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

2008－IOT－2　(7)
2008／7／25

ドメイン移動に適応した SIP における受信者のなりすまし防止機構

高原 尚志†　　中村 素典†
†総合研究大学院大学

概要　近い将来，インターネットを利用した電話においては，携帯端末を利用した通信が普及すると予測される。この際，ユーザがネットワーク（ドメイン）を移動しても，同じ端末を用いると考えられる．インターネットを利用した電話の代表的なセッション開始プロトコルに SIP(Session Initiation Protocol)がある．SIP においては，受信者の端末が，複数しかも異なるネットワークにある場合の受信端末認証機構は規定されているが，同じ端末がネットワークを移動した場合の認証機構は提案されていない．そのため，受信端末の古い登録情報を用いて「なりすまし」が行われる危険性がある．

そこで本研究では，受信者端末のドメイン移動に適応した受信者認証機構を提案し，「受信者のなりすまし防止」に活用する．

Spoofing Prevention System in SIP for Receiver Migration over Domains

Hisashi TAKAHARA†　　Motonori NAKAMURA†
† The Graduate University for Advanced Studies

Abstract　Spoofing for receiver is a problem in Internet phone service. To guarantee the certain communication, we need a mechanism for authentication of receivers for the first step. SIP (Session Initiation Protocol) is a major protocol used for internet phone services currently. In SIP, methods for receiver authentication are defined in RFC3261. If use of mobile terminals becomes more popular, the internet phone services should support user migration over domains with particular terminal. But current definitions do not assume that users move over domains with particular terminal. In this paper, we propose a receiver authentication method adapted to user migration over domains with particular terminal by expanding definition in RFC3261.

1. はじめに

一般の電話システムにおいては，携帯端末の普及にともない，受信者がある特定の端末を保持したまま，様々な場所に移動して通話要求を受けるという機会が増加した．同様に，インターネットを利用した電話サービスの場合も，受信者がある特定の携帯端末を持ったまま，ネットワークの管理単位であるドメインを移動することが考えられる．

今まで，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」を排除するために，署名を活用することによってユーザのドメイン移動に適応した発信者特定システム[7][8]を提案して来たが，インターネットを利用した電話サービスにおいては，受信者への確実な通信も大変重要な要素である．

インターネットを利用した電話サービスのセッション開始のための代表的なプロトコルとして SIP (Session Initiation Protocol) [1]がある．既存の SIP の仕様では，Registrar、Proxy 及び Location の各サーバが連携をして，複数の受信端末の中で，その時点で受信者が希望する受信端末へ通話要求を確実に転送する機構が規定されている．

しかし，携帯端末の普及を考えると，受信者がある特定の端末を保持したまま頻繁にドメイ

ンを移動するケースが容易に想定される．現在の規定では，複数の固定した端末への転送は考慮されているが，携帯端末など同一端末を受信者がドメインを越えて持ち歩くことは想定していない．このような状況を仮定した場合，受信者の「なりすまし」の危険性が生じるので，それを回避する機構が必要となる．

そこで，本研究では，受信者への通話要求の転送の際にも，[1]の共有鍵方式のチャレンジ・レスポンスを活用して受信者の認証を行い，受信者を確認した後，通話要求を転送することによって受信者への確実な通信を保証する新たな機構を提案する．

以下，2章では，既存のSIPの仕様における受信者への転送機構について言及する．3章では，本研究で扱うシナリオを設定し，そのシナリオにおける既存の規定の問題点を述べることによって，本研究の位置付けを明確にする．4章では，[1]のチャレンジ・レスポンス方式を活用して受信者の認証を行った後に，通話要求を転送する機構モデルを提案し，考察を行う．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

携帯端末の普及により，受信者がある特定の携帯端末を保持したまま様々な場所に移動し，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，携帯端末が接続する際に，様々なネットワークを利用することにも対応した，ドメイン移動に適応した受信者への確実な通信を保証する機構の実現が重要となる．

