SIP セキュリティに関する一考察

高原 尚志† 櫻井 幸一‡

†新潟県立大学
950-8680 新潟県新潟市東区海老ヶ瀬 471 番地
tkhara@unii.ac.jp

‡九州大学
819-0395 福岡県福岡市西区元岡 744 番地
sakurai@csce.kyushu-u.ac.jp

あらまし 近年，VoIPを利用したメディア通信が普及している．商用のIP電話では，専用線を用い，中継ゲートウエイも電話会社が管理しているので，電話会社を信頼する限り，途中の第三者及び中継ゲートウエイの介入を意識する必要はない．一方，インターネットのようなオープンなネットワークでは，だれでもが利用することができる公衆回線を用いているため，中継プロキシが必ずしも信用できるとは限らない．中継プロキシは，ネットワーク管理のすべての権限を持っていることが多く，介入が可能である．そこで本稿では，中継プロキシの機能を分析し，権限を分割した場合，どこまでを守ればネットワーク全体のセキュリティを保証することができるかについて検討し，その結果について報告する．

A Note on SIP Security

Hisashi Takahara† Kouichi Sakurai‡

†University of NIIGATA PREFECTURE
471, Ebigase, Higashi-ku, Niigata city, Niigata 950-8680, JAPAN
tkhara@unii.ac.jp
‡Kyushu University
744 Motooka, Nishi-ku, Fukuoka city, Fukuoka 819-0395, JAPAN
sakurai@csce.kyushu-u.ac.jp

Abstract In these days, media communication using VoIP is used at large. In closed networks like IP phone on business, using private line, gateways are managed by telecommunication companies and therefore as long as the company is reliable, man-in-the-middle adversary (MIMA) and geteways cannot make prevention. While, in open networks like Internet, for public line that everyone can use is adopted, all proxies are not reliable. Additionally, proxies usually have all authorities and they can make intervention. In this paper, we analyze functions and if the functions is divided, then we make clear functions needed for security of all over network.

1　はじめに

今日，VoIP を利用したメディア通信が広く普及しているが，IP 電話など電話会社が商用で提供しているサービスにおいては，利用者は，サービス提供者を信頼して，そのサービスを受けており，サービス提供者も信頼性を維持しようという努力をしている．また，上記の場合，サービス提供者が管理する専用回線を使用するクローズドなネットワークであることが多く，途中で第三者が介入する，いわゆる MIMA 攻撃（Man-In-the-middle Adversary 攻撃）の対象にはなりづらい．また，ゲートウエイとなるプロキシも，ユーザからの信頼を得たサービス提供者が管理しているので，そのプロキシが盗聴，改ざん，なりすましの介入を行うということも考えづらい．

一方，近年普及しつつある，インターネットのようなオープンなネットワークでは，誰でもが利用可能な公衆回線を利用するため，MIMA 攻撃は勿論，サービス提供者による介入も考える必要がある．このようなネットワークにおいて，end-to-end の通信を安全に行うため，メディア通信に共有鍵を用いた暗号通信を適用した SRTP[4]が広く知られているが，用いる共有鍵を安全に交換する方法については，規定されていない．そのため，DTLS[3],[6]のハンドシェイクプロトコルを用いて，SRTP で使用する共有鍵を安全に交換する DTLS-SRTP[8]が提案され，標準化されている．DTLS のハンドシェイクプロトコルで共有鍵を安全に交換するためには，事前に双方の端末の公開鍵を安全に交換する必要があるが，これは先立って行われるシグナリング通信（本稿では，シグナリング通信として広く知られたプロトコルである SIP[1],[2]通信を用いる）の保護機構を利用する．この全体像は，DTLS-SRTP-Framework[9]として標準化されている．この際，ゲートウエイとなるプロキシの署名を用いるが，そのため，プロキシの介入を許してしまうという問題が生じる．

そこで本稿では，SIP プロキシに注目し，その機能を分析した上で，どの機能を守れば通信全体を保護することができるかについて考察し，その結果について報告する．

2　本稿で扱う通信

この章では，本稿で扱う通信について，その理由も含めて説明する．

2.1　VoIP 通信

VoIP 通信には，各サービス提供者が提供する独自仕様に基づくものなどさまざまなものがあるが，本稿では，オープン・ネットワークを意識している関係で，仕様が広く公開され，RFC により標準化されている，シグナリング通信により IP アドレスやポート番号などの相手の情報を交換した後，メディア通信を行う方式を対象とする．（図1）

