安全な VoIP 通信を行うための一考察
- TWP 方式実現に向けて -

高原尚志[†1]

現在，電話会社が提供する IP 電話など，VoIP を利用したメディア通信が普及しているが，電話会社が管理する専用回線を用いるなどして，途中の第三者の介入を許さないようにしている．この場合のセキュリティは，サービスを提供する電話会社への信用と，専用回線というクローズドなネットワークを用いて途中の第三者の介入を防ぐことによって成り立っている．しかし，今日，VoIP 通信の中には，インターネットのようなオープンなネットワークを利用したものも少なからずあり，オープンなネットワークでは，だれもがサービスを提供できるため，サービス提供者が必ずしも信頼できるとは限らず，もしサービス提供者が盗聴，改ざん，なりすましなどを行った場合，既存の方式では，これを防ぐことはできない．そこで，著者らは，ある特定のサービス提供者を信頼できると仮定し，このサービス提供者が管理する Web プロキシをネットワーク上に設置することによって，通信全体の安全性を保証する TWP 方式を提案して来た．本稿では，TWP 方式について，既存の方式とのより詳細な比較を行い，TWP 方式の有益性を明確にすると同時に，プロトタイプを構築して問題なく動作することを確認したので，その結果について報告する．

A Consideration for Secure VoIP Communication
- Establishment of TWP Method -

Hisashi Takahara[†1]

Recently, VoIP communication like IP phone is used at large. In this case, security is kept by using closed networks like private lines and by reliability of telecommunication companies. However, today, there is VoIP communication in open networks like Internet. In open networks, for anyone can provide services like VoIP in public lines, all of service providers cannot be reliable. When any service providers make attacks, then they cannot be prevented by existing methods. Therefore, TWP method has been proposed. In this method, using a web proxy (TWP=Trusted Web Proxy) managed by a reliable provider, we can prevent attacks by service providers. In this paper, merits of TWP method is made clear, and, with a prototype, it has been proved that TWP method is performed without problems

1. はじめに

近年，インターネットのようなオープンなネットワークを利用した VoIP 通信が普及している. オープンなネットワークでは，だれでもがサービスを提供でき，パブリックな公衆回線を用いるため，だれでもがネットワーク全体の管理の一部を担えるので，商用の IP 電話のように，専用回線を有して，ある特定のユーザのみが独占的にネットワークの管理とサービスの提供を行うクローズドなネットワークを利用する場合と異なり，責任の所在が不明確になる傾向がある．そのため，回線の途中で第三者による盗聴，改ざん，なりすましなどの介入（中間者攻撃）を受ける危険性があるが，現在，これを防ぐ方式は既に標準化されている（DTLS-SRTP8)，DTLS-SRTP-Framework9)）.

更に，オープンなネットワークにおいては，だれでもがサービスを提供できるため，必ずしもサービス提供者が信頼できるとは限らず，サービス提供者自身による介入の可能性もある．これを防ぐ方式としては，8)の鍵交換を行う際に，9)の発展形として，端末で PKI を用いて end-to-end の通信を保証する方式が考えられるが，端末の負担が大きいことが課題となっている．

そこで著者らは，端末の負担を抑えつつ，中間者攻撃やサービス提供者の攻撃を防ぐ方式（TWP 方式 12）,13))）を提案してきた．TWP 方式では，信用できるサービス提供者をひとつ想定し，そのサービス提供者がネットワーク上に Web プロキシを設置し，これを利用することによって，オープンネットなネットワークでも，VoIP 通信全体の安全性を保証する．

TWP 方式では，PKI と異なり，ドメインの登録とは別に CA に改めてユーザ登録する必要がなく，鍵の維持管理についても，ドメイン内の作業で完結するので，端末の負担を抑えることができる．また，Web プロキシが PKI を用いる 9)では端末の負担は抑えられるが，VoIP 通信全体の安全性を保証するために，オープンなネットワーク上のすべてのサービス提供者を信用できる状態にする必要があるため，

†1 (株)新潟県立大学
University of NIIGATA PREFECTURE

実システムでの実現の容易性という観点から課題が残る．これに対して，TWP 方式では，ネットワーク上に信用できるサービス提供者をひとつ設置するだけなので，すべてのプロキシを信用できる状態にするのに対して，実現の容易性という意味で，優れていると考えられる．

本稿では，TWP 方式について，既存の方式と比較して，その有効性を明確にする．更に，この方式が実際に動作することを証明するために，プロトタイプシステムを構築し，動作確認のための実験を行ったので，その結果についても報告する．

2. 既存の方式

2.1 本稿で想定する VoIP 通信

クローズドなネットワークでは，サービス提供者が，VoIP 通信の仕様として，独自プロトコルを採用している場合も少なくないが，本稿では，インターネットのようなオープンなネットワークを想定しているため，RFC により仕様が公開されている，シグナリング通信を行い，その後メディア通信を行うという方式を想定する．（図１）

