Vol.2014-IOT-24 No.10
2014/2/27

TWP 方式のスケーラビリティに関する課題

高原尚志[†1]

著者らは，VoIP 通信をセキュアに行うための方式として，信頼できる Web プロキシ（Trusted Web Proxy=TWP）を用いて SRTP のための共有鍵を安全に交換する TWP 方式を提案した．しかし現在の TWP 方式は，一つの TWP を設定することによって，信頼性を保証する方式であるため，インターネットのような大規模ネットワークでは，TWP に過度に負荷が掛かるなどの課題がある．そこで本稿では，TWP 方式を大規模ネットワークに適用するための課題を明らかにし，解決に向けた提案を行う．

Problems on Scalability of TWP Method

HISASHI TAKAHARA[†1]

We have proposed TWP method that realizes secure VoIP communication with a trusted web proxy (TWP). Using that method, we can exchange a shared secret for SRTP. However, TWP method needs to use only one TWP for secure communication. So, in large scale network like Internet, TWP could be overloaded. In this paper, we clear problems on TWP method for large scale networks and suggest some solutions.

1. はじめに

現在，インターネットを利用した音声通信（VoIP）が普及し，従来型の電話通信をしのいでいるとも言える．これは，インターネットに接続できる環境があれば，誰でもどこからでも無料で通信ができるということに由来する．つまり，たとえ国際電話を掛けても，料金は無料である．また，通話時間を気にすることなく話すことができることも普及の大きな要因と考えられる．しかし，セキュリティの面から考えると，免許事業であるが故に国のお墨付きを得た電話会社が通話の安全性を保証する電話通信に対して，誰でもが参加できるインターネットを利用した VoIP 通信は必ずしも安全な通信が保証されるとは限らない．従って，VoIP 通信は，経済的には有用であり，友達同士の誰に聞かれてもよいような会話であれば問題ないが，セキュリティを第一に優先するような国家機密レベルの情報交換を扱う場合には利用できない．

通信の安全性を考える際には，通常途中の第三者による「盗聴」などによる介入が想定される．この対策として，既存の方式では，メディア通信を暗号化する SRTP が広く知られている．SRTP[2]は，代表的なメディア通信方式である RTP を共有鍵で暗号化して通信を行う手法であるので，共有鍵を安全に交換する方式が必要となる．この方式としては，共有鍵暗号化通信である TLS の際の共有鍵の交換方式を利用した DTLS-SRTP[5]及びメディア通信の前に行われる SIP[1]に代表されるシグナリング通信までを含めた，安全な鍵交換の仕組みを規定した DTLS-SRTP-Framework[6]が提案され，既に標準化されている（以降，この２つを合わせて DTLS-SRTP 方式と言う）．

DTLS-SRTP 方式では，SIP を利用したシグナリング通信の段階で，SIP の通信内容保証機構である SIP Identity[3]を用いる．SIP Identity は端末でも採用することができるが，保証を行うエンティティは PKI を採用し，CA により公に保証されていなければならず，端末で PKI を採用するのは大変負担が大きいため，通常，端末が所属するドメインのプロキシが PKI を採用し，通信内容に署名を行うことによって通信内容を保証する．これにより，端末間の通信が保証されるという仕組みであるが，プロキシが介入して「盗聴」などを行った場合には，これを防ぐことはできない．この際，前述の通り，端末が PKI を採用して，自らの通信内容を保証すれば，上記の問題は解決できれば，負担が大きくこのような方法は普及していない．

そこで，端末の負担を抑えると同時に，端末間の通信を保証する方式として，著者らは，ネットワーク上に信頼できる Web プロキシ（TWP=Trusted Web Proxy）を設置し，これを利用して端末間で安全な通信を行う方式（TWP 方式）を提案した[14][15]．この方式を利用すれば，端末に負担を掛けずに，また公開鍵を端末自らが確認するため，中継プロキシを含む途中の第三者が「盗聴」などの介入を行うことができない．著者らは，この方式のプロトタイプを作成し，実システムでの実装評価を行い，問題なくフローが成立することを確認している．