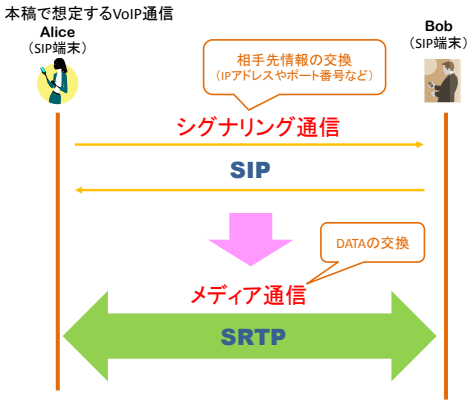

図1　本稿で想定する VoIP 通信

シグナリング通信のプロトコルとしては，SIP を，メディア通信のプロトコルとしては，暗号通信である SRTP を採用する．いずれのプロトコルも広く仕様が公開され，標準化されたものである．

2.2　SIP 通信

SIP 通信には，端末同士でダイレクトに通信を行う方式と，間にプロキシを介して通信を行う方式がある（図2）．

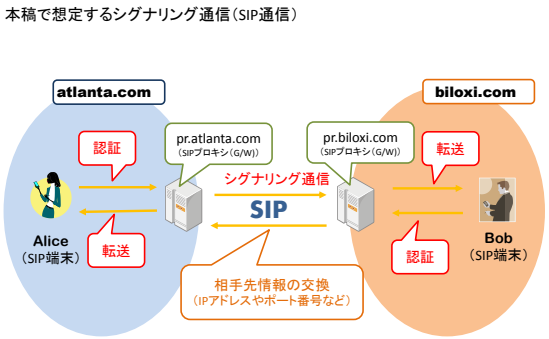

図2　本稿で想定する SIP 通信

前者の方式では，送信端末は，常に相手の IP アドレスを知っている必要があり，受信端末が移動して IP アドレスが変わる度に，その IP アドレスを把握しなければならず実用的ではない．これに対して後者は，受信側プロキシが受信端末への転送を請け負うので，受信端末が移動して IP アドレスが変更された場合には，新たな転送先 IP アドレスを受信側プロキシに登録すれば，送信端末が受信端末の IP アドレスを知らなくても，メッセージを転送して，常に end-to-end の通信を成立させることができる．この場合，送信端末は，受信端末の SIP アドレスさえ知っていればよいこととなり，通信の透過性が保証される．

また，間にプロキシが挟まることにより，送信側プロキシによる送信端末の認証や通信内容の完全性を保証するための署名なども行うことができるので，受信端末は，受け取ったメッセージの真正性及び完全性を保証されることとなる．

通信の透過性や通信の信頼性などの理由から，本稿では，送信側，受信側双方にプロキシを介する通信を扱うものとする．

3　既存の方式

前述の通り，オープン・ネットワークの場合，誰でもが利用することができる公衆回線を利用するため，MIMA による攻撃が想定される．これを防ぐため，メディア通信において共有鍵を用いた暗号通信である SRTP が提案され，広く仕様が公開され，標準化されているが，この暗号通信が安全に行われるためには，用いる共有鍵が安全に交換される必要がある．しかし，SRTP の仕様には，その交換方式が規定されていないため，新たに DTLS-SRTP が提案され，標準化された．本章では，この DTLS-SRTP について説明した後，その問題点について論じる．

3.1　DTLS-SRTP

前述の通り，DTLS-SRTP は，DTLS のハンドシェイクプロトコルを利用して，SRTP で用いる共有鍵を安全に交換する方式である（図3）．

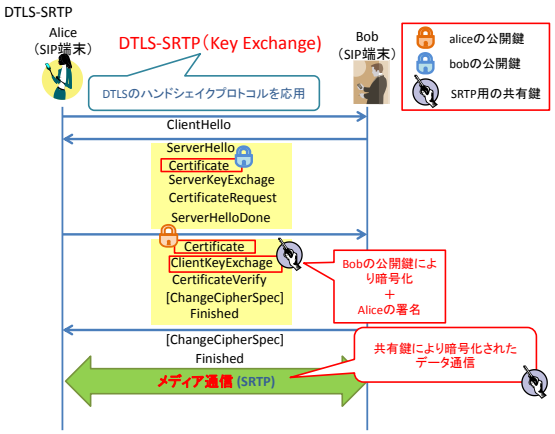

図3　DTLS=SRTP

このためには，互いの端末の公開鍵を，その真正性及び完全性を保証したまま交換する必要があるが，このために，先立って行われる SIP 通信の保護機構（Proxy Authenticate[1] 及び SIP Identity[7]）を用いる．SIP 通信では，ネットワークを流れるトラフィックの関係から，途中のプロキシが SIP のボディ（SDP）の容量を制限していることが多く，公開鍵をそのままボディに含めたのでは，通信が相手端末まで到達できない可能性がある．そこで，SIP 通信の段階では，公開鍵のハッシュである fingerprint を交換し，これを保護機構で保護することにより，公開鍵を保証している（図4）．このようにすれ

