこで, 通信相手の対策状況を確認するための手段が必要である.

課題 2:送信者がメッセージを管理できない

電子メールでは, 送信者は送信済みのメッセージを修正, 削除できず, また受信者がメッセージを閲覧したかを知ることもできない. なぜなら, メッセージが送信者の手元を離れてしまっているため, 送信者による操作や状態把握ができないからである. そこで, メッセージを送信者自身で管理するための方式が必要である.

課題 3:送信者, 受信者間で相互認証する手段がない

フィルタリングによる SPAM メール対策では, 通信相手のアドレス情報が正当であることに基づいている. そのため, 第 2.1 節の問題 2 で述べたように, アドレス情報が詐称された場合には, 全く機能しないという課題がある. そこで, 確実に認証された通信相手との間でのみメッセージが流通されることが必要である.

課題 4:非リアルタイム型のメッセージ交換

第 1 章で述べたとおり, 電子メールは, 受信者のネットワーク接続状態の如何にかかわらず送信者の都合で送付可能である. 次世代メッセージングサービスでも, この特長を保持する必要がある.

2.3 目的

第 2.2 節で示した課題を解決するために, SIP のセッション管理機能に着目し, 送信者, 受信者間での能

力交換に基づくメッセージングを行うことにより，SMTP のもつ脆弱性を解消する．さらに，メッセージの管理を送信者が行い，セッション管理下でのメッセージ流通を行う方式とすることで，電子メールの持つ課題を根本的に解決することを目指す．

3 SIP によるメッセージングサービス方式

3.1 実現方式

(1) 方式の提案

図 1 に，提案するメッセージングサービスの概要を示す．図 1 におけるサブジェクトとコンテンツは，それぞれ電子メールにおける件名(Subject)と本文(Body)相当の情報を示す．また，ここではサブジェクトとコンテンツの双方を含めたものをメッセージとする．

本方式では，送信者によるメッセージの管理を実現するために，メッセージ本体を送信者側に格納する．さらに，サブジェクト，コンテンツを送付する際に，SIP 信号を用いてセッションのための通信方法の合意おこなう．その際に SIP Proxy が送信者，受信者の認証を行うことで，確かなユーザ間での通信を実現する．メッセージの伝達については，サブジェクトのみ通知を既存の電子メールと同等の通知機能を確保し，かつ受信者継起で送信者からコンテンツを取り出す仕組みとすることで，メッセージ状態などを確実に管理できる．

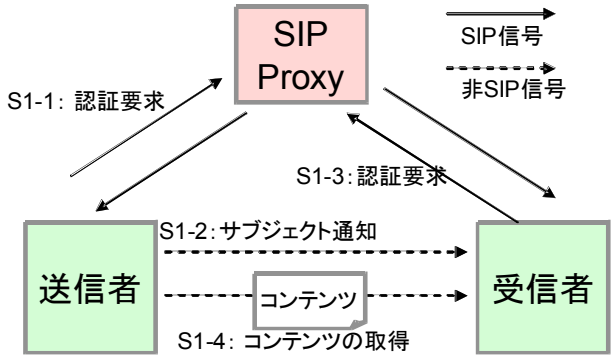

図 1: SIP によるメッセージングサービスの概要

ここで，メッセージの格納方法によって，2 つの実現方式が想定される．以下では，それらの概要について述べ，さらに要件から適切な方式を選択する．

(方式案 A) 端末格納方式

図 2 にメッセージを送信者と受信者のユーザ端末に格納する方式例を示す．これは，送信者端末，受信者端末，及びセッション確立要求を中継する SIP Proxy から構成される．