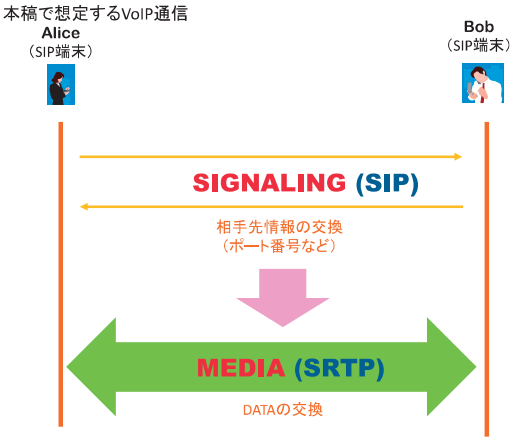

図１　本稿で想定する VoIP 通信
Figure1 VoIP Communication in This Paper

シグナリング通信としては，広く知られ仕様が公開されている SIP を採用する．一方，メディア通信としては，同様に仕様が公開されているプロトコルに RTP があるが，オープンなネットワークでは，経路の途中で第三者による盗聴，改ざん，なりすましの介入を受ける可能性があるため，RTP を共有鍵により暗号化した SRTP5)を採用する．これにより，共有鍵を安全に交換することができれば，途中の第三者の介入を防ぐことができる．なお，SRTP の仕様も公開されている．

2.2 想定するシグナリング通信

本稿で想定するシグナリング通信は，送信端末から受信端末までの間に２つのプロキシを経由する通信を想定する．（図２）

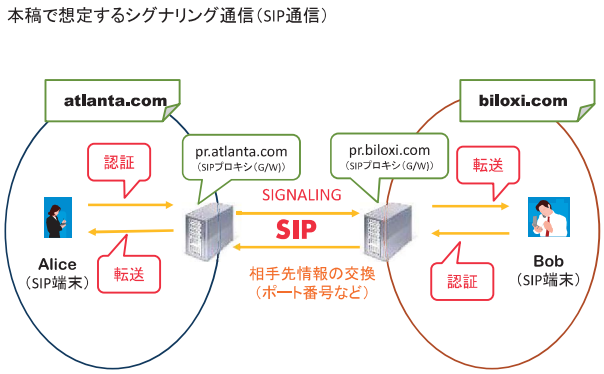

図２　本稿で想定するシグナリング通信
Figure2 Signaling Communication in This Paper

その理由として，ひとつは，異なるサービス提供者が運営するネットワーク（以下本稿では，“ドメイン”という）間での通信で，その際，プロキシがゲートウエイとなっていることを想定するためである．送信端末と受信端末が異なるドメインに属しているというケースは，オープンネットワークでは一般的であると考える．

また，もう一つの理由は，SIP では端末同士かプロキシを介さずに通信を行う方式もあるが，次のような理由から，プロキシを介するのが一般的である．

・プロキシを介することにより，送受信端末ともに認証が可能となり，これにより，プロキシを信頼する限り，端末のなりすましを防ぐことができる．

・受信側でプロキシを介することにより，端末が移動した場合でも，それに応じた転送が可能である．

・受信側でプロキシを介することにより，送信端末は受信端末の SIP アドレスのみを知っていればよく，受信端末が移動しても，プロキシが通信を転送するので，通信の透過性が保証される．

以上のような理由から，本稿では，シグナリング通信として，プロキシを介した通信を想定する．

2.3 既存の方式

2.1 で述べた SRTP では，途中の第三者の介入を防ぐため共有鍵による暗号化メディア通信を行うが，この際用いる共有鍵の交換方式については規定されておらず，既に安全に交換されていることが前提となっている．そこで SRTP

用の共有鍵を交換する様々な方式が提案されているが，本稿では，既存の方式として，仕様が公開され，RFC により標準化されている DTLS-SRTP とそのフレームワークを示した DTLS-SRTP-Framework について述べる．（図３）

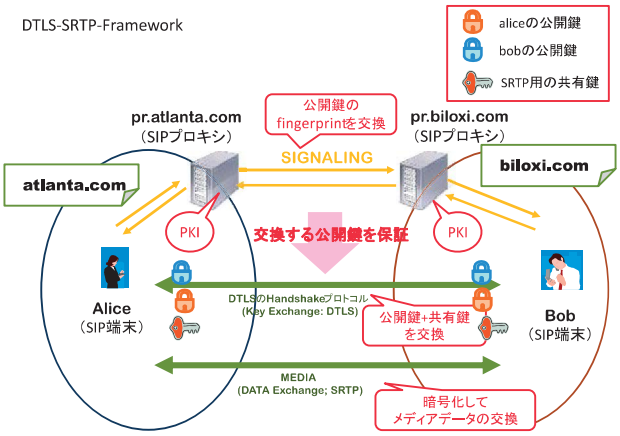

図３　DTLS-SRTP-Framework
Figure3 DTLS-SRTP-Framework

DTLS-SRTP 方式では，SRTP で用いる共有鍵を安全に交換するために，次の３つの STEP を経る．

STEP1　SIP 通信による，端末の公開鍵の fingerprint の交換
端末の公開鍵をメディア通信に先立って行われるシグナリグ通信である SIP 通信にて交換する．この際，SIP の保護機構である Proxy Authenticate や SIP Identity を用いて，fingerprint の完全性及び真正性を保証する．（図４）