そこで，本章では，既存の規定における通話要求の受信端末への転送及びそのための端末登録の方法について述べる．これにより，次章（3章）で，本研究のシナリオと既存の規定の問題点を扱う前に現在の状況を明確にする．

■既存の仕様(RFC3261)

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及びLocation, Registrar, Proxyの各サーバが連携した複数の受信端末の登録及び通話要求の転送機構が規定されている．

受信端末は，Registrarに対して端末登録要求(Register)を出し，要求を受けたRegistrarはLocationサーバの端末情報を更新する．この端末情報に従ってプロキシは通話要求を転送する．この流れを図1に示す．

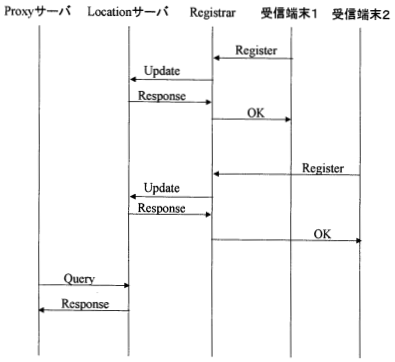

図1 既存の受信端末登録機構

3. シナリオ

ここでは，受信者がある特定の端末を保持しながらドメインを移動するという本研究のシナリオについて述べた後，そのシナリオにおける既存の規定の問題点を，受信者への確実な通信を保証するという観点から明らかにする．これにより，本研究の位置づけを明確にする．

3.1. 定義

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

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

技術的には，ドメインの入り口にファイア・ウオール(F/W)が存在し，内と外との通信において，ある一定の制限が加わることを想定している．

例えば，企業や大学のネットワーク，プロバイダによって提供されるネットワークなどがあげられる．

■ドメイン移動

「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．

上記の定義を図示すると，図2のようになる．

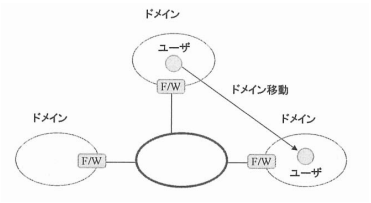

図２　ドメインとドメイン移動

3.2. ドメインの種類

次に，本研究で扱うドメインの種類について述べる．本研究では，図３で示すように，通話要求の経路を考慮して,次の３つのドメイン(①～③）を扱うこととする．

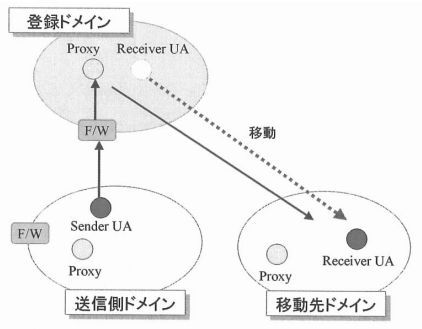

図３　ドメインの種類

①登録ドメイン

SIP の通信で用いるアドレス（以降 SIP アドレスと称す）を付与するドメイン．

登録ドメインの性質上，送信者に対しても受信者に対しても存在するが，本研究では通話要求の到達経路に着目してドメインの種類を分けていることから,『登録ドメイン』といった場合，主に受信者の登録ドメインとする．

従って，送信者の通話要求は，一旦このドメインに送られた後，受信端末に転送される．

②移動先ドメイン

受信者が移動した先のドメイン．

送信者の通話要求は，一旦，登録ドメインに送られた後，上記登録ドメインのプロキシによって，このドメインに転送される．

③送信側ドメイン

呼を発する端末が属するドメイン．

送信者が通話要求を発するドメインである．

3.3. シナリオ

本研究では，次のようなシナリオを想定する．

■前提条件

本研究では，SIP サービスを提供しているすべてのドメインを対象としている．種々多様なドメインにおいて,その入り口に設定された F/W では様々なフィルタリングが予測され，これに適応しなくてはならない．