ば，容量の問題もクリアすることができる．

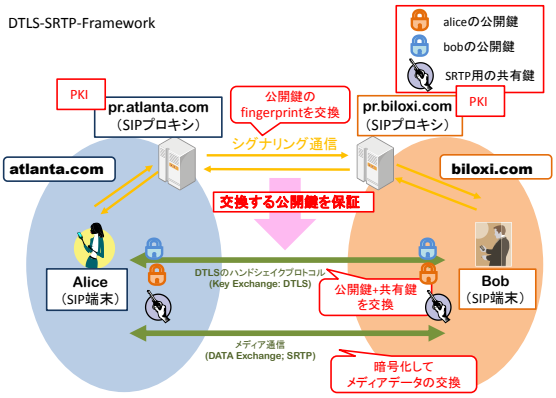

図4　DTLS-SRTP-Framework

ところで，SIP では，リクエストに関しては，保護機構が存在するが，レスポンスに関しては保護機構が存在しない．このため，レスポンス方向の通信は保護されず，受信端末から送信端末にfingerを送信した場合，MIMAによる改ざんが行われる可能性がある．そこで，レスポンス方向にUPDATEリクエストを送信することによって，SIP リクエストの保護機構を適用して，レスポンス方向の通信を保護する方式が提案されている．本稿では，レスポンス方向の通信を保護するため，この方式（仮に UPDATE 方式とする）を採用するものとする．

3.2　DTLS-SRTP の問題点

DTLS-SRTP では，メディア通信を暗号化する（SRTP）ことによって MIMA から通信を保護している．3.1 で述べたように，その際，SIP の保護機構を採用しているが，これはプロキシが署名を行うことによって成り立つ．このため，署名をするプロキシが，介入すれば通信全体の安全性を保証することはできない．[10],[11]本項では，プロキシによる具体的な介入例について述べる．

3.2.1.受信側プロキシが介入

送信端末からのメッセージを，受信側プロキシが受信端末に転送せず，受信端末になりすまして介入する場合，送信端末は，なりすましと気づかずに通信を行うこととなる．この場合，受信端末は通信があったことにも気づかない．（図5）

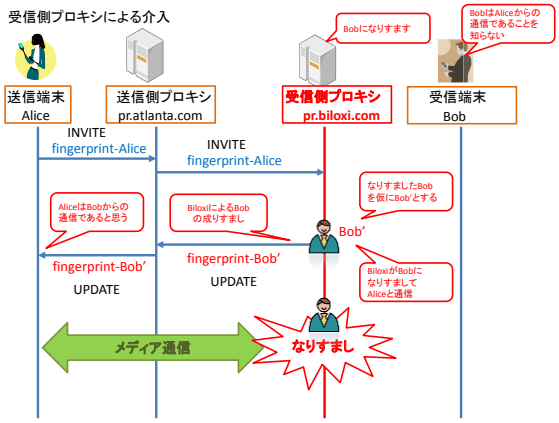

図5　受信側プロキシによる介入

3.2.2. 送／受信側プロキシが結託して介入

送信側プロキシと受信側プロキシが結託して介入しお互いに署名情報を交換した場合，送／受信双方の端末が交換する fingerprint の真正性及び完全性は保証されず，結託したプロキシによるfingerprintの改ざんが可能となる．この場合，以降のメディア通信に対する，結託したプロキシの盗聴，改ざん，なりすましが可能となってしまう．（図6）

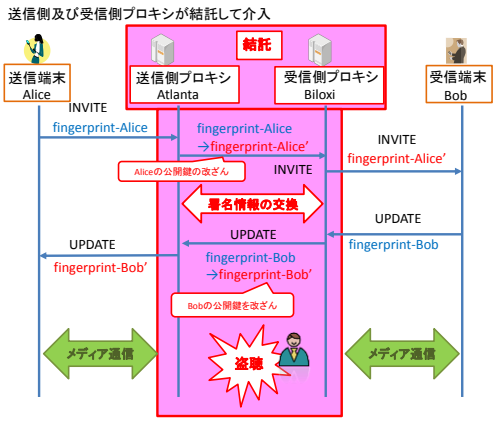

図6　送信／受信プロキシが結託して介入

4　プロキシの機能分析による解決

3 章で指摘したように，DTLS-SRTP においてはプロキシの介入を防ぐことができないという問題がある．本章では，プロキシの機能について分析し，プロキシの機能の内，最低限どの機能を守れば，end-to-end の通信において，プロキシの介入を防ぐことができるのかについて検討する．