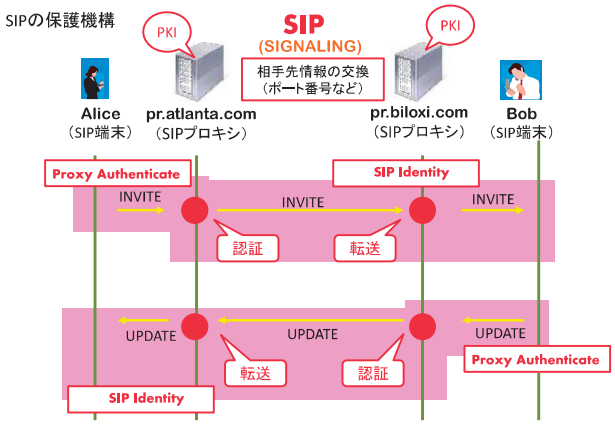

図４　SIP の保護機構による fingerprint の保証
Figure5 Protection by a SIP Mechanism for Assurance

STEP2　DTLS4)のハンドシェイクプロトコルによる公開鍵及びこれを利用した SRTP 用の共有鍵の交換
まず，DTLS のハンドシェイクプロトコルによって，端末の公開鍵を交換する．この際交換される公開鍵は，STEP1 で交換された fingerprint によって保証される．この後，交換された公開鍵を用いて，安全に SRTP 用の共有鍵が交換される．

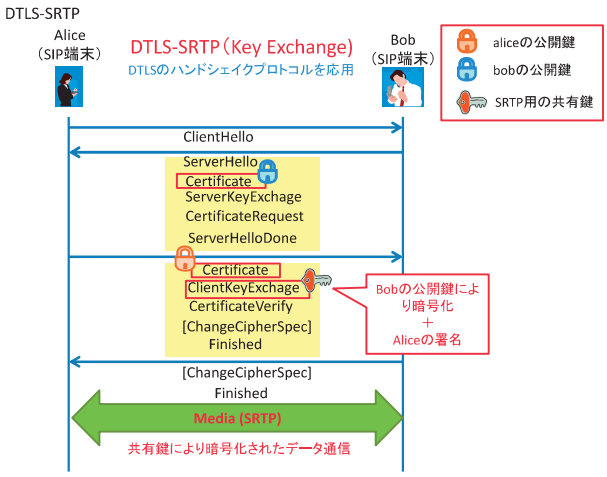

図５　DTLS-SRTP
Figure5 DTLS-SRTP

STEP3　SRTP 共有鍵暗号通信の確立
STEP2 で交換された共有鍵を用いて，共有鍵暗号通信である SRTP が確立される．

STEP1 のシグナリング通信（SIP 通信）で直接公開鍵を交換しないのは，SIP プロキシは，ボディに対する容量制限の設定がなされていることが多く，SIP 通信で公開鍵を交換する場合，容量制限により途中のプロキシで通信が中断してしまう可能性があるためと考えられる．

2.4　既存の方式の問題点

既存の方式（DTLS-SRTP）では，途中の第三者による介入(MIMA 攻撃)は防ぐことができるが，交換する fingerprint の真正性及び完全性を，PKI を採用している送信側，受信側，両プロキシの署名により保証しているので，署名をしているプロキシの介入は防ぐことができない．10),11)
以下では，当該プロキシの介入例を示す．

2.4.1 受信側プロキシが介入する場合

受信側プロキシは，受信端末からの送信メッセージに対して署名を施すことによって，送信メッセージを保証する役割を担っている．そのため，受信端末になりすましてメッセージを作成して，これを受信端末のものとして，署名

をすることが可能となる．従って，受信側プロキシの受信端末へのなりすましが成立する．（図６）

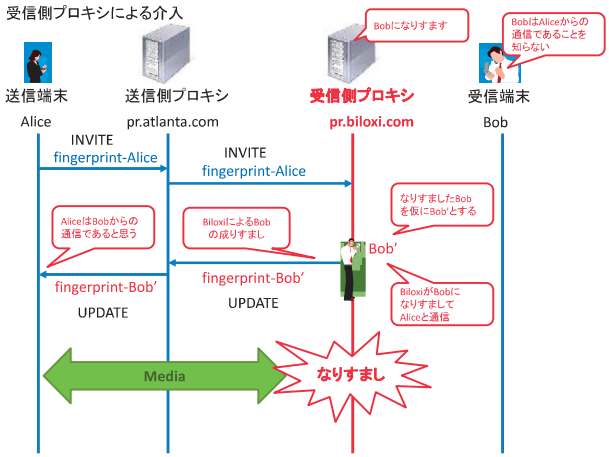

図６　受信側プロキシによるなりすまし攻撃
Figure6 Spoofing Attack by a Proxy of Receiving-side

この場合，受信側プロキシ自身が受信端末になりすまさなくても，なりすまし端末を設定して，その端末への転送を行えば，なりすまし端末によるなりすましも可能となる．

2.4.2 送信側・受信側プロキシが結託して介入する場合

送信側プロキシは，送信端末からメッセージの真正性及び完全性を保証するために署名を施し，一方，受信側プロキシは，受信端末からのメッセージを保証するために署名を施す．このため，両プロキシが結託して，署名情報を交換すれば，送信，受信，両端末からのメッセージを改ざんして，改ざんされたメッセージに署名を施すことが可能となる．その結果，交換される送受信端末の公開鍵を改ざんや SRTP でも用いる共有鍵を改ざんすることが可能となり，続く SRTP によるメディア通信に対して，盗聴，改ざん，なりすましなどの介入を行うことが可能となる．（図７）

