社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2008－GN－67 (12)
2008／3／21

ユーザのドメイン移動に対応した SIPにおける発信者特定手法

高原 尚志† 中村 素典‡

†総合研究大学院大学
‡国立情報学研究所

概要 電子メールにおけるSPAMのように，インターネットを利用した電話サービスにおいても迷惑電話は大きな問題である．これを排除するためには，まず発信者の特定を行うことが必要である．電話サービスのセッション開始プロトコルであるSIP (Session Initiation Protocol)には，RFC3261とRFC4474において，それぞれ共通鍵方式と公開鍵方式による発信者の特定手法が規定されている．しかし，携帯端末からの利用を考えた場合，携帯端末を持ったユーザがネットワークの管理単位であるドメインを移動した場合にも対応することが求められるが，SIPの既存の仕様では，ユーザがドメインを移動することは想定していない．そこで本研究では，RFC4474を拡張し，送信者のドメイン移動にも対応した発信者特定手法を新たに提案する．

Sender Authentication Method in SIP for User Migration over Domains

Hisashi TAKAHARA† Motonori NAKAMURA‡

† The Graduate University for Advanced Studies
‡ National Institute of Informatics

Abstract Spam is also a problem in internet phone service as e-mail. To resolve it, we need authentication of senders. SIP (Session Initiation Protocol) is a major protocol used for internet phone services currently. In SIP, methods for sender authentication are defined in RFC3261 and RFC4474. If use of mobile terminals becomes more popular, the internet phone services should support user migration over domains. But current definitions do not assume that users move over domains. In this paper, we propose a sender authentication method adapted to user migration over domains by expanding definition in RFC4474.

1. はじめに

インターネットを利用した電話サービスの普及にともない，メールの場合と同様に，勧誘などのような，受信者が望まない，いわゆる「迷惑電話」が大きな問題となることが予測される．これを排除するために，発信者の特定は欠かすことができない．

インターネット電話におけるセッション開始プロトコルにSIP (Session Initiation Protocol) [1]がある．既存のSIPの仕様では，発信者の特定（認証）を行うために，共通鍵を用いたチャレンジ・レスポンス方式の方法と公開鍵方式の認証サーバを用いた方法が，それぞれRFC3261[1]とRFC4474[2]に規定されており，ユーザとユーザが所属するドメイン（ネットワークの管理単位）におけるプロキシの間の認証を想定している．しかし，携帯端末からの発信などを考えると，発信者が自由にドメインを移動した場合でも同じ発信者アドレスを使用することができるようにすることが，受信者が発信者の識別を行う上での煩雑さを回避するという意味から重要であり，このような状況を仮定した場合でも，発信者の特定を行うことができる手法が必要となる．

そこで，本研究では，[2]の公開鍵方式に基づ

く認証プロトコルを拡張することにより，鍵の管理コストを抑えた送信者のドメイン移動にも対応することができる発信者を特定するための新たな手法を提案する．

以下，2章では，SIPの仕様にある発信者特定手法を中心に共有鍵方式の場合と公開鍵方式の場合について関連研究にも触れながら，本研究の位置付けを明確にする．3章では，本研究で提案する公開鍵方式を利用した発信者特定手法の様々なモデルについて説明する．4章では，3章のモデルの比較を行い，ユーザがドメインを移動する場合に最もよく適応するモデルを示す．5章では，本研究のまとめと今後の課題について言及する．

2. 既存の SIP の仕様における発信者特定手法

携帯端末の普及により，発信者が携帯端末を保持したまま様々な場所に移動しつつ電話サービスを利用する場面は今後増えていくことが予想される．IEEE802.11[abgn]のような公衆無線ネットワークサービスも一般的になり，移動にともなって携帯端末が接続されるネットワークを様々に切り替えながら利用することにも対応するためには，ドメイン移動を考慮した発信者認証手法の実現が重要となる．そこで，本章では，ドメイン移動の観点においてSIPにおけるユーザ認証に関する従来の研究とその問題点について述べる．

なお，本研究では「ドメイン」及び「ドメイン移動」を次のように定義する．

「ドメイン」とは，ある特定のポリシーによって管理されるネットワークのことをいう．

「ドメイン移動」とは，ユーザが現在いるドメインから別のドメインに移動することをいう．

2.1. RFC3216 のユーザ認証(共有鍵方式)

SIPにおいては，[1]の中で，共有鍵を用いたチャレンジ・レスポンス方式のユーザ認証が規定されている．

送信者がドメインを移動する状況において，個々の受信者と送信者の間で認証を行うためには，通話を行う送信者と受信者の組合せの数だけ共有鍵を相互に持たなくてはならないため，ユーザ数が多くなるにつれて鍵の管理コストが増大し，インターネットにおいて，自由に行き来する任意の送信者と受信者との間で通話するような状況に対応することは現実的ではない．