4.1　プロキシの機能の分析

SIP プロキシは，大きく送信に携わるプロキシ（本稿ではこれを送信プロキシと呼んでいる）と受信に携わるプロキシ（本稿ではこれを受信プロキシと呼んでいる）に分けることができる．一つのサービス提供領域（本稿ではこれをドメインと呼んでいる）において，送信プロキシと受信プロキシはそれぞれ役割が異なる．そこで本項では，送信プロキシと受信プロキシに分けてそれぞれの役割について分析する．（図7）

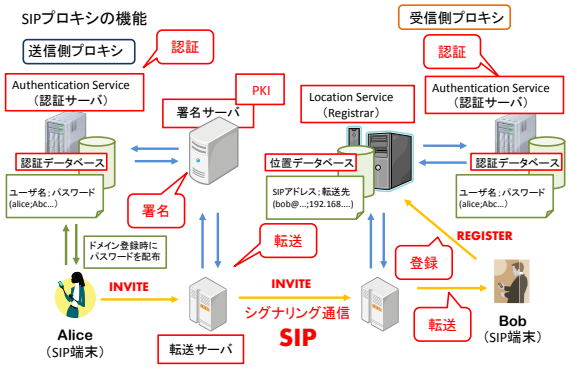

図7　プロキシの機能

4.1.1.送信プロキシ

送信プロキシの役割としては，次のものがあげられる．

(S-1)端末の認証…端末の送信時に，ドメイン登録時などに予め配布した共有鍵（パスワード）で端末の認証を行う機能である．この機能を担うのが Authentication Service[7]で，認証を行うSIPの仕組みがProxy Authenticate[2]である．ユーザ名とパスワードの対応を記したデータベースを元に認証を行う．通信の真正性を保証する．

(S-2)署名…SIP Identity による署名を行い，通信内容の完全性を保証する．①の認証を組み合わせることによって，真正性も保証できる．

(S-3)転送…DNS から，目的のドメインの（受信）プロキシの IP アドレスを検索して，メッセージを転送する

4.1.2.受信プロキシ

(R-1)転送先の登録…Registerリクエストにより，端末のSIPアドレスと転送先のIPアドレスの対応データベースに登録を行う．通常，Registrar[2]，Location Service[2]と呼ばれる．

(R-2)端末の認証…Register リクエストによる転送先の登録(R-1)の際に，予め配布した共有鍵（パスワード）で端末の認証を行う機能である．この機能を担うのが Authentication Service である．(S-1)でも用いるユーザ名とパスワードの対応を記したデータベースを元に認証を行う．

(R-3)メッセージの転送…受信したメッセージを(R-1)で作成したデータベースを元に転送する．

4.2　考察

3.2 で指摘した DTLS-SRTP の問題点を 4.1 で指摘したプロキシの機能の分析を用いて解決する方法を考察する．

まず，3.2.1 で指摘した受信プロキシの介入（なりすまし）の問題について論じる．

DTLS-SRTP では，受信端末は，INVITEリクエスト受信後，UPDATE 方式により，レスポンス方向にもUPDATEリクエストを送信するため，送信プロキシの内，S-1とS-2を守れば，防ぐことができる．たとえ，受信プロキシが受信端末になりすましたとしても，UPDATE リクエストを発信するときに署名を得ることができず，介

入は成功しない．つまり，Authentication Service と署名サーバを守ることにより，受信プロキシのなりすましを防ぐことができる．

次に，3.2.2 で指摘した，送信プロキシと受信プロキシが結託して介入する問題について論じる．

この場合，送信プロキシと受信プロキシが署名情報を交換することによって，fingerprint の改ざんが可能になるので，S-2 の署名機能を保護することにより，介入はできなくなる．この際，署名機能だけで認証機能を保護しないと，誤った認証情報によって，誤った署名がなされ，結果として fingerprint の改ざんが可能になってしまうので，認証機能と署名機能を合わせて保護する必要がある．つまり，Authentication Service と署名機能の両方を保護する必要がある．