そこで,「モデルに用いることができるプロトコルは SIP のみとする」という前提条件を設定する．

■シナリオ

本研究では,「受信者は携帯端末など持ち歩きが可能な端末を有しており，その端末を保持したままドメインを移動し，移動した先でも，同じ端末を用いて通話を行う」というシナリオを想定する．

但し，移動の際には，端末を一旦切ってから（ドメインへの登録を一旦解除してから）移動を行い，移動先のドメインにて，再び登録を行うものとする．この流れを図示すると，図４のようになる．

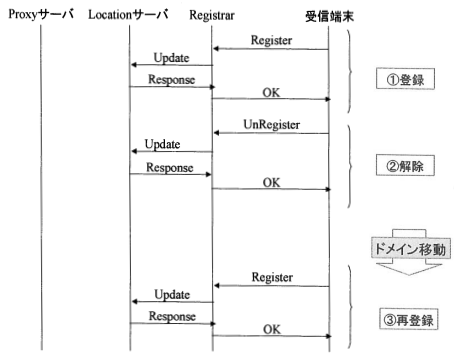

図４　ドメイン移動時における端末登録

3.4. 既存の仕様の問題点

上記のシナリオを考えた場合，既存の仕様では受信者がある特定の携帯端末を保持しながら

ドメインを移動することは想定されておらず，次のような問題を生じる危険性がある．

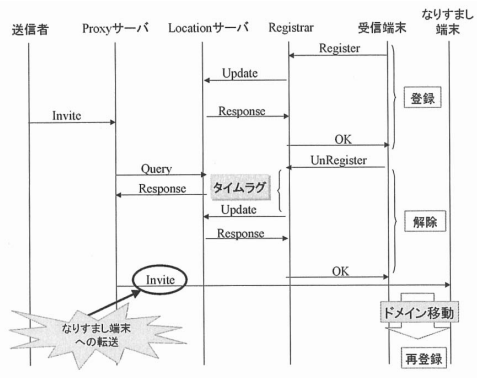

図５　既存の仕様の問題点

受信者が頻繁にドメインを移動する状況においては，受信者が保持している携帯端末のドメインへの登録と離脱が繰り返されることが想定される．携帯端末の登録及び離脱の際には，RegistrarとLocationサーバが情報を交換するため，両者の情報に若干のタイムラグが発生する．

そのタイムラグを用いて，離脱したIPアドレスに，別の端末が滑り込み，「なりすまし」が生じる危険性がある．上記の図５は，その流れを示したものである．

また，受信者がドメインを移動する場合，端末の登録解除を忘れたり，行わなかったりする場合も考えられる．このような場合も，受信端末が離脱しているにも関わらず，Locationサーバの端末情報は更新されないので，上記同様，「なりすまし端末」が生じる危険性がある．

図６でそのイメージを示す．

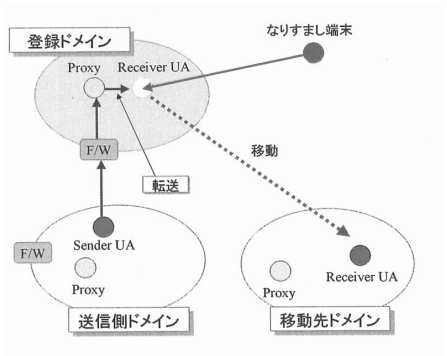

図６　なりすましの危険性

上記の問題を解決するため，受信者への確実な通信を保証するための新たな機構が必要となる．

4.「なりすまし防止機構」の提案

本章では，関連の先行研究に言及しながら，前の章（３章）での問題を解決するための「なりすまし防止機構」を提案する．

4.1. 先行研究及び本研究の位置付け

SIPにおける端末登録及びユーザ認証の先行研究として次のものがある．

draft-dotson-sip-certificate-auth-sol[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．