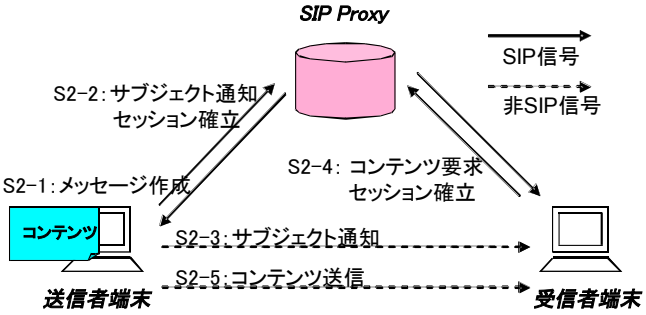

図 2: 端末格納方式の概要

メッセージ流通の手順は次の通りである．まず，送信者は送信者端末にてメッセージを作成し，格納する(S2-1)．メッセージ作成を契機に送信者端末はサブジェクト通知のためのセッションを SIP Proxy を経由して受信者端末と確立し(S2-2)，セッションにてサブジェクトを送信する(S2-3)．受信者は，サブジェクト情報を確認し，送信者端末に向けて(S2-2)と逆の手順でコンテンツ要求のためのセッションを確立し(S2-4)，セッションにて送信者端末からコンテンツを受信することにより(S2-5)，メッセージ流通が完了する．

(方式案 B) サーバ格納方式

図 3 に各端末が自身のもつ個人サーバ(送信者サーバ，受信者サーバ)[8] にメッセージを格納する方式を示す．同方式は，(方式案 A)の構成に加えて，端末ごとにメッセージを格納するためのサーバが存在する点が異なる．ここで，個人サーバはユーザの持つ様々なコンテンツをストックする“箱”という位置づけである．

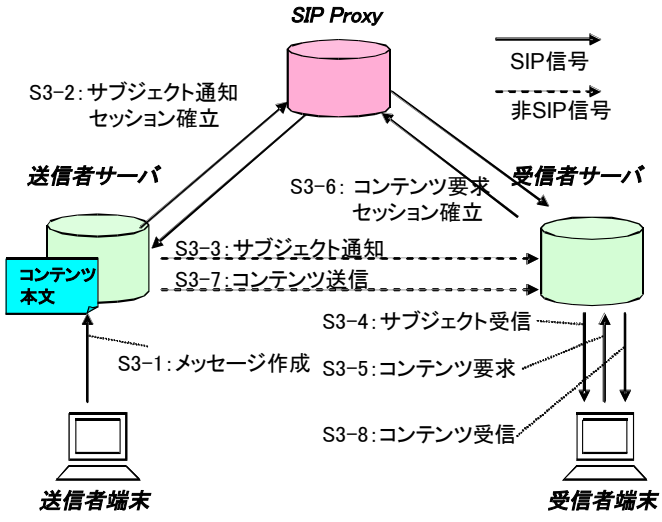

図 3: サーバ格納方式の概要

メッセージ送信の手順は次の通りである，送信者端末は送信者サーバにメッセージを格納する．サーバは（方式案 A）の(S2-2)，(S2-3)と同等の手順で受信者サーバにサブジェクトを通知する(S3-1～S3-3)．続いて，サブジェクトを確認した受信者は，受信者端末，受信者サーバを経由して送信者サーバからコンテンツを取得し(S3-4～S3-7)，コンテンツを閲覧する(S3-8)．

(2) 方式案の比較

表 1 に端末格納型とサーバ格納型の比較を示す．課題 1，課題 3 については，SIP クライアント機能をもつソフトウェアサーバ，クライアントにより実現可能である．また，課題 2 についてもメッセージ送信者側の端末，もしくはサーバでメッセージ状態を管理することで満たすことができる．課題 4 について，非リアルタイムでの通信を行うために常に着信可能な状態であることが必要であるが，端末格納方式では必ずしも要件を満たすことができない．そこで，以降の検討では（方式案 B）サーバ格納方式を前提に議論を進める．

表 1: 方式の比較

	課題1	課題2	課題3	課題4
（方式案A）端末格納方式	○SIPクライアント機能を持つ端末ソフトウェアにより実現	○端末内で管理	○SIP認証により実現	△端末が常に応答可能とは限らない
（方式案B）サーバ格納方式	○SIPクライアント機能をもつサーバソフトウェアにより実現	○サーバで管理	○SIP認証により実現	○サーバが常に応答する

