安全な SIP セッション確立方式の提案とその評価

田中　真也　　木村　成伴　　海老原　義彦
筑波大学大学院システム情報工学研究科

1　はじめに

VoIP のセッション確立，変更，切断などをするシグナリング制御プロトコルとして SIP (Session Initiation Protocol) が広く普及している．この SIP のメッセージはテキストで構成されその形式は厳密には定められていない．このため，これを中継するすべての SIP サーバはその内容を解析する必要があり，このメッセージ解析に対して約 50% の処理時間を費やしている [1]．これに加えてメッセージを暗号化すると処理時間が更に増えるため，SIP メッセージは平文で送られるのが一般的であるが，SIP メッセージの盗み見やセッションハイジャックなどが起きる可能性がある．そこで著者らは，メッセージ全てを暗号化せずに，一部のデータを暗号化することで SIP サーバの負荷の抑制をしつつ，セッションの不正切断を防ぐ安全な SIP セッション確立方式 [2] を提案した．本論文では，文献 [2] で出来なかった実験を行い，本方式の有効性を示す．

2　安全な SIP セッション確立方式

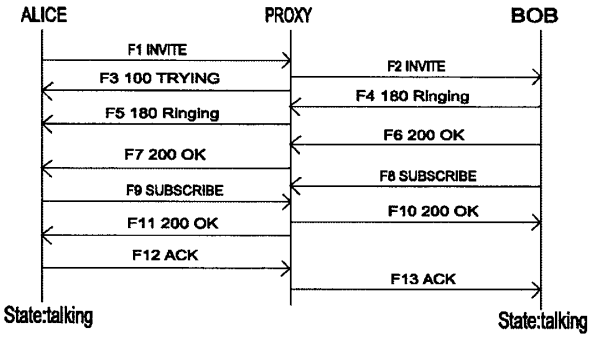

図 2.1　提案方式 (セッション確立)

安全な SIP セッション確立方式 [2] において，ALICE が SIP サーバである PROXY を介して BOB とセッションを確立するときのメッセージの流れを図 2.1 に示す．

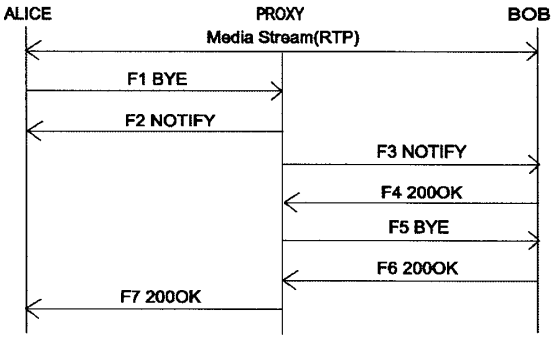

図 2.2　提案方式 (セッション切断)

ここで，ALICE と BOB は，共有鍵 Sa と Sb を，それぞれ PROXY と共有している．図 2.1 に示すように，セッション開始時にまず，従来の SIP と同様のセッション参加要求 (F1–F7) を行った後，ALICE と BOB は PROXY に対して SUBSCRIBE メッセージを送る (F8, F9)．これにより，BYE メッセージが届いたら直ちに NOTIFY メッセージを ALICE と BOB に通知するよう PROXY に要請している．そして，この要請を受諾すると，PROXY は返信メッセージ 200 OK のメッセージヘッダに Content-Type: application/binary-data，メッセージボディに共有鍵 Sa, Sb にて暗号化した 2 つのランダムな文字列 (Na, Nb) と 1 つのセッション共有鍵 (ALICE には La, BOB には Lb) を追加して送信する (F10, F11)．最後に，確認応答がやり取りされ (F12, F13)，セッションが確立されると，ALICE と BOB は自身の通話状態を表す state を talking (通話中) にする．次に，セッション終了時は，図 2.2 に示すように，まず従来方式と同様に ALICE が PROXY に BYE メッセージを送信する (F1)．この BYE メッセージにはランダムな文字列 Na を共有鍵 La にて暗号化した値をメッセージボディに加えている．これを受信した PROXY は，La で復号した文字列が Na と等しい場合のみ，ALICE と BOB に対して NOTIFY メッセージを通知する (F2, F3)．この際，ランダムな文字列 Nb を La, Lb にて暗号化して送信し，復号した時に等しい場合のみ state を free に変更をする．その後，BOB は PROXY に対して 200 OK メッセージを送信し (F4)，このメッセージを受信した PROXY は，F1 の BYE メッセージを BOB に転送する (F5)．state が free に変更さ

Evaluations of Safe SIP Session Establishment Method
†Shinya Tanaka　†Shigetomo Kimura　†Yoshihiko Ebihara
†Graduate School of Systems and Information Engeneering, University of Tsukuba