2.2. RFC4474 のユーザ認証(公開鍵方式)

既存のSIPの仕様では，公開鍵方式を用いたユーザ認証手法が[2]の中で規定されている(以下RFC4474方式と称す)．RFC4474方式では，プロキシが送信者に成り代わって通話要求(INVITE)に署名を付与するため，私有鍵と公開鍵はプロキシが管理する形をとなっている．

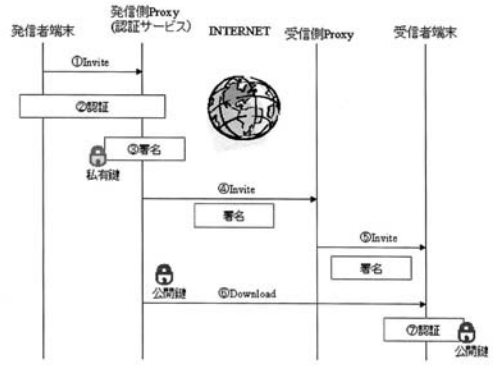

図1　RFC4474に規定されている
公開鍵方式による認証

所属ドメインにおいて送信者が通話要求を行う(INVITEを発する)場合，ユーザの認証(受信者による送信者の認証)は，次の手順で行われる．(図1)

①送信者のSIPプロキシに対するINVITEの発信
②SIPプロキシ(認証サービス)によるユーザの認証(例えば，2.1.の共有鍵を用いたチャレンジ・レスポンス方式など)
③SIPプロキシ(認証サービス)の私有鍵による署名
④SIPプロキシから受信側プロキシへの署名付きINVITEの転送
⑤受信側プロキシから受信者への署名付きINVITEの転送
⑥受信者による送信側プロキシ(認証サービス)からの公開鍵の取得
⑦受信者の取得した公開鍵による署名の認証

但し，RFC4474方式では，ユーザがドメインを移動し，所属するドメインの外からプロキシに対して署名を要求する状況は想定しておらず，通話要求を出す際に移動先プロキシを経由しな

ければならないという制限が加わった場合には対応することができず，新たな手法が必要となる．

2.3. その他の先行研究

SIP において公開鍵方式を用いた RFC4474 方式以外のユーザ認証方式としては次のものが上げられる．

draft-dotson-sip-certificate-auth-sol-00.txt [3] では Registrar とユーザの間における公開鍵方式を用いたユーザ登録のための認証手法が提案されている．しかし，送信者認証については触れてはおらず，本研究とは位置付けが異なる．

また，draft-ietf-sip-certs-05 [4]では，公開鍵方式を用いた正しい受信者への通信を保証する方法として，同一識別子(AOR: Address Of Record)を複数の端末で用いた場合の公開鍵を用いた暗号化手法を提案している．しかしこの提案も，暗号化を用いて正しい受信者へデータを送信する方法について述べたものであり，本研究とは目的が異なる．

3. 公開鍵方式を用いた発信者特定手法モデル

3.1. ドメイン移動に適した鍵の管理手法

端末がドメインを移動した状況において受信者に通信要求を行う場合，移動先のドメイン名を From ヘッダに記述する場合と移動元のドメイン名を記述する場合の 2 つの選択肢がある．

移動先のドメイン名を記述する場合には，すべてのドメインにおいて，それぞれのドメインに属する認証サーバは，移動して来たすべてのユーザに対して公開鍵を配布する必要が生じる．このため，規模が大きなネットワークでは，鍵の管理コストが高くなる．また，すべてのドメインがプロキシを備えているとは限らず，ドメインに接続するユーザの管理を行っているとも限らない点も問題となる．

また，ユーザ側から考えた場合，ドメインを移動するたびに新たに鍵を受け取ることとなり，移動するドメインの数が増えるに従って鍵の管理が煩雑になる．

一方で，From ヘッダに移動元ドメインを記述する場合，公開鍵は移動元ドメインのみが発行することとなり，鍵の増加がない．

そこで本研究では，移動元のドメイン名を From ヘッダに記述して受信者に通信要求を行うモデルが最もユーザのドメイン移動に適応していると考え，これを想定したユーザ認証モデルについて議論する．