3.2 メッセージ流通方式の詳細

図 4 にサーバ格納型におけるメッセージ流通の詳細シーケンスを記す．

メッセージ送信の手順は次のとおりである．まず，送信者はメッセージを作成し，送信者サーバに登録する(S4-1)．メッセージを受け取った送信者サーバは，受信者サーバとの間でサブジェクト通知のためのセッションを確立し，サブジェクトを通知する(S4-2～S4-6)．この時，SIP Proxy の ID 情報に基づく発信者認証を行うことで(S4-3)，送信者の正当性を保証する．受信者端末の情報要求を受けた受信者サーバは，受信したサブジェクトの一覧を受信者端末に送信する(S4-7～S4-8)．受信者端末からのコンテンツ要求があった場合には，個人サーバでのコンテンツ取得のためのセッションを確立する(S4-9～S4-13)．この時に，(S4-3)と同様の発信者認証を行うことで，受信者の正当性が保証される(S4-11)．その後，受信者サーバは当該セッション情報を利用して送信者サーバからコンテンツを取得し(S4-14)，受信者端末に送信することでコンテンツ閲覧を実現する(S4-15)．このように，受信者のコンテンツ閲覧時のタイミングで送信者サーバからコンテンツを流通させることにより，サブジェクト送信後の修正や削除 (S4-A) 及びメッセージ状態の確認(S4-B)が可能となる．