ところが，TWP 方式は，ネットワーク上に一つの TWP

†1 新潟県立大学
University of NIIGATA PREFECTURE

を設置することによって，公開鍵の改ざんを防ぎ，通信の安全性を保証する方式であるため，ネットワークスケールをインターネットのような大規模なネットワークにまで広げると，TWP に負荷が集中し，レスポンスの遅延などの問題が発生するといった問題が推測され，このままでは，ごく限定的なスケールのネットワークでしか用いることができない．

そこで本稿では，TWP 方式を，インターネットのような大規模なネットワークにまで広げて使用できるように，TWP を複数設置する方式（拡張 TWP 方式）について，様々な観点から検討し，現在の最良の方式を提案する．

本稿では，第 2 章で本稿で扱う VoIP 通信について述べ，第 3 章で安全な通信を保証するための既存の方式である DTLS-SRTP 方式の説明とその問題点について述べ，第 4 章でこれを解決する TWP 方式とその問題点を，第 5 章で TWP 方式を拡張するための様々な手法と問題点及び検討した結果の最良の TWP 方式（これを拡張 TWP 方式と言う）について述べ，第 6 章で本稿のまとめと今後の問題点について論ずる．

2. 本稿で扱う VoIP 通信

インターネットを利用した VoIP 通信として，まずシグナリング通信で使用するメディアやポート番号など互いの情報を交換した上で，メディア通信に移行する方式が広く知られている．本稿では，広く利用できるシステムを対象とするため，上記の方式（シグナリング通信を行った後にメディア通信を行う方式）を対象とする（図 1）．シグナリング通信としては，広く知られた SIP を用い，メディア通信としては，こちらも広く知られた RTP の暗号化通信である SRTP を用いる．

またシグナリング通信としては，直接端末同士が通信を行うこともできるが，スケールの大きな，ドメイン間での通信を考慮して，ゲートウエイ（G/W）に SIP プロキシを配し，互いの端末が，それぞれ所属する SIP プロキシを介してシグナリング通信を行うものとする．このようにすることによって，スケールの大きな通信ができると同時に，受信端末が移動した場合でも，プロキシが移動を把握し，適切な場所に通信を転送することが可能となる．

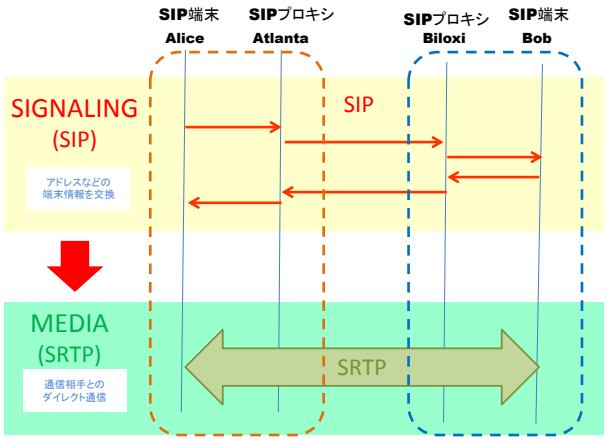

図 1　本稿で扱う VoIP 通信
Figure1 VoIP in this paper

3. 既存の方式（DTLS-SRTP 方式）

インターネットを利用した VoIP 通信において，本稿ではメディア通信は共有鍵暗号化通信である SRTP を用いることによって，途中の第三者の介入を防ぐことができるものとしている．しかしこれには，SRTP で用いる共有鍵を安全に交換する方式が同時に提唱されていなければならない．これには，既存の方式として DTLS-SRTP 方式がある．DTLS-SRTP 方式では，DTLS のハンドシェイクプロトコルを用いて共有鍵を交換する（図２）．

