講演番号： 82

スケーラブルな次世代ネットワーク間接続方式の提案

B－16　A Proposal of Scalable Next Generation Internetwork Connection Method

小林 裕太† 小林 大毅† 小林 大翼† 宮保 憲治† 小川 猛志†
Yuta KOBAYASHI† Daiki KOBAYASHI† Daisuke KOBAYASHI† Noriharu MIYAHO† Takeshi OGAWA†
† 東京電機大学情報環境学部
† 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，本方式を応用したクライアント-サーバ間接続サービス[2]に着目し，同サービスの適応範囲を１つの ISP(Internet Service Provider)から異 ISP 間へ拡大する際に必要となる ISP 間の接続手段を提案する．

2. ISP 間接続の問題点

文献[2]では，発端末が属する網が，着端末(サーバ)に代行して，発端末からの発信を規制する通信サービスを提案している．異 ISP 間の通信に拡大するためには，発側 ISP の発信規制機能を着端末が信頼できる仕組みが必要である．仮に，発側 ISP と着端末間で直接信頼関係を構築すると，必要な信頼関係の数が膨大(インターネット上の全 ISP 数×サーバ数)となりスケーラビリティ上問題と考えている．

3.提案する ISP 間接続方式

3.1 信頼関係構築の考え方

着端末は，属する着側 ISP に発端末からの発信規制(アクセス制御)を委託し，着側 ISP は発側 ISP へ再度委託することで，必要な信頼関係を「ISP 数^2」まで削減．さらに ISP 間に SSO(Single Sign-On)を応用した仲介サーバを置き必要に応じて ISP 間で信頼関係を構築することで，事前に必要となる信頼関係を「ISP 数×仲介サーバ数」まで,通信中に必要な信頼関係を「通信中の ISP 数^2」まで削減させる．

3.2 SSO 応用の課題

SSO 技術では，Web サーバに対して，仲介者(IdP)が，クライアントの本人性認証と当該 Web サーバへの接続認可を代行することができる．ISP 間接続においては，発着 ISP 間で，双方向の認証と接続認可を実施できるように機能を拡張する必要がある．

また，SSO 技術ではサーバはクライアントと IP レイヤで接続後に，IdP と通信してクライアントの認証結果を確認するため，悪意端末からの DoS 攻撃や認証前の上位レイヤ攻撃を防ぐことが出来ない．ISP 間で信頼関係の構築が不可能になると当該 ISP に属する端末間の新規通信に影響するため IP レイヤのセキュリティを確保する必要がある．

3.3 提案する接続手順

図 1 に概要を示す．仲介サーバと各 ISP 制御部間は事前に信頼関係があって相互に通信可能であり，仲介サーバは各 ISP のアクセス制御能力(ISP が発信規制に利用可能な端末の属性の種類など)を把握している，とする．また ISP 間でのユーザデータの転送はインターネット上の MITM 攻撃を防ぐため VPN(IPsec トンネル)を使用することとし，仲介サーバは各 ISP 間の VPN 設定情報(トンネル終端部の IP アドレスや認証用共通鍵等)を保持している，とする．

ISPA は発端末からの DNS クエリで着端末が ISP B に属することを検出すると，仲介サーバに ISP B 間との仲介要求を送信．仲介サーバは ISP A, B 双方のアクセス制御能力と通信相手への要件を比較し，条件が合致すれば， 両 ISP に対向 ISP の VPN 設定情報を通知．両 ISP は対向 ISP からの受信パケットが GW(Gate Way)を通過できるように FireWall の穴あけを行い，ISP 間接続を確立し，発端末に DNS 検索結果を応答する．

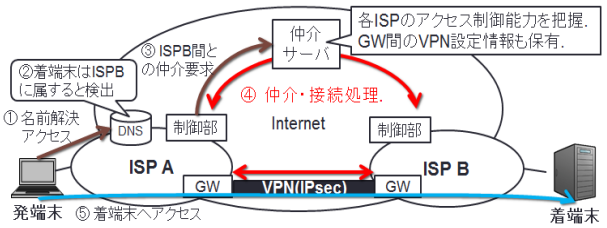

図 1 提案する接続手順の概要

4. DNS 応答遅延時間の評価

提案方式では信頼関係がない ISP に対する DNS クエリについては，応答が 3.3 節の処理分遅延する．OpenAM をもちいた既存の SSO 処理時間と VPN 設定時間を実験した結果から類推し，おおよそ 2.8 秒の遅延になることが分かった．既存インターネットの DNS 応答は数 10m 秒であるのでユーザビリティへの影響が考えられるが，WindowsPC 等の DNS タイムアウトは 10 秒のため実用範囲と考えられる．

5. 今後の予定

仲介手順の詳細化と応答遅延時間短縮化の検討を行う．

参照文献

[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.

[2] 小林大毅 他，"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，" 信学会東京支部学生会研究発表会，東京，2016.3 予定