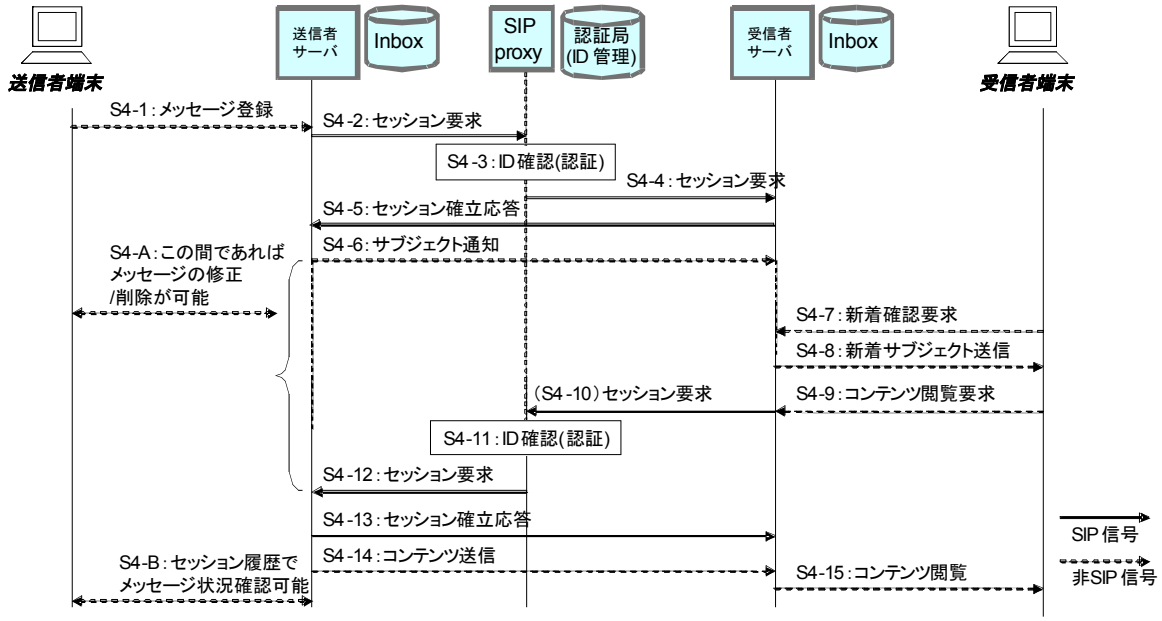

図 4: メッセージ送信の概要シーケンス

4 プロトタイプの実装と評価

4.1 プロトタイプの開発

第 3 章で提案した方式について, プロトタイプを用いたフィージビリティの検証を行った. 本実装では, 送信者端末, 受信者端末において一般的な Web ブラウザで実行させることを想定し, Blog システムをベースとした. 個人サーバ間のサブジェクト通知機能は, Blog の更新 Ping 機能を改造して実現した. また, サーバ間の通信の際には, 接続相手の SIP URI に対して SIP 信号を送信することで, セッション情報及びアプリケーション情報を交換しつつセッションを確立し, 当該セッション管理下にてメッセージの流通を行うよう実装した. また, 受信相手 SIP URI に基づくフィルタリングを行う友達リンク機能を追加し, さらにサブジェクト受信とコンテンツ要求を行うために, 新たに受信箱機能を実装した. また, サーバと端末間でのサブジェクト送信には RSS を利用することにより, 端末に特殊な専用ソフトウェアを不要にした. これら実装のユーザインタフェースを Appendix. A にて示す.

プロトタイプにおいては, SIP と HTTP とを連携させることでセッション管理下でのメッセージの流通を実現した. 図 5 に実装したシーケンスの1つとして, コンテンツ閲覧の例を示す. その手順は次のとおりである. まず, 受信者は受信者端末を経由してからコンテンツ閲覧要求を送信し, 要求を受けた受信者サーバは, コンテンツを保持する送信者サーバとのセッションを要求するための SIP 信号である INVITE を SIP Proxy に送る(S5-01). この時, Proxy は認証により正当な受信者であることを確認し (S5-02～S5-06), 送信者サーバへ INVITE を転送する (S5-07～S5-10). 送信者サーバは, 受信した INVITE(S5-09)から受信者アドレス, 要求アプリケーションを確認した上でセッション要求に対する応答の SIP 信号である 200 OK(S5-11)を返送し, セッションを確立する (S5-11～S5-16). 受信者サーバは, 受信した 200 OK(S5-13)に記載された情報に基づく HTTP 通信を行い, コンテンツを受信し, 受信者に提示する (S5-17～S5-18). さらに, コンテンツ受信後にセッションを終了するための SIP 信号である BYE を送信し(S5-19～S5-24), コンテンツ閲覧を終了する.