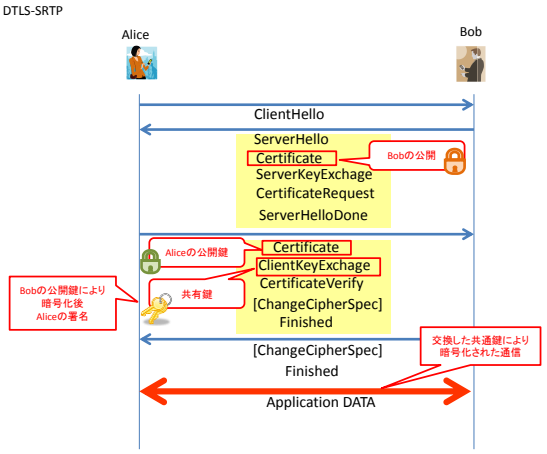

図２　DTLS-SRTP
Figure2 DTLS-SRTP

しかし，安全な共有鍵の交換に際して，端末同士が安全に公開鍵を交換していなければならず，これを保証するために，事前に行われる SIP を利用したシグナリング通信において，公開鍵の fingerprint を交換する（図３）．

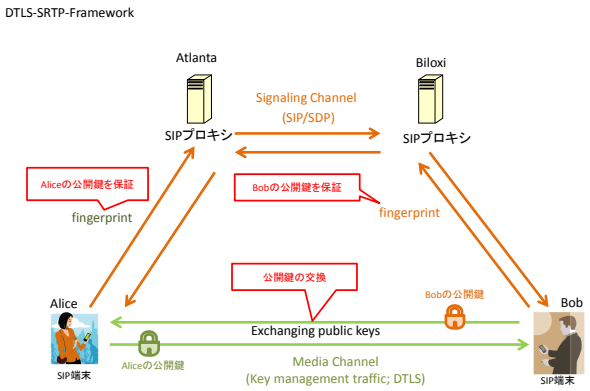

図３ DTLS-SRTP-Framework
Figure3 DTLS-SRTP Framework

更に交換される fingerprint を保証するために，SIP の保護機構である SIP Identity を用いる．この際，送信端末，受信端末双方の公開鍵が保証される必要があるため，受信端末は送信端末から公開鍵の fingerprint が添付された INVITE を受け取ると，送信端末に対して UPDATE を送信し，これに受信端末の fingerprint を含める[4]．この際，INVTE 及び UPDATE を送信する際に，送信側プロキシ及び受信側プロキシにおいて署名を行い，SIP Identity によってそれぞれの fingerprint の完全性を保証する（図４）．また，端末とプロキシの間の通信も，Proxy Authenticate や TLS などを用いて安全に行われている．

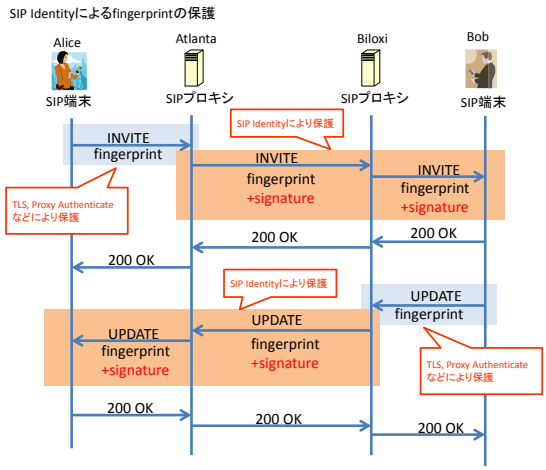

図４ SIP Identity による fingerprint の保護
Figure4 Protection of fingerprint using SIP Identity

この方式を用いれば，PKI を採用している SIP プロキシによって署名が行われ，通信の安全性が保証され，途中の第三者による介入を防ぐことができる．しかし，この方式は，プロキシの信頼性に依存しているため，プロキシが介入を行い，公開鍵を改ざんすれば，通信全体の信頼性は保証されない．つまり，この方式では，プロキシによる「盗聴」を防ぐことはできない（図５）．[11][12][13]