結論として，署名機能と認証機能を保護すれば，プロキシの介入を防ぐことが可能となり，結果，通信全体を保護することができる．但し，オープンなネットワークにおいて，すべてのサービス提供者の認証サーバと署名サーバが信頼できるとするのは，すべてのプロキシが信用できるとするのと同様に現実的ではない．そこで一つの提案であるが，認証機能を担っている Authentication Service と SIP Identity の署名サーバは，送信端末と同じドメインに属している必要はないので，これを独立させて，ある特定の信用がおける第三機関が運営するものを用いるようしても，プロキシの介入を防ぐことができる．このようにすれば，すべてのサービス提供者に信頼性のある認証サーバや署名サーバを求める必要がなくなり，ある限られた信用がおけるサービス提供者のみということになり現実的となる．既にクローズド・ネットワークでは，サービスを提供する，ある特定のサービス提供者をユーザが信じることによって，セキュリティが保証されていることを考えれば，オープン・ネットワークにおいても，ある特定のサービス提供者を信用するのは無理がない前提と考えられる．

また，信頼できるサービス提供者が複数存在すれば，ネットワークの規模が大きくなった場合でも，ひとつの Authentication Service と署名サービスを提供するサービス提供者に処理が集中して負荷が大きくなるという問題は生じない．更に，Authentication Service と署名サービスとで，別のサービス提供者のものを使用するということも可能であると考えるが，その仕組みについては更なる検討が必要である．

5 まとめ

本稿では，オープンなネットワークにおける MIMA やプロキシの介入に関する問題をクローズドなネットワークの場合と比較して指摘した．MIMA の介入に関しては，メディア通信を暗号化した SRTP を用いることにより防ぐことができるが，安全に共有鍵を交換するなどこれを実現する既存の方式として DTLS-SRTP を紹介した．一方，プロキシの介入に関しては，オープンなネットワークでは十分可能性があり，DTLS-SRTP では，通信の信頼性を，メディア通信に先立って行われるシグナリング通信（SIP 通信）の保護機構（Proxy Authenticate 及び SIP Identity）に依存しているが，これらの方式では署名や認証などをプロキシが行うため，通信全体の信頼性はプロキシの信頼性に依存する．従って，プロキシの介入を防ぐことはできないという問題を指摘した．

そこで，プロキシの機能を送信プロキシと受信プロキシそれぞれにおいて分析し，どの機能を守れば通信全体の信頼性を保証することができるかについて考察した．その結果，送信プロキシの認証及び署名機能を守れば，通信全体の信頼性を保証できる結果となった．しかし，オープンなネットワークにおいて，すべてのサービス提供者が，認証と署名両方のサービスの信頼性を保証することは，すべてのプロキシの信頼性を保証することと同様に現実的ではない．そこで，ひとつの提案として，認証と署名サービスをドメインから独立させ，信頼できる第三者に委託するという提案をした．このようにすれば，

信頼性が求められるのは，ある特定のサービス提供者のみであるため，現実的であると考える．

今後は，この提案について，更に検討を加え，実験を行い，その有効性を確認する予定である．

謝 辞

本研究は JSPS 科研費 23500096 の助成を受けたものである．

参考文献

[1] R. Pandya, "Emerging mobile and personal communication systems," IEEE Communications Magazine, Vol. 33, pp. 44--52, June 1995.

[2] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler, "SIP: Session Initiation Protocol," RFC3261, IETF, June 2002.

[3] Modadugu, N. and E. Rescorla, "The Design and Implementation of Datagram TLS", Proceedings of ISOC NDSS2004, February 2004.

[4] M. Baugher, D. McGrew, M. Naslund, E. Carrara and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)," RFC3711, IETF, March 2004.

[6] E. Rescorla, N. Modadugu, "Datagram Transport Layer Security," RFC4347, IETF, April 2006.

[7] J. Peterson, NeuStar and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC4474, IETF, August 2006.

[8] D. McGrew and E. Rescorla, "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)," RFC5764 , IETF, May 2010.

[9] J. Fischl, H. Tschofenig and E. Rescorla, "Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)," RFC5763, IETF, May 2010.

[10] 高原尚志，中村素典，"DTLS-SRTP における共有鍵交換の課題,"インターネットコンファレンス 2012，インターネットコンファレンス 2012(IC2012) 論文集，pp.111-112. November, 2012.

[11] 高原尚志，中村素典，"SIP を用いた SRTP の共有鍵交換における課題"，電子情報通信学会技術研究報告，Vol.112，No.352，pp.85-90, December, 2012.