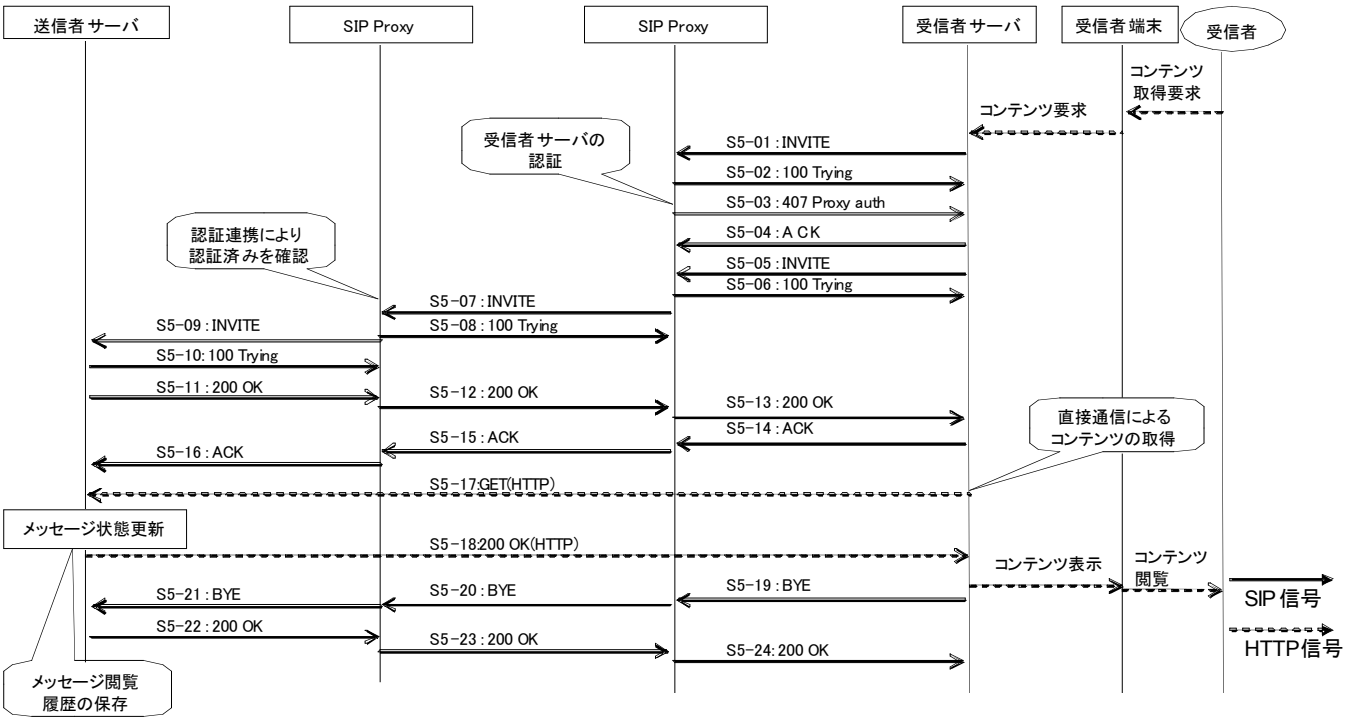

図 5: コンテンツ閲覧時の詳細シーケンス

4.2 評価

4.2.1 動作確認

提案方式のフィージビリティについて，第 2.2 節に示した課題に基づいて論じる．

課題 1 の通信相手の対策状況の確認に関して，図 6 に S5-01: INVITE の SIP 信号詳細の例を示す．本プロトタイプでは，独自拡張した SDP（Session Description Protocol）[9] を，SIP 本文を用いて交換することで通信相手の対策状況の確認する．具体的には，SDP の s 行を用いてアプリケーションの種類や実装している通信機能等の情報（MAKYUU 及び REQUEST_CONTENTS）を交換し，m 行を用いて通信プロトコルのネゴシエーションを行う．SIP メッセージを受信したサーバはこれらパラメータと自サーバの対策状況を確認した上で適切なレスポンスを返す．上記の動作により，双方で対策状況の確認を可能とした．

```
INVITE sip:user50001@example.com SIP/2.0
Via: SIP/2.0/TCP
10.7.70.90:5060;branch=z9hG4bK2139512358004099948
To: sip:user50001@example.com
From: sip:user00001@example.com;tag=1070773879158831855
Max-Forwards: 70
CSeq: 2 INVITE
Call-ID: 52132c4011417092178857PcnsSip0@10.7.70.90
Allow: INVITE,ACK,CANCEL,BYE,OPTIONS
Contact: <sip:user00001@10.7.70.90:5060;transport=    tcp>
Content-Length:141
Content-Type:application/sdp

v=0
o=UserA 2890844526 2890844526 IN IP4 here.com
s=MAKYUU REQUEST_CONTENTS
c=IN IP4 pc33.atlanta.com
t=0 0
m=application 49172 TCP/HTTP 0
```

図 6: INVITE 信号詳細

課題 2 のメッセージを送信者が管理できない問題に関して述べる．まず，送信メッセージの修正，削除については送信者サーバへのコンテンツの格納により可能であることを第 3.2 節にて述べた．一方，メッセージ状態の管理についても，図 5 に示すシーケンスによって確立された SIP セッション管理下での直接通信により解決される．具体的には，送信者サーバは，受信者からの HTTP アクセスから確かに受信者がコンテンツ閲覧要求を出したことを，セッション終了のための SIP 信号の受信から受信者サーバがコンテンツを受信したことを，それぞれ確実に知ることが可能である．これらからメッセージの閲覧状況を管理することが可能となる．

課題 3 の送信者，受信者の認証手段に関しては SIP Proxy が送信者，受信者の代理として認証することにより実現されている．具体的には，SIP Proxy が各サーバを認証し，認証結果に基づいて SIP 信号を転送することで，個人サーバには認証された相手の SIP 信号しか到達しないことが保証される．さらに，個々の通信のセキュリティが守ることによって，送信者，受信者の確実な認証が保証される．個々の通信のセキュリティついては，第 4.2.2 節 にて詳細に考察する．