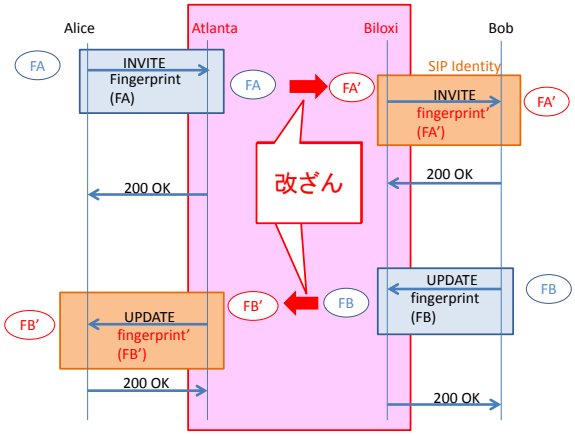

図５ プロキシによる改ざん
Figure5 Falsification in SIP proxy

インターネット上の通信は誰でもが利用できるため，所属ドメインのプロキシが必ずしも正しい動きをするとは限らない．このような状況のもとでは，DTLS-SRTP 方式は，インターネット上の安全な VoIP 通信を保証するとは言えない．

4. TWP 方式

第 3 章で指摘した既存の方式の問題点を解決する方式として，著者らは TWP 方式を提案した．TWP 方式では，ネットワーク上に信頼できる Web プロキシ（TWP）を設置して，端末の公開鍵をキャッシュさせることによって，端末自身が，自らの公開鍵の完全性を確認することができると言う方式であり，概要は次の通りである（図６）．

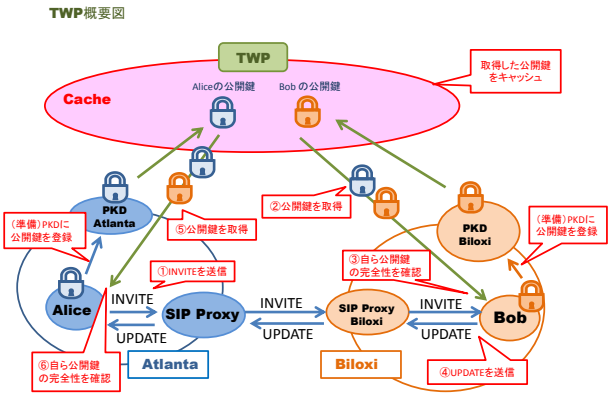

図６ TWP 方式の概要図
Figure6 Overview of TWP method

TWP で扱うエンティティは，送信及び受信用の SIP 端末，SIP プロキシ，所属する端末の公開鍵を公開する公開鍵配布サーバ（pkd）及び TWP である．

流れとしては，次の通りである．

事前準備

送信端末（alice）及び受信端末（bob）は，事前に公開鍵対を作成し，所属するドメイン（atlanta 及び biloxi）の公開鍵配布サーバ（pkd.atlanta 及び pkd.biloxi）に，自らの公開鍵をアップロードしておくものとする．また，alice は，共有鍵を作成し，公開鍵配布サーバ及び TWP は，PKI を採用しているものとする（図７）．

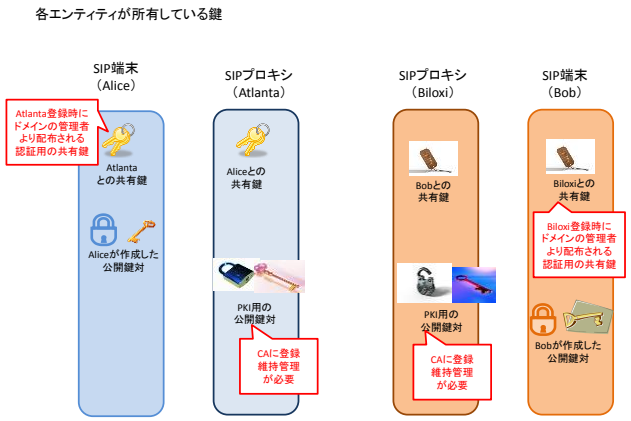

図７ 各エンティティが所有している鍵
Figure7 Keys of entities

TWP 方式による鍵交換の流れ

（１）alice はは bob に向けて，通信要求（INVITE）を送信する．この際，alice が所属するドメインのプロキシサーバ（pry.atlanta）及び bob が所属するドメインのプロキシ（pry.biloxi）を経由する．