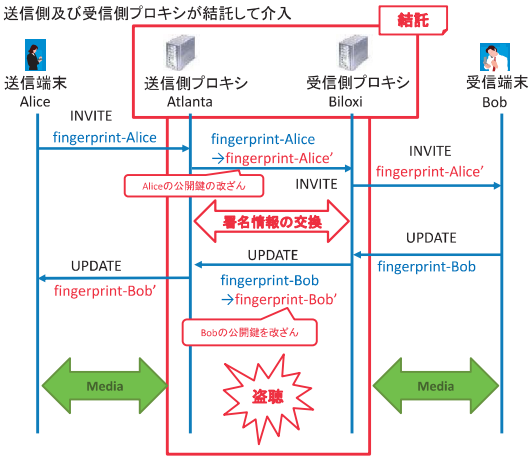

図７　送信側，受信側，両プロキシの結託による介入
Figere7 Attack by Conspiracy with Both Proxies of Sending-side and Receiving-side

2.5 PKI による解決と問題点

2.4 で指摘した既存の DTLS-SRTP の問題を解決する方法として，端末で PKI を採用する方式がある．この方式を用いれば，2.4 で問題となっていた，プロキシの署名によって端末のメッセージを保証する部分を，端末自身が署名を施すようにすることによって解決することができる．

しかし，PKI を採用するためには，CA による認証が必要で，この作業に大きな負担を要する．また，認証後も，公開鍵対に設定された保証期限に対して，鍵の更新，廃棄などについて CA に申請するといった，鍵の維持管理の負担も発生する．

この結果，現在，端末で PKI を採用する方式は普及していない．

3. TWP 方式

著者らは，2.5 で指摘したプロキシの介入という DTLS-SRTP の問題点と端末で PKI を採用する場合の端末の負担の問題を解決する方式として TWP 方式を提案して来た．本論では，TWP 方式について，その実用化に向けた，より詳細な提案を行う．

3.1 概要

TWP 方式では，ネットワーク上に信頼できる Web プロキシ（TWP）をひとつ設置する．オープンネットワークでは，だれでもが参入できるため，すべてのプロキシを信頼することは現実的ではないが，ある特定のサービス提供者を信頼し，このサービス提供者が提供する Web プロキシを信頼することは十分現実にも考えられる．事実，従来の電話システムなどでも，電話サービスを提供するサービス提

供者（電話会社）を信頼することによって，電話サービス全体の信頼性を保証しているという実績がある．

TWP 方式では，各端末の公開鍵を，TWP にある一定期間キャッシュして，適宜，端末自身がその公開鍵の完全性を検証する．そのため，キャッシュされている公開鍵の完全性及び真正性が，端末自身によって保証される．これを用いて，安全に共有鍵を交換し，この共有鍵を用いて，SRTP 共有鍵暗号メディア通信を行う．（図８）

また，TWP は Web プロキシのため，認証などは行わないため，PKI のように認証による端末の負担も発生しない．

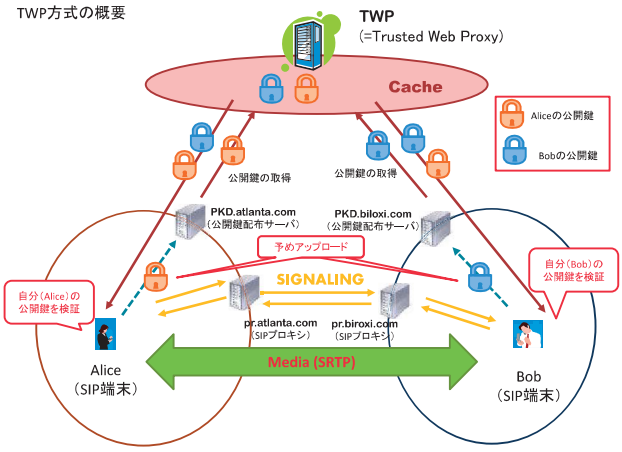

図８　TWP 方式の概要

Figure8 Overview of TWP Method

3.2　エンティティ

TWP 方式では，以下のエンティティを扱う．

・送／受信端末…端末は，SIP によるシグナリングの通信機能と SRTP による暗号メディア通信機能を有する．また，公開鍵対及び共有鍵を独自に作成する機能を有する．また，予め，ドメイン登録時に，サービス提供者から，認証用の共有鍵（パスワードなど）を得ているものとする．

