科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　１８　日現在

機関番号：　２３１０２
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５０００９６

研究課題名（和文）ＳＩＰによる通信のセキュリティに関する研究

研究課題名（英文）Study for Secure Communication with SIP

研究代表者
高原　尚志（TAKAHARA, Hisashi）

新潟県立大学・国際地域学部・講師

研究者番号：９０３４０１３２

交付決定額（研究期間全体）：（直接経費）　　4,000,000円、（間接経費）　　1,200,000円

研究成果の概要（和文）：本助成を通じて、「SIPを用いたセキュアなVoIP通信を実現する」ための問題点を明らかにした。特に、途中のプロキシの介入を防ぐことができないという点に着目した。これを解決するため、ネットワーク上に信頼できるWebプロキシを設置することによって、端末の信頼性を保証する方式（TWP方式）を提案し、プロトタイプを実装して問題なく動作することを証明した。これによって、安全なVoIP通信を低コストで実現することができる。また、上記TWP方式の発展形として、大規模ネットワークにも適応した拡張TWP方式を提案した。また、以上の結果を論文やシンポジウムなどで発表することで、助成の成果を広く社会に還元した。

研究成果の概要（英文）：We pointed out some problems for "Secure Communication with SIP". Especially, we focused on a problem that we could NOT protect communication from intervention of proxies. Thus we have suggested TWP method that we established a reliable web proxy in a network. Then we can realize secure VoIP communication. Additionally, we also suggested extended TWP method that adapt to large scale networks. Finally, we wrote some papers and had presentations at some symposiums, and we have returned benefits from this grant to society.

研究分野：　情報学

科研費の分科・細目：　計算機システム・ネットワーク

キーワード：　SIP　VoIP　TWP　DTLS　SRTP　セキュリティ　プロキシ

１．研究開始当初の背景

現在、インターネット電話をはじめとして、インターネットを利用したメディア通信が普及しつつある。しかし、誰でもが利用できるインターネットを用いているため、第三者による盗聴、改竄、なりすましなどの危険がある。そこで、SIP などで広く用いられている RTP 方式に対しては、共有鍵を用いて音声通信を暗号化するための手法（SRTP）が提案されている。しかし、この共有鍵が事前に安全に交換できなければ、SRTP の効果が得られず音声通信自身の信頼性も失われてしまう。共有鍵を安全に交換する手法はすでにいくつか提案されているが、それらも、メディア通信の前に、互いの情報をやり取りするためのシグナリング通信において、安全に情報が交換されることを前提としている。
現在、シグナリング通信には、パスワードによる送信端末の認証や、PKI に基づく通信内容の保証のための方式が、既存の技術として提案されている。しかし、SRTP のための共有鍵を安全に交換するためには、これだけでは不十分で、第三者による介入の危険性を残している。特に、送受信側プロキシの介入を防ぐ方法については、いずれの提案もなされていない。インターネットにおいては、誰でもがプロキシを提供することが可能である。従って、電話会社が提供する電話システムと異なり、提供されたプロキシによる介入も充分考慮される必要が生じる。

２．研究の目的

インターネット上で電話をはじめとするメディア通信サービスを提供する技術として広く用いられている SIP において、続くメディア通信においての「盗聴」、「改竄」、「なりすまし」を防止するセキュリティ対策技術は重要な要素技術の１つである。具体的には、メディア通信での第三者による介入を防ぐための暗号通信に必要な暗号鍵を、先立って行われるシグナリング通信（SIP 通信）において安全に交換するための方法は、安全なメディア通信実現に欠かすことができない。
現在、既存の方式として全ての端末において PKI を用いることにより交換する端末の鍵の信頼性を保証する手法があるが、鍵の維持管理など運用コストが高くなるため、現在普及しておらず、コストを抑えつつ効率の良い対策技術が求められている。そこで、メディア通信で行われる暗号通信のための共有鍵を安全に交換するために、メディア通信に先立って行われるシグナリング通信において、端末の公開鍵を安全に交換する SIP のための認証方式を検討し、そのための詳細な拡張方法を設計する。また、提案する方式が実システムでも問題なく動くことを検証するため、その方式を組み込んだプロトタイプを構築し評価を行う。これにより、その効果の検証を行う。そして、提案内容や検証結果を論文として発表するとともに標準化することによって、本助成の成果を広く社会に還元することを目指した。