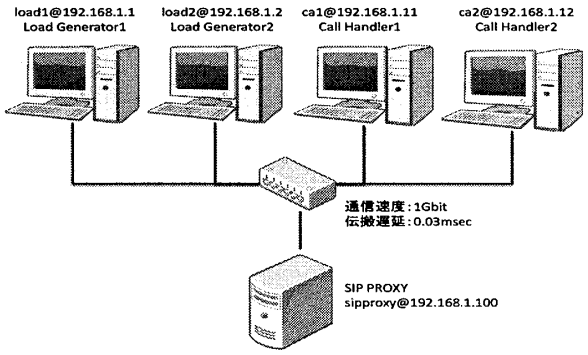

図 3.1　ネットワークトポロジ

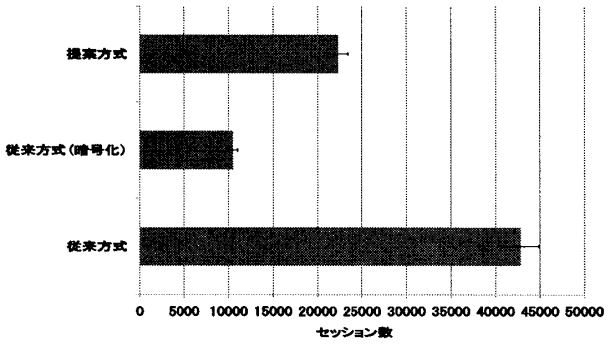

図 3.2　接続成功セッション数

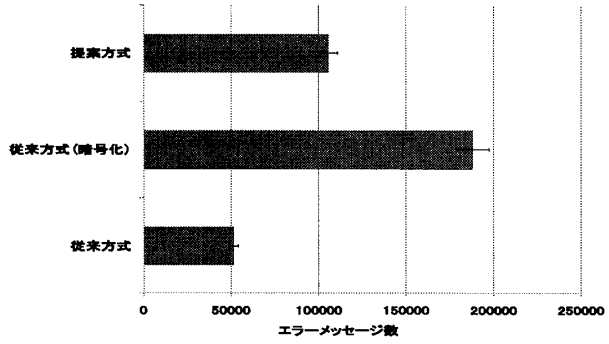

図 3.3　エラーメッセージ数

れているため，この BYE メッセージは受諾され，従来方式と同様に，200 OK メッセージが BOB から ALICE に転送されると (F6, F7) セッションの切断が完了する．

3　評価実験

提案方式の有用性を確認するために，従来方式で暗号化を行わなかった場合，従来方式で送るメッセージを全て DES (共有鍵は Sa と Sb) で暗号化した場合，そして提案方式を用いた場合を対象として，セッション接続からセッション切断までの一連の処理を連続して行った際，正しくセッション確立を行えた数と，処理できなかったメッセージ数を元に測定する．実験のネットワークトポロジを図 3.1 に示す．実験では，各 Load Generator が PROXY を経由して INVITE メッセージを Call Handler に送信して SIP コネクションを確立し，その後，直ちにこれを切断する．各 Load Generator が 1 秒ごとに INVITE メッセージを 500 メッセージ送信する測定を 60 秒間行い，これを 10 回行った時の接続成功セッション数と，キュー溢れなどの理由でメッセージが正しく処理出来なかったメッセージ数の平均と信頼係数 95% の信頼区間を図 3.2 及び図 3.3 に示す．

図 3.2 より，従来方式 (暗号化あり) と，提案方式の平均接続成功セッション数は，従来方式 (暗号化なし) のそれぞれ 24.5% と 52.1% になった．暗号化を行うと処理量が増えるため，接続に成功するセッション数が大幅に減少するが，提案方式では一部のメッセージのみしか暗号化しないため，従来方式 (暗号化あり) のときよりも 2 倍以上のセッションの接続に成功していることが分かる．次に，図 3.3 において，従来方式 (暗号化あり) と提案方式は従来方式 (暗号化なし) と比べて平均未処理メッセージ数がそれぞれ 3.6 倍と 2.0 倍になった．図 3.2 と同様に，暗号化の処理量の違いによって，提案方式で処理できなかった平均メッセージ数は従来方式 (暗号化あり) の約半分に抑えられることが分かる．

4　まとめ

本論文では文献 [2] の安全な SIP セッション確立方式で行えなかった実験を行い，ネットワークを介して通信を行った際も提案方式が有効であることを確認した．また，提案方式を採用した SIP サーバを介して従来方式にしか対応していないクライアント同士がセッションを確立し正しく切断を行えることも確認している．今後の課題として，メッセージ解析部の高速化及び，PROXY が複数台ある際の検証を行うことが挙げられる．

参考文献

[1] J. Yin, “Session Initiation Protocol Benchmark Suite,” Master’s Thesis, Delft University of Technology, May 2004.

[2] 田中 真也, 木村 成伴, 海老原 義彦, “SUBSCRIBE メッセージを使用した安全な SIP セッション確立方式,” 信学技報 ,IN2009-101, pp. 81–86,Dec. 2009.