・送／受信側プロキシ…ここで言うプロキシとは，シグナリングの中継をする SIP プロキシのこと，一般に用いられている SIP サーバである．各ドメインのゲートウエイの役割もあり，メディア通信についてもこのプロキシを経由するものとする．このプロキシは PKI を採用し，端末からの SIP リクエストに対して SIP Identity の署名を施したり，ドメイン登録時に各端末に配布された共有鍵を用いて Proxy Authenticate による認証を行ったりするものとする．

・送／受信側公開鍵配布サーバ（PKD）…このサーバ（Public Key Distributor）は，TWP 方式で新たに設置するサーバで，所属ドメインの各端末の公開鍵の各端末からのアップロードを認証の後受け付け，TWP の要求に応じて，公開鍵を TWP に提供する．PKI を採用しており，TWP への鍵の提供にあたっては，HTTPS 通信を用いて，安全に鍵を提供するものとする．

・TWP…Trusted Web Proxy の略で，信頼できるサービス提供者が，ネットワーク上に新たに設置する，Web プロキシである．端末からの要求に基づき，各ドメインの PKD から端末の公開鍵を取得した後，ある一定期間キャッシュする．PKI を採用し，これにより，端末との通信を HTTPS 通信により保証することができる．端末の認証などは行わず，すべての端末からの公開鍵取得要求に応じる．

なお，上記のエンティティの内，メディア通信開始要求が行われた場合，送／受信端末及び TWP は信頼でき，PKD 及びプロキシは必ずしも信頼できるとは限らないものとする．

3.3　手順

まず各端末は，通信を始める前に予め次の準備を行っているものとする．

（準備１）各端末の公開鍵を所属ドメインの PKD にアップロードする

この上で，TWP 方式の手順は，以下の通りである．（図９）

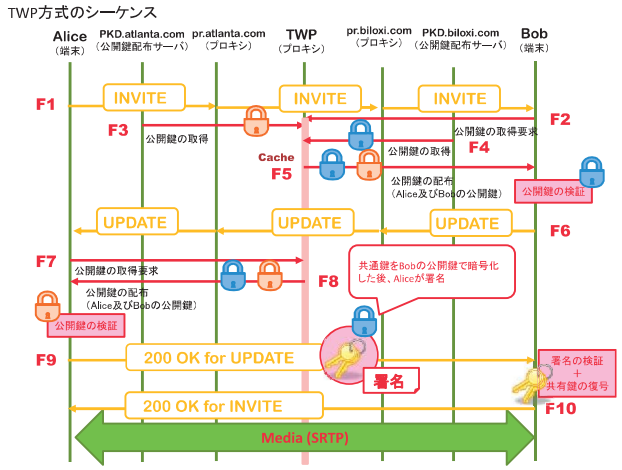

図９　TWP 方式の通信手順

Figure9 Sequence of TWP Method

（手順１）送信端末は，接続要求である INVITE リクエストを受信端末に向けて送信する．（F1）

（手順２）受信端末は，（手順１）の INVITE リクエストを受け取ると，TWP に対して，自らと相手の公開鍵を取得するための要求を発する．（F2）

（手順３）TWP は，（手順２）の公開鍵取得要求を受け取ると，自らのキャッシュに当該公開鍵がないことを確認し，

当該ドメインの PKD に対して，公開鍵取得要求を発する．キャッシュに公開鍵があった場合には，即座に端末に対して公開鍵を配布する．

（手順４）PKD は，（手順３）の要求を受け取ると，TWP に対して，当該の公開鍵を配布する．（F3，F4）

（手順５）TWP は，（手順４）により公開鍵を受け取ると，（手順２）で公開鍵取得要求を発した受信端末に対して，公開鍵を配布する．（F5）

（手順６）受信端末は，（手順５）で受け取った公開鍵の内，自らの公開鍵の完全性を検証する．

（手順７）受信端末は，（手順６）の検証に成功すると，UPDATE リクエストを送信端末に対して送信する．（F6）

検証が失敗した場合には，（手順２）で受け取った INVTEITE に対して，エラーレスポンスを送信端末に返し，通信は中断される．

（手順８）送信端末は，（手順７）の UPDATE を受け取ると，TWP に対して，自らと相手の公開鍵の取得要求を発する．（F7）

※受信端末からの UPDATE リクエストを受け取った時点で，TWP にキャッシュされている受信端末の公開鍵の真正性及び完全性は，受信端末によって保証されている．

（手順９）TWP は，（手順８）の要求に応じて，自らのキャッシュから，当該公開鍵を，送信端末に配布する．（F8）

（手順１０）送信端末は，（手順８）で取得した公開鍵の内，自らの公開鍵の完全性を検証する．

（手順１１）送信端末は，検証に成功すれば，自らが作成した SRTP で用いる共有鍵を（手順９）で取得した公開鍵で暗号化した後，署名を施したものを（手順８）で受け取った UPDATE のレスポンス（200 OK）に含めて，受信端末に返す．（F9）

検証に失敗した場合は，UPDATE のレスポンスとして，エラーレスポンスを返し，通信が中断される．

（手順１２）受信端末は，（手順１１）からの 200 OK レスポンスに含まれた，送信端末からの署名を検証した後，受信端末自身の公開鍵で暗号化された SRTP 用の共有鍵を，対をなす私有鍵で復号する．