３．研究の方法

インターネット電話については、既に相当程度普及している。しかし、専用の回線を利用しているため使用できる利用者が制限されたり、通信の安全性を保証していなかったりと、どれも課題を残している。本研究では、これらの課題を解決するため、誰もが利用できるインターネットを用いた、安全なメディア通信を実現するためのアイデアを考案し、その実用性を検証したが、その際に、次のステップを採用した。

（ステップ１）連携研究者とのミーティングによるアイデアの洗練

連携研究者とのミーティングを重ねることによって、アイデアを洗練されたものに仕上げた。

（ステップ２）外部の専門家からの意見

連携研究者とのミーティングにより洗練したアイデアを、シンポジウムや国際会議などで発表することによって、広く専門家からの意見を得た。そして、更なるブラッシュアップを行った。

（ステップ３）プロトタイプによる検証

（ステップ１）及び（ステップ２）で洗練したアイデアの実用性を検証するため、実際にプロトタイプシステムを構築して評価を行った。実際にシステムを動かすことによって、実用上の問題点を見出し、更なる改良を重ねるというサイクルを繰り返した。

以上、３ステップサイクルを繰り返すことにより、実用的なシステムを実現し、その結果を論文にまとめた。今後は、この成果を世界中の多くの人々が利用できるようにするため、国際標準化活動も合わせて行っていく予定である。

４．研究成果

３年間の本助成期間を通じて、多くの学会に参加し、SIP を用いたセキュアな VoIP 通信を実現するために多くの専門家の意見をきくことができた。成果としては、次の３段階であった。

（第１段階）既存の VoIP 通信の問題点を明らかにする

国際会議やシンポジウムなどを通じて、既存 SIP を用いてセキュアな VoIP 通信を実現するための問題点を明らかにした。

具体的には、端末がプロキシを介して通信を行う場合、既存の方式では、通信全体の信頼性が送信側、受信側それぞれのプロキシによって保証されるため、プロキシ自身が介入した場合（通信の改ざんや盗聴などを行った

場合）には、信頼性を保証することができないという問題点を明らかにした。

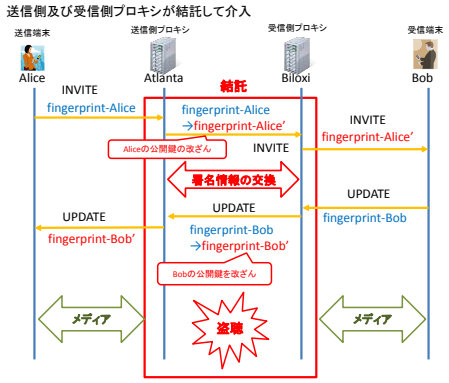

図１　既存の VoIP 通信の問題点

これを解決する既存の方式としては、各端末で PKI を用いるという方法があるが、公開鍵対の維持管理にコストが掛かるため、普及していない。そこで、コストを抑えた方式が求められることを指摘した。

（第２段階）上記の問題の解決策を提示する

上記の問題点を解決するため、ネットワーク上に信頼できる Web プロキシ(TWP=Trusted Web Proxy）を設置する方式（TWP 方式）を提案した。TWP 方式は、ネットワーク上に信頼できる Web プロキシを設置し、そこに端末の公開鍵をキャッシュさせる方式である。TWP にキャッシュされた公開鍵を互いの端末が確認することにより、途中の改ざんを防ぐことができる。この方式においては、Web プロキシに公開鍵をキャッシュさせるだけなので、PKI と比較してコストを抑えることができる。この方式（TWP 方式）の有効性を検証するためプロトタイプを実装して、一連のシーケンスが問題なく動作することを確認した。また、通信開始までの時間を計測して、既存の SIP 通信と比較し、その実用性も確認した。