3.2. 認証モデル

本研究では，送信者の From ヘッダに移動元のドメイン名を用いる状況で認証を行うことを考える．すでに，RFC4474 では公開鍵を用いたプロキシで署名する認証方式が定義されているので，これを拡張する形で，どのような認証形態をとりうるかについて検討を行うこととする．

まず，拡張の可能性について，発信者特定手法を「署名場所」と「転送形態」の両面から次の観点でもれなく分類する（表 1）．

（ｉ）署名場所･･･端末 or プロキシ

（ii）移動元プロキシを経由させる or させない

（iii）移行先プロキシを経由させる or させない

その結果，次のような 8 種類（2×2×2）の分類モデルが得られる．

表 1　署名場所及び転送形態による分類モデル

署名場所	移動先プロキシ経由	移動元プロキシ経由	備　考
端末	×	×	Model1
端末	×	○	Model2
端末	○	×	Model3
端末	○	○	Model4
プロキシ	×	×	不可能注 1
プロキシ	×	○	Model5
プロキシ	○	×	不可能注 2
プロキシ	○	○	Model6 注 3

注 1 プロキシで署名をするためプロキシを経由する必要がある
注 2 移動先プロキシで署名をすることができない
注 3 署名は移動元プロキシで行う

表 1 に示すように，意味があるのは 6 つである（表 1 の備考の Model1～Model6）．

以下，その 6 つのモデルの署名位置及びプロキシ経由の有無について説明する．

3.2.1. 直接通信／端末署名方式(Model1)

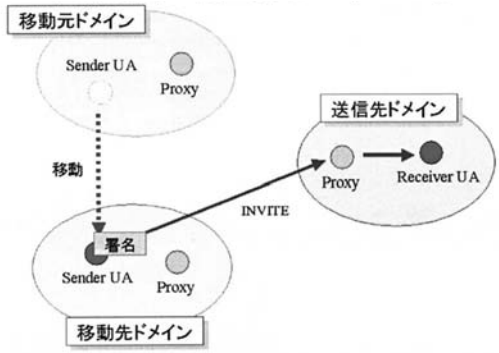

図 2　直接通信／端末署名方式(Model1)

Model1（図 2）は，転送形態としては，送信者が受信者に対して，プロキシを介さずに直接通話要求をするモデルである．

送信者自身が私有鍵を所有し，端末で署名して通話要求を行う．

3.2.2. 移動元 Proxy 経由（直接通信）／端末署名方式(Model2)

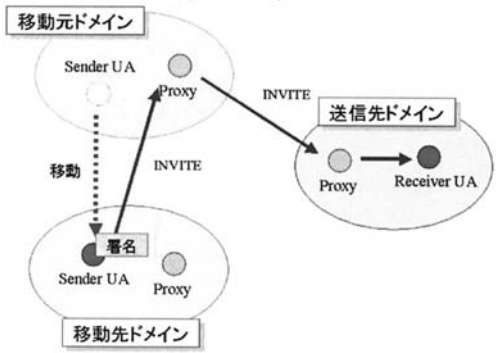

図 3　移動元 Proxy 経由（直接通信）／端末署名方式(Model2)

Model2（図 3）は，移動元プロキシを経由させる方式である．但し，Model4 と異なり，移動先ドメインのプロキシを介さずに，直接移動元プロキシを経由するモデルである．

署名方式としては，送信者自身が署名を行う方式である．従って，端末が私有鍵を保持する必要がある．

3.2.3. 移動先 Proxy 経由／端末署名方式(Model3)

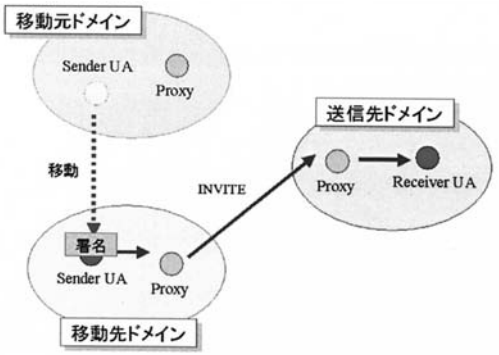

図 4 移動先 Proxy 経由／端末署名方式(Model3)

Model3（図 4）は，転送方式としては，移動先プロキシを経由して受信者に通信を行うモデルである．

Model1 同様，送信者自身が署名を行う方式であるため，端末で私有鍵を保持する必要がある．

3.2.4. 移動元 Proxy 経由（Proxy 経由）／端末署名方式(Model4)