（手順１３）受信端末は，（手順１２）の検証及び復号に成功すると，（手順２）で受け取った INVTE に対する 200 OK レスポンスを送信端末に返す．（F10）

この後，交換した共有鍵を用いた SRTP 暗号メディア通信を開始する．

なお，各端末は，定期的に TWP から自らの公開鍵をダウンロードして TWP にキャッシュされている公開鍵の完全性を検証する．これにより，なりすまし端末が異なる公開鍵をキャッシュしている場合，これを発見することができる．

3.4 現在運用されている SIP システムとの親和性

TWP 方式では，現在運用されているシステムからの移行の容易性を考慮し，従来の SIP 通信との親和性を持たせるため，次の点に配慮している．

①TWP 方式未対応の端末との親和性

送信端末が受信端末に INVTE リクエストを送信する際に，当該通信が TWP 方式の通信であることを示すヘッダを用意する．これにより，受信端末が TWP 方式に未対応である，または TWP 方式を望まない場合，受信端末は（手順７）の UPDATE の代わりに，通常の SIP 通信の INVITE に対するレスポンス（200 OK など）を受け取るので，送信端末は，受信端末が TWP 方式を行っていないことを理解し，通常の SIP 通信を行うか，通信を中断するかを判断することができる．また，これにより，TWP 方式未対応の受信端末にも対応することができ，現在運用されている SIP システムとの混在も可能になる．

②プロキシとの親和性

TWP 方式では，従来運用されている SIP プロキシに何の改良も加えずに，通信を行うことができ，親和性が高く，速やかな移行が期待される．

但し，SIP プロキシでは，メッセージボディ（SDP）の容量制限を行っているものが多いため，交換する公開鍵をボディに含めた場合，途中のプロキシを通過できず，通信が中断してしまう可能性がある．そのため，TWP 方式では，容量制限が行われていないことが多いヘッダに公開鍵を含めることによって，途中のプロキシを通過できず，通信が中断するというリスクを軽減している．

3.5 端末で PKI を用いる方式との比較

以下に TWP 方式と端末で PKI を用いる方式との比較を次の観点で行ったので，その結果を，表 1 に示す．

（１）端末の負担

認証と公開鍵対の維持管理に分けて比較した．

（２）各方式を実現するための条件

各方式の前提とそれを実現するための方式及びその条件について比較した．

（３）対攻撃性（攻撃に対する強度）

信頼するサービスに対する攻撃と SIP プロキシに対する攻撃に分けて対攻撃性を比較した．

以下，比較結果について考察を加える．

（１）端末の負担

TWP 方式では，公開鍵の登録や変更，抹消については，端末が所属するドメインの公開鍵配布サーバ（PKD）が行うため，ドメイン登録時に配布されたパスワードや共有鍵を利用することができるため，端末に新たな負担は生じない．これに対して，PKI 方式では，公開鍵の登録や変更，抹消などをドメインの外側にある認証局（CA）に依頼するため，新たに認証を受ける必要が生じ，端末に新たな負担

が生じる．

（２）各方式を実現するための条件

TWP，PKI 両方式とも，実現にあたっては，信頼できる第三者の存在を仮定する必要があり，実現性という面からは優劣をつけがたい．

（３）対攻撃性

信頼できる第三者が乗っ取られることに対する対攻撃性に関しては，TWP 方式がひとつの TWP を仮定しているため，攻撃が集中する可能性があるのに対して，PKI 方式では，複数の CA があるため，ひとつの CA が乗っ取られても，乗っ取られていない他の CA を用いるなどすればよいため，PKI 方式の方が優れていると考えられる．これに対しては，TWP 方式でも，複数の TWP を用いることができる方式について検討する必要があると考える．

比較項目	TWP 方式	端末で PKI を用いる方式
端末の負担（登録（認証））	所属ドメインの公開鍵配布サーバ（PKD）への登録をドメイン登録時に配布された共有鍵を利用して行えば、認証の負担は抑えることができる。	ドメインの登録とは独立に、改めて外部の（所属ドメインではないところにある）認証局（CA）への登録（認証手続きなど）を行うため大きな負担となる。
端末の負担（公開鍵対の維持管理）	公開鍵対の維持管理について、更新や廃止の際には、所属ドメインの PKD に新たにアップロードするだけでよいので端末の負担は少ない。	更に公開鍵対の維持管理についても、CA に対する手続きが必要で、端末に大きな負担を強いることになる。
前提	ネットワーク上に信頼できる Web Proxy（TWP）を設置する。	ネットワーク上に信頼できる認証局（CA）を設置する。
前提（絶対的な信頼を得るサービス提供者）の実現するための方式	ユーザ同士の共通認識として、ある特定のサービス提供者が信頼できるとする。（既に Closed Network では、そのような共通意識は存在する） 例）NTT などの電話会社など	既に、世界的に信頼できる、特定の認証局が存在する 例）Verisign などの root CA
前提のもとで各方式が成立するための条件	複数存在しても、同一セッション内では、送受信端末は、互いに共通の信頼できるサービス提供者（TWP）を使用する必要がある。	同一セッション内でも、送/受信端末は、異なる CA を使用することができる。
攻撃に対する強度（信頼サービスに対する攻撃）	同一セッションでは、同一の TWP を使用するため（危険の集中）、外部からの攻撃に対しては、端末 PKI 方式に比べて弱い。	同一セッションでも、異なる CA を使用していてもよいため、複数の CA を用いることができるという意味（危険の分散）で、TWP に比べての強度は強い。
攻撃に対する強度（SIP プロキシに対する攻撃）	送/受信の SIP プロキシが外部攻撃で乗っ取られても、または正しく動作しなくても、VoIP通信全体の安全性は保証される。	送/受信の SIP プロキシが外部攻撃で乗っ取られても、または正しく動作しなくても、VoIP通信全体の安全性は保証される。