4.2.2 セキュリティの考察

提案方式は，複数のプレーヤ間で様々なプロトコルを連携させるものである．ここでは，個々のセキュリティについて不正利用防止の観点から次の 4 項目で論じる．

(1) 端末⇔個人サーバ

端末と個人サーバ間では，1 対 1 の直接通信が行えるため，HTTPS などの通信路の暗号及びパスワード等を利用したアクセス認証によりセキュリティ確保を行うことができる．

(2) 個人サーバ⇔個人サーバ

個人サーバ間は SIP セッション管理下での直接通信であり，HTTPS などを用いた暗号化が可能となる．さらに，接続時には，SIP の Call-ID など SIP セッション確立時に用いた情報を個人サーバ間通信時にも確認することで，正しく SIP 通信を行った相手であることが確認可能となる．すなわち，SIP 通信路のセキュリティ確保を前提に接続相手の正当性が保証される．

(3) 個人サーバ⇔SIP Proxy

個人サーバと SIP Proxy 間との盗聴対策として，TLS による暗号化通信を行うことが考えられる．個人サーバから SIP Proxy へのアクセスについては，SIP でも規定されている Digest 認証など発信者認証を SIP Proxy が行うことで，個人サーバの正当性を確保することが可能である[3]．一方で，SIP Proxy から個人サーバへのアクセスについては，着信用アドレスの通知に用いられた REGISTER 認証に基づいて着信を行うことで，正当性を確保することが可能となる．

(4) SIP Proxy⇔SIP Proxy

SIP Proxy 間の通信路は，個人サーバとの間と同様に TLS により暗号化が可能である．さらに SIP Identity[10] ないし SIP-SAML[11][12] など署名技術に基づく ID 連携を用いることで，着信側 Proxy が発信者の正当性を確認することが可能となる．

このように，認証，通信の暗号化，署名等の既存技術を組み合わせることで，アプリケーション全体について通信のセキュリティを確保可能となる．

4.2.3 性能評価

図 5 に示したとおり提案方式ではサブジェクトやコンテンツの送信ごとに SIP のセッションを確立するため，1 セッション確立に複数の SIP 信号の伝達が必要となる．このことから，メッセージ送信時間の増大が容易に想定され，性能低下によるサービス品質の低下が懸念される．そこで，実験により性能への影響を定量的に評価した．

実験環境は及び手順は次の通りである．CPU Pentium® 4 2.4GHz，メモリ 512MByte 搭載の Linux マシンを 4 台用意し，うち 2 台にはメッセージサーバ機能を，残り 2 台には SIP Proxy 機能をインストールした．また，これらを接続する 100Mbps の LAN を構築した．実験では，送信者サーバのセッション確立にかかる時間，すなわち INVITE 信号の送出から ACK のレスポンス受信までの時間を測定した．さらに，メッセージサーバの SIP プロセスの CPU 負荷を測定した．ここで，サブジェクトないしコンテンツの送信時間は直接通信にかかる時間であり，既存の SMTP と提案方式との間で差分がないことが想定されるため，ここでは評価対象外とした．

測定の結果，セッション確立にかかる時間の平均は 870 ミリ秒であった．また，送信者サーバ，受信者サーバそれぞれの SIP プロセスの CPU 負荷は最大で 5%程度であった．これら数字は，実サービスの観点から考えると比較的小さく，問題はないと考えられる．

以上により，SMTP による電子メールの持つ課題を解消した次世代メッセージングサービスが実現可能であることを示した．

5 むすび

セッション型通信を用いた次世代メッセージングサービスを提案した．SIP によるセッションにより通信方法の交換を，SIP 認証により送信者，受信者の正当性確認を実現した．さらに，送信者サーバを介したメッセージ流通により，送信者によるメッセージの管理と非リアルタイムのメッセージングを実現した．また，Blog 等既存のツールを用いたプロトタイプの開発によりフィージビリティの確認を行い，提案方式が SMTP による電子メールの課題を解消していることを示した．