また，draft-ietf-sip-certs[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，いずれの研究も同じ端末を用いてドメインを移動する際の受信端末への通話要求の転送方法については触れられておらず，本研究とは目的が異なる．

従って，受信端末がドメインを移動した場合にも適応した新たな通話要求転送機構が必要になる．

そこで，本研究では，送信者からの通話要求があった場合，受信者の登録ドメインのプロキシがRFC3261の認証機構を活用して認証を行ない，正しい受信者と確認した後に通話要求を転送するという方法により，受信者への確実な通信を保証するモデルを提案する．

モデルの提案に当って，次項(4.2)の機能の追加を提案する．また，提案する手法を確実なものとするため，端末同士の直接通信は許可されず，必ず受信側登録ドメインのプロキシを経由するものとする．

4.2. 機能追加

ここでは，3.4.の問題点を解決するモデルを提案するに当って必要となる追加機能について述べる．

■受信側プロキシにおける機能追加

プロキシは，受信端末の認証において，RFC3261 のチャレンジ・レスポンス方式の認証機構を活用する．

具体的には，「401 Unauthorized」を対象端末に発する．既存の規定では，Invite に対してのレスポンスとして上記を返すが，ここでは認証として用いるため，Invite がなくても上記を発する機能を追加する．

■受信端末における機能追加

受信端末は，プロキシからの「401 Unauthorized」のチャレンジ値に対して，共有鍵で暗号化されたダイジェスト（レスポンス）を Invite の中に含めて，プロキシに送信する．既存の規定では，自分が発した Invite に対して上記チャレンジが返って来た場合に，上記のレスポンス付き Invite を発するが，ここでは，Invite を発していなくても，「401 Unauthorized」をプロキシの認証要求とし，それに対する応答として上記レスポンスダイジェスト付き Invite をプロキシに返す機能を受信端末に追加する．

4.3. 提案モデル

ここでは，上記の機能追加を踏まえて，受信端末に通話要求を転送する前に，受信者の認証を行うモデルを「なりすまし防止機構」として提案する．送信者からの通話要求の経路に沿って，3.2.であげた「送信側ドメイン」，「登録ドメイン」及び「移動先ドメイン」を想定し，図 7 で示すように受信者の認証を行っている．以下で，この流れを説明する．

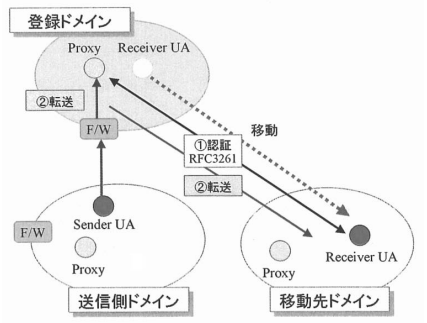

図 7　提案モデル

送信者が受信者の SIP アドレスに対して通話要求を発すると Proxy は Location サーバ及び Registrar と連携しながら，予め受信者によって登録された情報から転送可能な受信端末を把握する．この後、登録されている受信端末が目的の受信者のものかどうかを RFC3261 の共有鍵を用いたチャレンジ・レスポンス方式の認証を行い（図 7 ①），目的の受信者のものであることを確認した後，発信者からの通話要求を転送する（図 7 ②）．

このようにすることによって，受信者への確実な通信を保証し，「なりすまし」を防止する．

4.4. 通話要求の流れ

次に，［①受信者のドメインへの登録］→［②受信端末登録］→［③受信者の認証］→［④通話要求の転送］の流れを述べる．なお，この流れに対する詳細なシーケンスを図 8 に示す．