（２）bob は INVITE を受けとると，自ら（bob）と送信元（alice）の公開鍵の取得命令を TWP に対して送信する．

（３）TWP は pkd.atlanta 及び pkd.biloxi から両者の公開鍵を取得して，bob に送信すると同時に，一定期間キャッシュする．

（４）bob は，取得した自らの公開鍵の完全性を確認した後，alice に対して UPDATE メソッドを送信する．

（５）alice は bob からの UPDATE を受け取ると，自ら（alice）と相手（bob）の公開鍵を TWP を通じて取得し，自らの公開鍵の完全性を検証する．

（６）alice は，共有鍵を作成し，bob の公開鍵で暗号化した後，署名を施して，UPDATE に対する 200 OK レスポンスに含めて bob に送信する

（７）bob は，取得した alice の公開鍵を用いて署名を確認し，暗号化された共有鍵を復号する

（８）bob は，復号に成功すると，alice に対して INVITE に対する 200 OK を返す

以上のようにすることにより，端末自身が自らの公開鍵を確認することができるため，プロキシも含めた途中の第三者による改ざんを防ぐことができる．なお，上記において TWP と端末との間の通信及び TWP と公開鍵配布サーバとの間の通信は PKI を用いた https 通信であり，安全に通信が行われるものとする．

以下に詳細なシーケンスを示す（図８）．

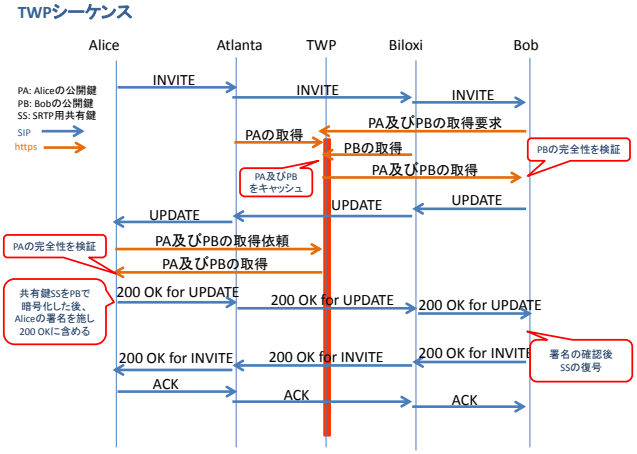

図８ TWP 方式のシーケンス図
Figure8 Sequence of TWP method

TWP 方式の利点

端末同士の通信を安全に行う方式として，端末自身が PKI を採用するという既存の方式がある．しかし，PKI は登録・維持・管理などのコストが大きいため，現在普及していない．これに対して，TWP 方式では，TWP 用に端末を改良するという初期コストはあるものの，一度導入してしまえば，通常の SIP 通信に比べて維持管理に要するランニングコストは掛からない．また，DTLS-SRTP 方式では SIP プロキシで署名など SIP Identity のための処理を行う必要があるため，SIP プロキシが SIP Identity に対応している必要があるが，TWP では SIP プロキシによる署名は必要ないため，SIP プロキシが SIP Identity に対応していない場合でも，安全に通信ができ，DTLS-SRTP 方式と比較して多くのドメインとの通信も可能となる．

TWP 方式の問題点

ところで，TWP 方式では，ネットワーク上に唯一の TWP を設置することにより，公開鍵の完全性を保証している．つまり，所有している端末自身が検証した公開鍵と同じ公開鍵を TWP のキャッシュから相手が取得することにより，

相手に正しい公開鍵を取得させるという方式である．しかし，この方式では，ネットワークのスケールを大きくすると TWP に負担が掛かり，レスポンスが遅くなるという問題が考えられる．インターネットのような大規模なネットワークで TWP を用いるためには，この問題を解決する必要がある．

5. 拡張 TWP 方式

第４章で指摘した TWP 方式のスケールに関する問題(以降，スケール問題という）を解決する方式として，いくつかの方式が考えられる．ここでは，現在検討している方式について述べた後，現段階で最善と考えられる方式を提案する．

(1) TWP の性能強化（TWP 強化方式）

上記の問題を解決する最も単純な方法は，TWP の性能を強化し，どのようなスケールにも対応できるようにする方法である．しかし，インターネット全体の要請に素早く応えられるような性能を有するコンピュータがあるとは考えづらく現実性がない．