今後は，実サービスへの展開に向けて，ネットワーク負荷や CPU 状態など様々な条件を想定した性能評価を実施する．また，既存の電子メールアプリケーションとの互換性を考慮し，SMTP と連携させる方式を検討する．さらに，本稿では電子メールに代わる次世代メッセージングサービスについて考察したが， SIP セッション管理下での個人サーバの連携という点に着目すると，スケジューラ[13] などメッセージング以外の新サービスが実現可能と考えられる．今後はサービスに共通する要件を抽出することで，個人サーバ間での SIP を利用したアプリケーション基盤の実現を目指す．

参考文献

[1] J. Postel, Simple Mail Transfer Protocol, RFC 2821,2001 年.

[2] 警察庁, 平成 18 年警察白書, p.13, 2006 年.

[3] J. Rosenberg, SIP: Session Initiation Protocol, RFC 3261, 2002 年.

[4] E. Allmanl et al., DomainKeys Identified Mail (DKIM) Signatures , RFC 4871, 2007 年.

[5] T. Hansen et al., Message Disposition Notification, RFC 3798, 2004 年.

[6] B. Ramsdell, Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification, RFC 3851, 2004 年.

[7] ニフティ株式会社, 「@nifty メール」に「消せるメール」機能を追加, http://www.nifty.co.jp/cs/07kami/detail/070719003257/1.htm , 2007 年 7 月 19 日.

[8] O. MIZUNO et al., Personal Information Sharing Service in Next Generation Network

Era, World Telecommunications Congress 2006, 2006 年.
[9] M. Handley et al., SDP: Session Description Protocol, RFC 2327, 1998 年.
[10] J. Peterson et al., Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP), RFC 4474, 2006 年.
[11] H. Tschofenig et al., SIP SAML Profile and Binding, http://www.ietf.org/internet-rafts/draft-ietf-sip-saml-02.txt, 2007 年.
[12] 外山 他, SIP サービスへの SAML の適用に関する一検討, 2007 信学総大, B-7-8, 2007 年 3 月.
[13] 白神 他, ユーザ主導型認証方式とコミュニケータアプリケーションの開発, NTT 技術ジャーナル 2007 vol.19 no.1 p.56-59, 2007 年.

Appendix. A

提案システムの実装結果を以下に示す. 図 A-1 は, SIP-URI を用いたフィルタリングを実現する友達リンク機能の画面である. 第 4.2.2 節に示した通り SIP 認証により SIP-URI が保証されていることから, 確実なフィルタリングが可能となる.

図 A-1: 友達リンク画面

図 A-2 にメッセージ作成画面を示す. 通常の Blog のインタフェースから友達リンクに基づく宛先指定により, SIP-URI を利用した受信者の指定が可能となる.

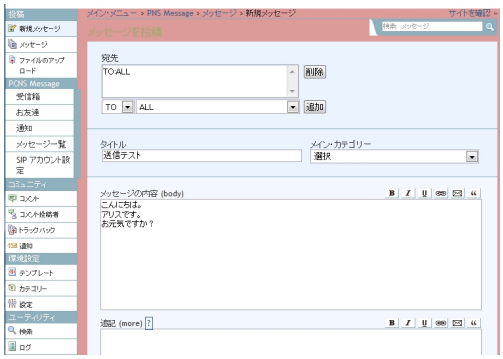

図 A-2: メッセージ作成画面

図 A-3 に送信者サーバのメッセージ状態一覧の画面を示す. 図5のシーケンスに示したように, 送信者サーバからサブジェクトやコンテンツを送信した際に, 送信者サーバ内のメッセージ状態を変更することにより, メッセージの閲覧状況を詳細に管理することが可能となる.

図 A-3: 送信者サーバのメッセージ状態一覧画面

図 A-4 に受信者サーバの受信箱の画面を示す.

図 A-4: 受信者サーバの受信箱画面