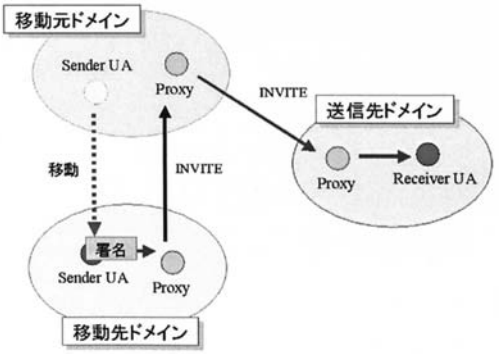

図 5　移動元 Proxy 経由（Proxy 経由）／端末署名方式(Model4)

Model4（図 5）は，転送方式として移動先プロキシを経由した後に，更に，一旦移動元のプロキシを経由させるモデルである．

送信者自身が署名を行うので，端末が私有鍵を保持する必要がある．

3.2.5. 移動元 Proxy 経由（直接通信）／移動元 Proxy 署名方式(Model5)

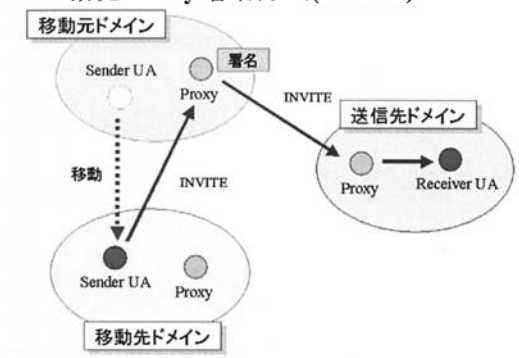

図 6　移動元 Proxy 経由（直接通信）
／移動元 Proxy 署名方式(Model5)

Model5（図 6）は，移動元プロキシが署名を行うモデルである．従って，通信はすべて移動元のドメインを経由させる必要がある．

但し，送信者が直接移動元プロキシに署名及び転送を要求する形態をとる．

移動元プロキシが署名を行うため，プロキシが私有鍵を持ち，送信者は私有鍵を持たない．RFC4474 と同様にしてプロキシと送信者の間で別途共有鍵等を用いた認証を行う．

3.2.6. 移動先 Proxy 経由／移動元 Proxy 署名方式(Model6)

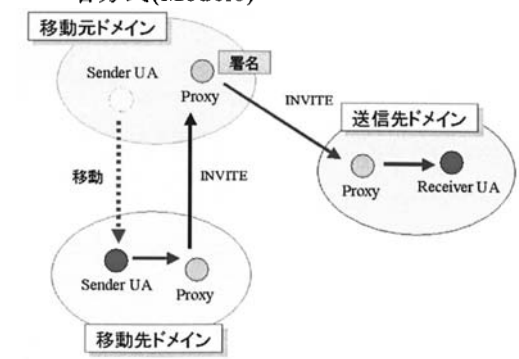

図 7 移動先 Proxy 経由
／移動元 Proxy 署名方式 (Model6)

Model6（図 7）も，Model5 と同様に移動元のプロキシが署名を行うモデルであるが，Model5 と異なり，移動先のプロキシを経由する形で移動元のプロキシと通信する形態をとる．

Model5 と同様，移動元プロキシが署名を行うため，プロキシが私有鍵を持ち送信者は私有鍵を持たない．RFC4474 と同様にしてプロキシと送信者の間で別途共有鍵等を用いた認証を行う．

4. 各認証モデルの比較

ここでは，3 章で示した有効なすべての認証モデルについて考察・比較を行い，端末がドメインを移動する状況における，受信者が送信者を特定する方法として最適なモデルについて議論する．

4.1. 直接通信に対する制約

今後 SIP を利用したインターネット電話において，発信者の詐称は大きな問題となることが予測される．メールにも同様の問題があるが，メールにおける対策としては，OP25B(Outbound Port 25 Blocking)[5]がある．今後 SIP においてもこれと同様の手法（通信においては，発信ドメインのプロキシを経由しなくてはならない）が，導入される可能性が大きいとすると，直接通信を許可しているモデル(Model1，Model5 及び Model2)は成立しなくなる．従って，このような制約があっても実用可能なモデルを採用することが現実的であると考えられる．

4.2. 署名なし通信に対する制約

Model6 においては，署名がない通信をプロキシが転送する．この場合，プロキシがユーザを認証せずに通話要求を転送することとなるため，転送プロキシが，発信者を詐称する通話要求に対する踏み台となってしまうという問題を生じる可能性がある．従って，Model6 は推奨すべきでないモデルと考えるのが妥当である．