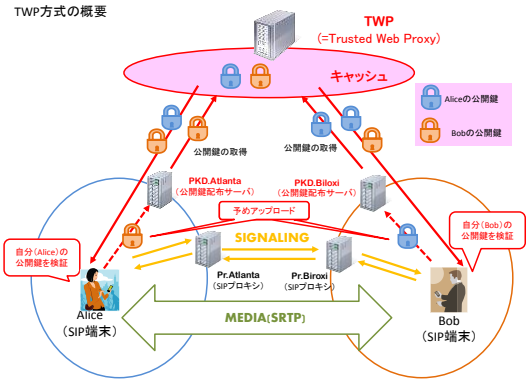

図２　TWP 方式

（第３段階）上記 TWP 方式の発展形として、大規模ネットワークにも適応した拡張 TWP 方式を提案した

上記 TWP 方式では、送受信端末の公開鍵の信頼性を保証するために、ネットワーク上に設置する信頼できる Web プロキシは、ひとつである必要があった。そのため、大規模ネットワークでは、TWP に負荷が集中し、うまく適応できない可能性があった。そこで、複数の TWP をネットワーク上に設置して、同一セッションにおいては、送受信端末が同一の TWP を選択するという方式（拡張 TWP 方式）を考案し提案した。この方式では、複数の TWP を負荷に応じて臨機応変に増減するため、P2P ネットワークで用いられている DHT の原理を応用する。これにより、アドホックな TWP の増減に対応する。また、この方式を活用すれば、負荷の増減に応じた TWP の増減も可能となる。

以上の結果を、適宜論文にまとめ、研究会やシンポジウムなどで発表した。これにより、本助成の成果を広く社会に還元した。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 8 件）

① 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、査読有、pp.111-112., November 2012.

② 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．、IN2012-136(2012-12)、情報ネットワーク、Vol.112、No.352、pp.85-90.、December 2012.

③ 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、MoMuC2012-43(2013-1)、モバイルマルチメディア通信、Vol.112、No.404、pp.19-24.、January 2013.

④ 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）、査読有、June 2013.

⑤ 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、査読有、IPSJ Symposium Series Vol.2013、No.2、pp.1964-1969、July 2013.

⑥ 高原　尚志,、中村　素典、TWP 方式のスケーラビリティに関する課題、情報処理学会研究報告.、IOT、[インターネットと運用技術]、Vol. 2014-IOT-24、No. 10、pp.1-6.、2014.2.

⑦ 高原　尚志,、TWP 方式の実装評価,、電子情報通信学会技術研究報告.、IN、情報ネットワーク、Vol.114、 No.7,、pp.17-22.、April 2014.

（他１件）

〔学会発表〕（計 10 件）

① Takahara, Nakamura, “Problems on Secure Exchange of Shared Secret for SRTP Using DTLS-SRTP,” The 7th International Workshop on Security (IWSEC2012), (at Nishijin Plaza, Kyushu University, Fukuoka, Japan.), November 2012.

② 高原　尚志,、第三者によるインターネット電話への介入防止方式、第８回パーソナルコンピュータ利用技術学会全国大会（於、大阪国際大学（枚方キャンパス））、第８回パーソナルコンピュータ利用技術学会全国大会講演論文集（CD-ROM 版）、pp.159-162., December 2013.

（他８件：上記雑誌論文に記載）

〔図書〕（計　0 件）

〔産業財産権〕
○出願状況（計　0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　0 件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織

(1)研究代表者　高原尚志
（025）270-7179

研究者番号：90340132

(2)研究分担者　なし
（　　）

研究者番号：

(3)連携研究者　中村素典
（03）4212-2541

研究者番号：　30268156