講演番号： 81

セキュアな端末間匿名 IP 通信サービスの提案

B-16 A Proposal of Highly Secure Anonymous IP communication Services

小林 大翼† 小林 大毅† 小林 裕太† 宮保 憲治† 小川 猛志†

Daisuke KOBAYASHI† Daiki KOBAYASHI† Yuta KOBAYASHI† Noriharu MIYAHO† Takeshi OGAWA†

† 東京電機大学情報環境学部情報環境学科

† School of Information Environment, Tokyo Denki University

1.はじめに

現状のインターネットには，DoS 攻撃や IP アドレスの成りすまし，名寄せ等のセキュリティ上の問題が多く存在する．筆者らは，それら問題の発生を根本的に防止することを目指し，端末が事前に ISP 網(以下，網)へ設定したセキュリティ条件に基づき，網が端末間のコネクションレス接続制御を行なう，次世代ネットワーキング方式を検討している[1]．本稿では本方式の応用として従来にないセキュアな端末間匿名 IP 通信サービスを提案する．

2.既存の端末間 IP 通信の問題点

既存網では第三者からのパケットを端末まで到達不可にする為，ファイアーウォール(FW)の設置が一般的であり，IP レイヤでの着信が阻害されている．しかし，FW のグローバルアドレスは通信相手に公開されるため，悪意ある第三者から DoS 攻撃をされる危険がある．さらにグローバルアドレスをキーに通信相手に分散する個人情報を名寄せされ，プライバシ侵害の危険もある．SIP や WebRTC 等，FW を通過し IP レイヤの直接通信を可能とする技術があるが，グローバルアドレスの公開が前提のため上記問題は解決されず，また通信毎に端末と網内のシグナリングサーバ間でコネクション設定処理が必要であり，短時間で完了する通信や，性能の低いマシン間の通信には適さない問題がある．

3.提案する端末間匿名 IP 通信サービス

上記問題を解決すべく，グローバルアドレスを使用せずに IP レイヤでの直接通信を可能とする，端末間匿名 IP 通信サービスを提案する．通信手順を図 1 により説明する．

まず，着端末は端末間での通信の前に，発信を許可したい端末に，自端末のグローバルな識別子を網の公開鍵で秘匿して通知する．次に発端末は当該識別子を網に転送する．そして，網は発端末と網間の接続認証結果を用いて発端末を特定，また発端末から転送された当該識別子を秘密鍵で復号し着端末を特定する．網は発着端末間の対応をとり，加入者データベース(DB)に通信を許可した端末のペアを登録する．さらに，両端末に通信相手を識別するローカルなアドレス(仮アドレス)を配布し，仮アドレスとグローバルアドレスの変換ルールを FW に設定する．両端末は通信相手のグローバルアドレスを知ること無く，以後当該仮アドレスを用いて，既存の VPN 内通信と同様に端末間の IP レイヤ直接通信が可能となる．

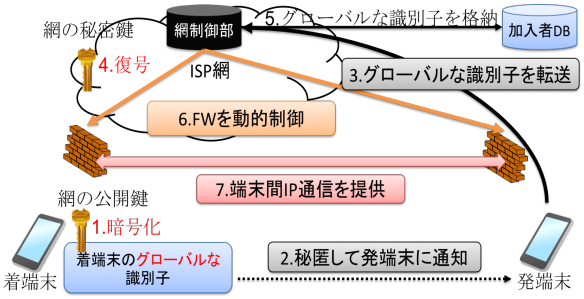

図1 提案サービス 端末間匿名 IP 通信確立手順

4.提案サービスの評価

提案サービスは，IP 通信を許可する端末のペアを網内 DB に登録する処理が必要な為，IP 通信が可能になるまでの遅延時間がユーザビリティに影響する可能性がある．その為，プロトタイプを実装し，WebRTC との接続遅延の相対評価を行った．なお，提案サービスは一旦通信許可を網に登録すれば，以後端末間でシグナリングが不要であるが，WebRTC は，通信毎にシグナリング処理が必要である．

提案サービスの DB をディスクベースとして測定したところ(図 2)，遅延時間が WebRTC に比べ 29ms 長い結果となった．提案サービスの遅延時間の内訳を分析すると，DB 処理時間が支配的であることが分かった．そこで，提案サービスの DB をインメモリに変更し，再評価を行った．その結果，DB 処理時間が 31.5ms 改善でき，WebRTC よりも遅延時間が 6ms 少なく，ユーザビリティの観点で問題がないことを確認した．

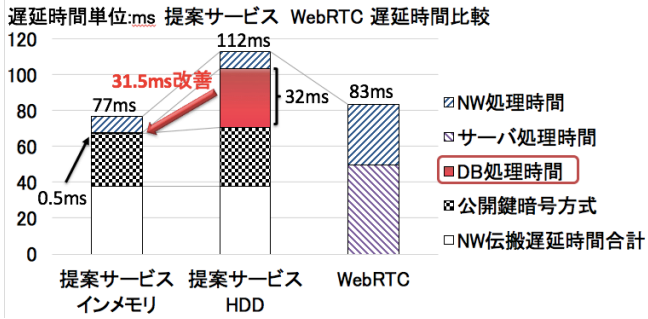

図 2 提案サービス WebRTC 接続遅延評価結果

5.今後の予定

今後学内ネットワークへの適用について検討を進める．

参考文献

[1] 小川猛志，他，次世代インターネットに向けた動的な匿名閉域通信方式の提案，IC2015，pp.85-92，神戸，2015.10.