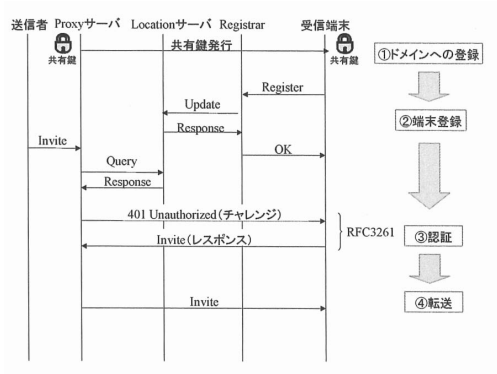

図 8　提案モデルのシーケンス

［通話要求転送までの流れ］

①ドメインへのユーザ（受信者）の登録

ユーザは少なくとも一つ以上のドメインから SIP アドレスの発行を受ける(登録ドメイン)．この際，共有鍵の発行も受ける．

②（受信）端末の登録

受信者は，Registrar を通じて Location サーバに端末を登録する．

③受信者の認証

3.3.の前提条件より，認証に用いることができるプロトコルは SIP のプロトコルのみである．従って，本研究では，下のように，SIP のプロトコルである RFC3261 の認証機構を活用したユーザ認証を用いる．

発信者から登録ユーザ（受信者）に対して通話要求があった場合，登録ドメインのプロキシは，Registrar によって更新された Location サーバの端末登録情報を用いて，目的のユーザの端末（転送先の端末）を見出し，RFC3261 の仕組みを活用したチャレンジ・レスポンス方式のユーザ（受信者）認証を行う．

④通話要求の受信端末への転送

端末が目的の受信者の端末であることを確認した後，その端末に通話要求を転送する．

以上のようにすることによって，携帯端末のように，同じ端末が異なるドメインを渡り歩く場合でも，確実な通信を保証することができる．

4.5. 提案モデルの考察

ここでは，本研究で提案した「なりすまし防止」に関するモデルについて「移行コスト」の面から考察する．

3.4.でも述べた通り，受信者が端末の登録解除を怠ったり，解除が遅延したりすることによって「なりすまし」が生じる危険性がある．この場合，受信端末自体に登録自動解除機能を追加すれば問題は解決するが，端末への機能追加というコストを受信者が負担することとなる．また，技術的にも，「登録解除のタイミング」や「解除トリガーの取得技術」などの開発コストも生じる．

これに対して，提案モデルでは，プロキシと受信者端末の間の認証方法として RFC3261 の認証機能を活用しており，既存のプロトコルを活用した，実装ベースでの機能拡張のみで実現することができる．これにより，プロキシ及び受信者の負担を最小限に抑えることができる．

従って，本研究で提案したモデルを用いれば，移行コストを抑えながら，有効に機能する「なりすまし防止機構」を実現することができる．

5. まとめと今後の課題

インターネットを用いた電話システムにおいて，受信者がある特定の携帯端末を保持したままドメインを頻繁に移動する場合，受信端末のドメインからの離脱情報の更新が遅延したり，行われなかったりする可能性があり，その際に，「なりすまし」が発生する危険性が生じる．既存の規定は，上記の状況を想定しておらず，対応することができない．

そこで本研究では，受信側プロキシと受信端末に RFC3261 を活用した認証機構のための機能を追加することによって，受信者を認証した後，通話要求を転送するという受信者への確実な通信を保証するための「なりすまし防止機構」の提案を行い，「なりすまし防止」について充分な効果があり，また移行によって生じるコストも最小限に抑えることができる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，本研究のモデルを，以前に提案した送信者のドメイン移動に適応した送信者特定手法と組み合わせることによって，送信者及び受信者が，携帯端末を用いてドメインを移動する場合の安全な通信システムを構築する必要がある．

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-06 (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).

[7] 高原尚志，中村素典，“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，”情報処理学会グループウエアとネットワークサービス研究報告(2008-GN-67), Vol.2008, No.31, pp.67-72, March, 2008.

[8] 高原尚志，中村素典，“SIP における既存のシステムからの移行に対応したドメイン移動適応型発信者特定手法，”電子情報通信学会技術研究報告(IN2008-9～25), Vol.108, No.92, pp.61-66, June, 2008.