4.3. 最適モデル

4.1.と 4.2 の検討の結果，Model3（移動先 Proxy 経由／端末署名方式）及び Model4（移動元 Proxy 経由（Proxy 経由）／端末署名方式）のみが，本研究で仮定しているネットワークに適したモデルということができる．以降，Model3 と Model4 の 2 つのモデルについて比較する．

Model3 は端末にて署名を行い，その署名を移動先プロキシが認証した後，受信側プロキシに転送することができるモデルである．

Model4 においても，Model3 と同様の認証を移動先プロキシで行うことができる．但し，Model4 の場合は，端末からの INVITE（署名付き）を移動先プロキシが移動元プロキシに一旦転送した後，受信側プロキシに転送する．これにより，次のようなメリットとデメリットが考えられる．

［デメリット］

①経由するプロキシの段数（通信コスト）が Model3 の場合よりも大きくなる．

②要求を移動元プロキシ（From ヘッダに記述されたプロキシ）へ転送するための機能を，新たに移動先プロキシに追加しなければならず導入コストが掛かる．

［メリット］

①一旦移動元プロキシ（送信者が登録されているドメインのプロキシ）に転送されるため，From ヘッダに記述されたドメインを経由し，きちんと登録されたユーザか否かを確認することができる．

②移動元プロキシに一旦転送されるため，署名の有効性（端末が所有する私有鍵の期限などの有効性）について，リアルタイムで確認するステップを持つことができる．これにより，鍵の更新時差の問題を解消することができる．

上の比較により，総合的な評価は次のようになる．

Model3 は，Model4 に比べて経由するプロキシの段数（運用コスト）やプロキシの機能追加の面（初期コスト）で，コストを抑えることができる．これに対して，Model4 は，移動元ドメインのプロキシによって，ユーザの登録や署名の有効性をリアルタイムに確認することができるなど Model3 に比べて，より信頼性が高いモデルということができる．

従って，総合的に判断すると，プロキシに新たな機能を追加するという初期コストと，通信コスト（運用コスト）を抑えることができるという点で，通常の運用においては，Model3 が推奨される．但し，より高い信頼性が求められる状況においては Model4 が推奨される．

上述の通り，両モデルともユーザ認証の観点から，詐称などを防ぐことができるモデルであるので，使用する状況によって使い分けることが適当である．

5. まとめと今後の課題

本研究では，インターネットにおける電話システムにおいて，迷惑電話を排除するために必要となる発信者の特定について，ユーザのドメイン移動を考慮した手法の提案を行った．本手法では，公開鍵方式に基づく RFC4474 方式をドメイン移動に対応させるべく拡張し，可能性のある 6 つの運用モデルの中から望ましい 2 つを選定するとともに，それらをコスト面で比較検討した．その結果，状況に応じて使い分けることが望ましいという結論に至った．

今後の課題としては，本研究で示した各モデルに対して，転送モデルや詐称モデルなどを用いて，コストや信頼性などの面から評価実験を行い，より詳細な評価を行う必要がある．

また，本研究では，アプリケーション層に着目したが，今後，Mobile IP など他の層にも着目して，より広い視野から，実装可能性を検討する必要がある．

更に，本研究では，送信者のドメイン移動に着目し，受信者側に立ったユーザ認証手法（送信者認証手法）を提案したが，今後は，受信者がドメインを移動する可能性にも着目し，受信者のドメイン移動にも適応した受信者認証手法についても検討する必要がある．

参 考 文 献

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler: SIP: Session Initiation Protocol, RFC3261 (2002).

[2] J. Peterson, NeuStar, C. Jennings: Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP), RFC4474 (2006).

[3] S. Dotson, SIP Certificate Authentication Solution: SIP Certificate Authentication Solution, draft-dotson-sip-certificate-auth-sol-00.txt (2007).

[4] C. Jennings, J. Peterson, J. Fischl, Ed: Certificate Management Service for The Session Initiation Protocol (SIP), draft-ietf-sip-certs-05 (2008).

[5] JEAG Recommendation ～Outbound Port25 Blocking について～, JEAG (Japan Email Anti-Abuse Group) OP25B サブワーキンググループ(2006). http://jeag.jp/news/pdf/op25b20060223.pdf

[6] E. Allman, M. Delany, M. Libbey, J. Fenton, M. Thomas: DomainKeys Identified Mail (DKIM) Signatures, RFC4871 (2007).