※赤く塗られた部分は，他方に対して優れていると考えられる項目

表１．TWP 方式と端末で PKI を用いる方式との比較

Table1. Comparison between TWP Method and Method with PKI at UA

4. 評価

今まで述べてきた TWP 方式について，プロトタイプを作成し，動作確認を行ったので，本章では，その結果について報告する 17).

4.1 実験の目的

次の２点を確認することを目的として，作成したプロトタイプを用いて評価実験を行った．

・プロトタイプで TWP 方式の一連のシーケンスを動かすことによって，システムが問題なく動作することを証明する

・接続要求を発してから，メディア通信が始まるまでの時間を測定し，通常の SIP 通信の場合と比較することによって，TWP 方式が実用に耐え得る方式であることを証明する

以上を確認するため，評価実験を行った．

4.2 実験環境

実験に用いた環境は次の通りである．

・各 PC をひとつのモニタ機能付きスイッチングハブに接続して，他のネットワークの影響を受けないで，純粋に TWP 方式のみに要する時間を測定した．（図１０）また，リピータハブではなく，スイッチングハブを用いることによって，測定に際して，目的の通信以外の通信の影響も受けないようにした．

・途中に２つのプロキシを介するように設定して，プロキシをゲートウエイとした通信を実現した．

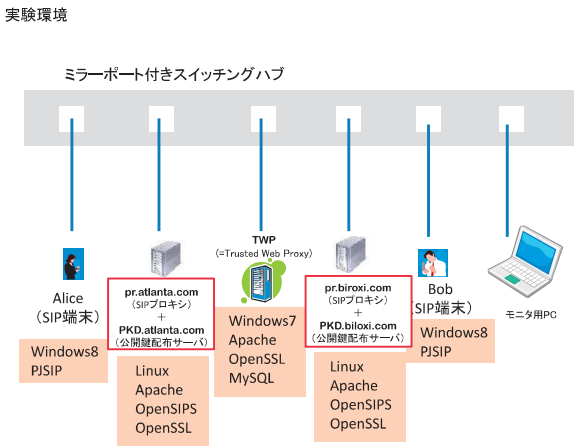

図１０　実験環境

Figure10 Environment for Experiment

4.3 実装

今回の実験では，次のような実装を行った．

・端末…OS として Windows8 を用い，通信プログラムとしては，PJSIP16)を TWP 方式用に C 言語で約 1000STEP の改良を行った．また，TWP に公開鍵を取得するためのプログラムとして，C 言語で約 150STEP ほどの独自プログラムを開発した．

・TWP…OS として Windows7 を用い，キャッシュ機能付き https サーバとして apache をベースに約７０STEP ほどの PHP を付加した．
・PKD…OS として Linux を用い，公開鍵配布サーバとして apache の https サーバの機能をベースに PHP を約１０STEP ほど追加した．
・SIP プロキシ…OS として Linux を，SIP プロキシサーバとして OpenSIPS14)のスクリプトを約１０STEP ほど変更したものを用いた．
・各 PC の暗号化モジュールとして OpenSSL15)モジュールを用いた．

4.4 実験

実験は次のような条件のもとで行った．
・暗号方式
公開鍵暗号方式として RSA（鍵長 2048bit），共有鍵暗号方式として AES（ブロック長　56bit，鍵長　12byte）で実験を行ったが，いずれも実用上問題がないセキュリティレベルである．
・PKI について
TWP，PKD，SIP プロキシの各サーバは，PKI を採用することを前提としているが，今回の実験では，CA を用いて実際に PKI を採用することはせず，各サーバの公開鍵は保証されているものとして実験を行った．
・端末から PKD への公開鍵のアップロードについて
TWP 方式では，端末は，PKD に公開鍵を予めアップロードすることになっているが，今回の実験では，既に公開鍵がアップロードされているものとして，実験を行った．
なお，今回の実験では，SIP プロキシと PKD を同じ PC 上に構築した．

4.5 実験結果

4.4 のような条件で実験を行った結果，問題なく TWP 方式のシーケンスが実行された．これにより，TWP 方式が問題なく動作することが確認された．また，端末が接続要求を発してからメディアが開始されるまでの時間（INVITE から 180 Ring までに要する時間）を計測し，通常の SIP と比較した結果を以下に示す．（表１，図１１）

