大規模 VPN を実現するための P2P-VPN 技術の提案

A proposal for P2P-VPN technology supporting large scale VPN

松田 和浩†　　大崎 博之††

Kazuhiro MATSUDA　　Hiroyuki OHSAKI

†日本電信電話株式会社　NTT 情報流通プラットフォーム研究所

†NTT Information Sharing Platform Laboratories, NTT Corporation

††大阪大学大学院情報科学研究科

††Graduate School of Information Science and Technology, Osaka University

1. はじめに

我々は、文部科学省の産学官共同研究の効果的な推進プログラムにより「サイバーソサイエティを実現する仮想網技術」の研究に取り組んでいる。本研究では、ブロードバンドアクセス／モバイルアクセスが普及した社会において、「人」にとって利便性の高いサービスを享受できる環境や、多様な労働環境などを実現するために、様々な社会組織のネットワーク化を可能にする、高セキュアかつ高信頼なサイバーソサイエティ構築のための基盤技術の確立を目標としている[1]。

2.L2-VPN/L3-VPN、インターネット VPN

高セキュアなサイバーソサイエティの構築のためには、企業／教育機関／行政機関／同好などの非営利団体といったセキュリティポリシの異なる膨大な数の組織に対して、閉域性を確保する必要がある。

現在、プロバイダサービスとして L2-VPN(広域イーササービス)、L3-VPN(IP-VPN)が提供されている他、インターネットをインフラとするインターネット VPN(IPSec-VPN[2]、SSL-VPN)が用いられている。L2/L3-VPN はプロバイダ側が用意する大規模ルータを用いた企業向けサービスであり、多数の拠点の収容が可能である。CUG(クローズドユーザグループ)数は L2-VPN では VLAN タグ長の制約から 4,094CUG/NW に制限される。また、L3-VPN では方式的な制約はないが、拠点間にフルメッシュにパスを張る必要があるため数万程度と考えられる。一方、インターネット VPN ではノード性能の制約から拠点数は数十程度であるが、CUG 数についてはネットワーク的な制約がない。

3. 提案方式

本稿では多数の CUG を収容可能である IPSec-VPN をベースに CUG 数スケーラビリティを改善した P2P-VPN 方式を提案する。図 1 に P2P-VPN の構成を示す。各 CE(カスタマエッジ) は二つの IP トンネルを持ち、仮想的なリング網を構成する。例えば、CE#1 は隣接する CE#2 をゲートウェイとして全てのパケットを暗号化した後に転送する。CE#2 はパケットを復号し、自 CE 配下に転送先がない場合には次の CE#3 をゲートウェイとしてパケットを転送する。同様の手順でリング上の全 CE 間での通信が行われる。この構成により、各 CE は二つの IP トンネルのみで、全 CE 間の通信が可能になる。また、CE をアドホック的に追加する場合の網への影響を局所化できる。

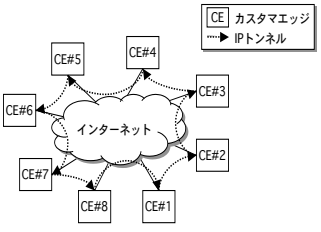

図 1 P2P-VPNの基本構成

4. カットスルー機能

仮想的なリング網では隣接 CE が必ずしも地理的に隣接しているとは限らない。また、CE に処理性能の低いものが混在する場合、網全体の転送性能を律速する。この帯域の問題を解決するために、P2P-VPN ではカットスルー機能を持つ。図 2 はカットスルー通信の契機にポート番号を使用する例であり、特定のポート番号を用いた通信については、仮想リング網を介さずに CE 間での直接通信を行う。通信のセキュリティは SSL[3]等により確保する。

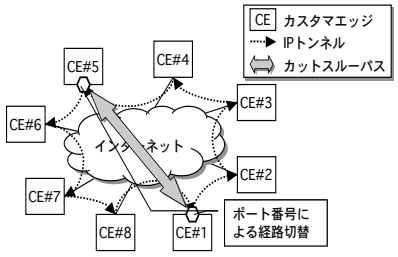

図2 カットスルー通信による帯域の確保

5. 自律的切替機能

インターネットおよび個人設備を前提とするため障害／人為的な遮断があっても通信が維持される必要がある。P2P-VPN ではトポロジ観測を行いゲートウェイが応答しない場合にゲートウェイを自律的に切り替えることで通信を維持する。

6. むすび

今後、Linux 等による実装を行い基本動作の確認を行う。

参考文献

[1]http://61.193.204.197/html/20224A00018.htm

[2]S.Kent et al., "Security Architecture for the Internet Protocol," Request for Comments(RFC) 2401, Nov. 1998

[3]T. Dierks et al., "The TLS Protocol Version 1.0," Request for Comments (RFC) 2246, Jan. 1999.