(2) 複数の TWP の同期（TWP 同期方式）

その他の解決方法として，ネットワーク上に複数の TWP を設置して，互いに TWP がキャッシュの同期を行う方式が考えられる（図９）．しかしこの方式では，ネットワークの規模が大きくなると TWP の台数も増加し，互いに同期をとるのに時間が掛かるという問題がある．また，同期のタイミング，同期がとれていない場合の対応，同期時に異なる鍵をキャッシュしていた場合の対応など様々な問題が生じることが予測される．

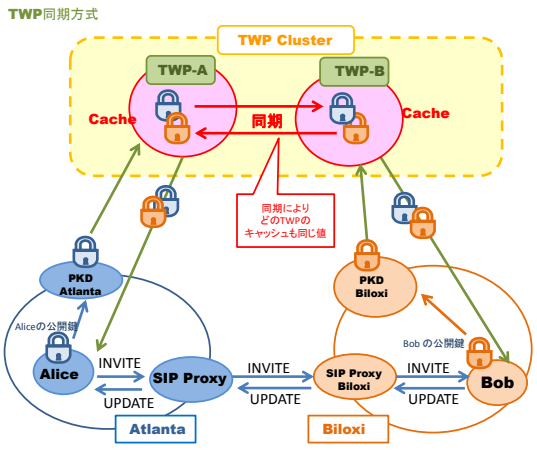

図９ TWP 同期方式
Figure9 TWP method with synchronization

(3) 複数の TWP から一つを選択（TWP 選択方式）

この方式は，複数の TWP の中から，送信端末と受信端末がなんらかのルールに基づいて，同じ TWP を選択する方式である．この方式であれば，スケール問題にも対応でき，同期方式のときのような問題も存在しない．ここで問題となるのは，送信端末と受信端末が同じ TWP を安全に選択するルールである．「安全に」とは，途中の第三者の介入を受けた結果，送信端末と受信端末が異なる TWP を選択し，結果として通信相手が改ざんされた公開鍵を取得することがないようにするということである．

この解決策として，受信端末の SIP アドレスをもとに TWP を選択するという方法が考えられる．呼が送信端末から受信端末に送信される場合，送信端末のアドレスは，途中の第三者によって書き換えられる可能性がある．つまり，送信端末と受信端末の間に第三者が介在して，通信を「盗聴」することが可能となる（図６）．これは，受信端末が送信端末のアドレスを事前に知り得ないことから生じる問題である．これに対して，TWP 選択の基準として受信端末のアドレスを用いれば，この問題は解決する．送信端末は，送信相手である受信端末のアドレスを知っているのと同時に，受信端末も通信が到達した時点で自らのアドレスを知っている．つまり，受信端末のアドレスは，送信端末，受信端末双方に自明のアドレスとなり，途中の第三者による改ざんを受けない．

受信端末のアドレスを使用すれば，途中の第三者による「盗聴」を防ぐことができるということを述べたが，次の段階として，負荷をうまく分散するようにルールを決めなければならない．複数の TWP を設置して，安全に TWP を選択できても，ある TWP に負荷が集中すれば，複数の TWP を設置している意味がなくなる．

その一つの答えとして，DHT(=Distributed Hash Table)を用いることが考えられる．DHT は，P2P の際の負荷分散などに用いられるハッシュ方式で，これを TWP の選択に適用する．例えば，COM 用の TWP，EDU 用の TWP といったように受信端末のアドレスのドメインごとに TWP を決める方式も考えられる．しかし，この方式では，あるドメインに負荷が集中する可能性がある．そこで，ドメインと関係がない形で TWP を選択する方式を考察した．例えば，bob@biloxi であれば，@の部分をドット（.）に置き換えて bob.biloxi をハッシュした値 DHT(bob.bioxi)によって TWP を決めるという方法が考えられる．この場合，事前にハッシュ値と TWP のアドレスのリストを端末が取得しておく必要がある．リストの取得については，ルート証明書のように予め端末に埋め込む方式もあるが，リストを TWP のサイトで公開し，https などで配布する方法がよいのではないかと考えている．このようにすることによって，予め端末に埋め込むといった端末配布メーカに負担を強いることもなく，TWP の負荷の状態によっては適宜リストの修正ができるという利点もある（図１０）．