単位：秒

	１回目	２回目	３回目	４回目	５回目
TWP 方式	2.38	2.20	2.57	2.63	2.57
通常の SIP	0.09	0.09	0.09	0.09	0.09

表１　TWP 方式と通常の SIP との開始時間の比較
Table1 Comparison of Starting Time between TWP Method and Regular SIP Communication

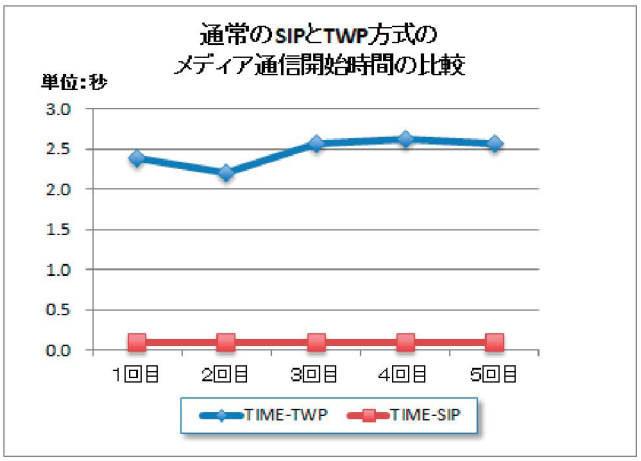

図１１　TWP 方式と通常の SIP との開始時間の比較
Figure11 Comparison of Starting Time between TWP Method and Regular SIP Communication

4.6 考察

実験により，TWP 方式が問題なく動作することを確認することができた．また，開始時間については，通常の SIP 通信が 0.09 秒だったのに対して，TWP 方式では，約 2.5 秒を要した．この内，約 2 秒は，次の２つの部分で要している．
・端末が INVITE リクエスト（図９の F1）を受け取ってから，TWP に対して公開鍵取得要求を送信する（図９の F2）まで
・UPDATE リクエスト（図９の F6）を受け取ってから TWP に対して公開鍵取得要求を送信する（図９の F7）まで
これは TWP 方式のリクエストヘッダなどの構文を解析して TWP 要求ということを認識するまでの処理に時間を要しているものと考えられる．従って，この部分を改善すれば，開始時間の短縮は可能であると考える．

5. まとめ

本稿では，インターネットのようなオープンネットワークにおいて，VoIP 通信を安全に行うための方法について述べた．既存の方式（DTLS-SRTP）では，通信の信頼性を所属ドメインのプロキシの署名に頼っているため，プロキシ自身が盗聴,改ざん,なりすましの介入を行った場合には，これを防ぐことができない．これを防ぐ方法として，端末が PKI を採用する方式があるが，この方式では，認証や認証後の公開鍵の維持管理に負担が掛かるため，現在普及していないということを指摘した．これを解決するため，ネットワーク上に信頼できるサービス提供者を想定して，そのサービス提供者が管理運営する Web プロキシを設置することによって，既存の方式の問題を解決する方式である

TWP 方式について，その手順を説明した．この際，信頼できる Web プロキシを設置するという仮定の妥当性について触れた．加えて，TWP 方式において，公開鍵の検証が失敗した場合の流れについても合わせて説明した．また，TWP 方式についても，なりすましを発見することができることについても触れた．

以上の後，プロトタイプを構築し実験を行ったことを述べ，TWP 方式が問題なく動作することが確認されたことを示した．更に，接続要求を発ししてからメディア通信を開始する時間について通常の SIP 通信と比較して多くの時間を要することについて言及して，その原因について考察した．

今後は，システムを改善することによって，開始時間を短縮し，更に実用的なシステムを構築する予定である．

謝辞

本研究は，ISPS 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) H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, “RTP: A Transport Protocol for Real-Time Applications,” RFC3550, IETF, July 2003

4) Modadugu, N. and E. Rescorla, "The Design and Implementation of Datagram TLS", Proceedings of ISOC NDSS2004, February 2004.

5) 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.

12) 高原尚志，中村素典，“信頼できる Web プロキシを用いた第三者の介入を許さない VoIP 通信の実現方式,” 第 14 回 インターネットテクノロジーワークショップ (WIT2013)，ソフトウェア科学会 インターネットテクノロジ研究会, June 2013.

13) 高原尚志，中村素典，“信頼できる Web プロキシを用いた安全な VoIP 通信の確立方式,” マルチメディア,分散,協調とモバイル(DICOMO2013)シンポジウム論文集, pp.1964-1969, June 2013.

14) "openSIPS | Main / HomePage," http://www.opensips.org/, March 2014 Access.

15) "OpenSSL: The Open Source toolkit for SSL/TLS," http://www.openssl.org/, March 2014 Access.

16) "PJSIP - Open Source SIP, Media, and NAT Traversal Library," http://www.pjsip.org/, Nov. 2013 Access.

17) 中村素典，“TWP 方式の実装評価”，電子情報通信学会技術研究報告, Vol.114, No.7, pp.85-90, December, 2012.