講演番号： 80

セキュアなクライアント-サーバ間 IP 通信サービスの提案

B－16　A Proposal of Highly Secure IP communication Services for Clients and Servers

小林 大毅† 小林 大翼† 小林 裕太† 宮保 憲治† 小川 猛志†

Daiki KOBAYASHI† Daisuke 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クライアント-サーバ間 IP 通信サービスを提案する．

2. 既存のクライアント-サーバ間通信の問題点

既存網において，不特定多数のクライアントへサービスを提供する Web サーバは，クライアントが IP レイヤで接続後に，上位レイヤでクライアントの認証を行なう必要がある．このため，IP 又はトランスポートレイヤでの DoS 攻撃や認証前の上位レイヤ攻撃を防げない問題がある．

3. 提案方式

3.1 提案サービスの概要

上記問題を解決すべく，網が持つクライアントの認証結果や端末種別等の加入者情報を活用し，網がサーバに代行して，サーバが事前に設定したアクセス許可条件に合致するクライアントのみ IP 接続を可能とするアクセス制御を，網入口で実施する方法を提案する．これにより，信頼性の低いパケットは網入口側で破棄されるため，網内やサーバ側のリソースを消費せずに，悪意者からの攻撃を防ぐことが可能となる．また，年齢制限や端末の位置によるサーバ振り分けといった，高度サービスへの応用も可能となる．

3.2 実現手順

実現方法を図 1 に示す．前提として，ISP はクライアント A の本人認証済であり，Web サーバ A は DNS の TXT レコードを利用し，アクセス条件(例: ISP が認証済の Android クライアントのみアクセス可)を DNS へ登録しているものとする．

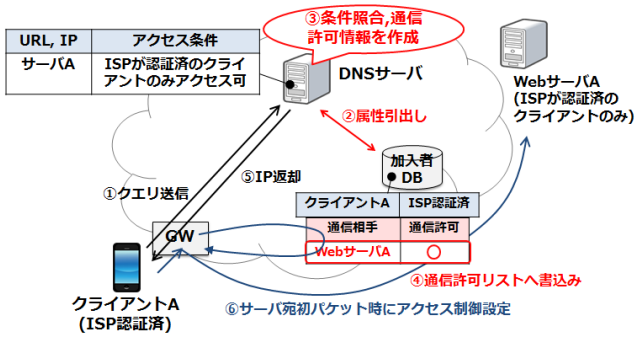

図 1 実現方法

クライアント A が Web サーバ A へアクセスを試みると，はじめに DNS への問い合わせが行なわれる．DNS では加入者データベース(以下，DB)からクライアント A の属性(ISP が認証済等)を引出し，Web サーバ A のアクセス条件と照合を行なう．そして，照合結果に基づいた通信許可情報を作成し，加入者 DB へ書込み，クライアント A へ IP アドレスを返却する．クライアント A から Web サーバ A への初パケットを契機に，加入者 DB の通信許可情報に基づいたアクセス制御設定を網入口のゲートウェイへ行なう．

3.3 実用化に向けた課題

本提案 DNS では，従来の DNS と比べ処理が多いため，クライアントから見た遅延時間も増大すると考えられる．従って，本提案 DNS を実運用した場合の遅延時間を見積もり，クライアントへの影響の有無の評価が必要である．

4. 提案 DNS における遅延時間の評価

4.1 評価方法

本提案 DNS を実運用した場合の遅延時間を，(1)現在実運用されている DNS の遅延時間に，(2)従来と本提案 DNS の遅延時間の差分を加えることで見積もり，評価を行なった．(1)については，Namebench を利用し，GoogleDNS の遅延時間を測定した．(2)については，従来と本提案 DNS のプロトタイプを作成し，差分を測定した．ここで，本提案では，加入者 DB をディスク DB とインメモリ DB の 2 パターンを実装した．理由は，処理速度が異なるからである．

4.2 測定結果と評価

GoogleDNS の遅延時間は 42.75ms であった．これを基に本提案の遅延時間を見積もったところ，加入者 DB がディスクの場合は約 2 倍の 85.23ms，メモリの場合は約 14%増の 48.67ms となった．よって，インメモリ DB を採用することでクライアントに影響のない遅延時間を実現できると分かった．

5 まとめ

本通信方式の応用サービスとして，悪意者からの攻撃を防止するセキュアなクライアント-サーバ間 IP 通信サービスを提案した．また，インメモリ DB の利用により，クライアントに影響なく本サービスを実現できることを確認した．しかし，インメモリ DB は電源ダウンを考慮するとデータの永続が困難であり，今後はこの課題の検討を行なう予定である．

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.