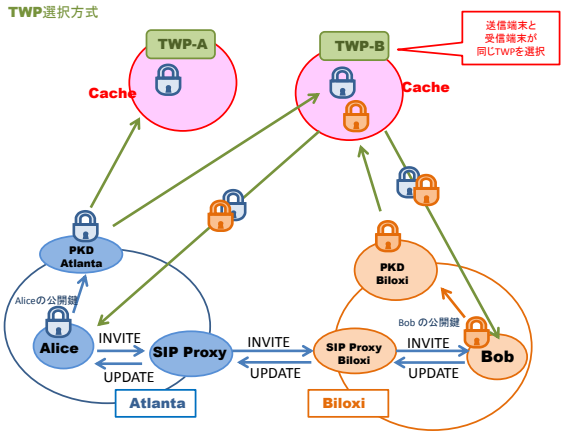

図１０ TWP 選択方式

Figure10 TWP method with section

以上により，本稿では，TWP 方式のスケール問題に対応した方式として，複数の TWP の中から，受信端末のアドレスに基づいてハッシュ処理を行い選択された TWP を用いて TWP 方式を行う拡張 TWP 方式を提案する．

6. まとめ

インターネット上の VoIP 通信を安全に行うための方式について，既存の方式として DTLS-SRTP 方式を紹介した．DTLS-SRTP 方式では，途中の第三者の介入を防ぐことはできるが，SIP プロキシの信頼性に依存しているため，プロキシの介入を防ぐことはできないという問題があることを指摘した．この問題を解決するために，著者らは TWP 方式を提案しているが，TWP 方式はネットワーク上にただ一つの TWP を設置することにより，通信の安全性を保証するものであるため，スケールの大きなネットワークでは TWP の負荷が大きくなり，適用が困難であるという問題を指摘し，本稿でこの問題を解決する複数の方法を提案し考察を加えた結果，ネットワーク上に複数の TWP を設置して，受信端末のアドレスに基づいて TWP を選択する方式が最適であるという結論に至った．更に，ひとつの TWP に負荷が集中しない選択方式についても考察し，P2P などでも用いられている DHT 方式がよいのではないかという考えに至った．従って，本稿では，スケール問題に対応した TWP 方式として，複数の TWP から受信端末のアドレスを基に DHT を利用して一つを選択する方式を提案に至った．

謝辞 本研究の一部は JSPS 科研費 23500096 の助成を受けたものである．心より感謝の意を表するものである．

参考文献

[1] 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.

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

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

[4] J. Elwell, "Connected Identity in the Session Initiation Protocol (SIP)," RFC4916, IETF, June 2007.

[5] 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.

[6] 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.

[7] 高原尚志，中村素典，"SRTP のための鍵交換の安全性を向上させる SIP におけるドメイン内認証方式,” 電子情報通信学会技術研究報告，Vol. 109，No.476，pp.13-18, March 2010.

[8] 高原尚志，中村素典，“SIP における DTLS-SRTP fingerprint 交換の完全性検証方式,” 第 11 回 インターネットテクノロジーワークショップ (WIT2010)，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 2010.

[9] 高原尚志，中村素典，“シグナリングボディの完全性検証方式,” マルチメディア,分散,協調とモバイル(DICOMO2010)シンポジウム論文集，pp.976-982，June 2010.

[10] Hisashi Takahara and Motonori Nakamura: "Enhancements of SIP Signaling for Integrity Verification," The Forth Workshop on Middleware Architecture in the Internet (MidArch2010), Proceedings of the 2010 International Symposium on Applications and the Internet (SAINT2010), pp. 289-292, July 2010.

[11] Hisashi Takahara and Motonori Nakamura: " Problems on Secure Exchange of Shared Secret for SRTP Using DTLS-SRTP," The 7th International Workshop on Security (IWSEC2012), Fukuoka, Japan, Nov. 2012.

[12] 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. Nov., 2012.

[13] 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, Dec., 2012.

[14] 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 通信の検証方式,” 電子情報通信学会技術研究報告, Vol.112, No.404, pp.19-24, Jan., 2013.

[15] 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, July 2013.