ラベルスイッチング技術を用いたネットワークにおけるファイヤウォールの実現

宇多 仁

北陸先端科学技術大学院大学 情報科学研究科

平成 11 年 2 月 15 日

キーワード： インターネット, ラベルスイッチング, ファイヤウォール, セキュリティー, パケットフィルタリング.

インターネットは、多くのルータの相互接続により構成されている。ルータは第 3 層 (ネットワーク層) におけるパケット転送を行うため、転送を行うパケット毎に経路探索等の複雑な処理を行わなければならない。インターネット利用者は急激に増加しており、広帯域・低遅延を要求するアプリケーションも増えつつある。このような状況から、ルータで大容量のデータを高速に処理することが求められている。この問題の一つの解決方法として、ラベルスイッチング技術を用いた方法が提案されている。

ラベルスイッチング・ネットワーク内を流れるパケットには「ラベル」が付けられる。ラベルは、第 2 層 (データリンク層) の識別子に対応している。ラベルスイッチルータ (LSR) では、ラベルの付いたパケットが第 3 層の介在なしに第 2 層スイッチにより転送される。この状態をカット・スルー状態と呼び、第 3 層の介在がないため大容量のデータの高速な処理が可能である。

一方、インターネットの拡大に応じて、利用者の情報や資源を外部から守ることが大きな課題となっている。この解決方法として、ファイヤウォールを構築するという手法が広く用いられている。ファイヤウォールの構築においては、ルータで提供されるパケット・フィルタリング機能が重要な位置を占める。パケット・フィルタリング機能を提供するルータでは、各パケット毎に第 3 層以上の情報の取得、評価、評価結果に応じた転送の制御を行わなくてはならない。

広帯域・低遅延を実現するラベルスイッチング・ネットワークにおいても、ファイヤウォールを構築する技術が必要とされている。しかし、ラベルスイッチング・ネットワーク上ではパケットが第 2 層で転送されるという特性により、パケット・フィルタリング機能に必要とされる第 3 層以上の情報の取得や転送の制御が困難である。

そこで本論文では、ラベルスイッチング・ネットワークの長所を生かしつつ、ファイヤウォールを実現する手法として、以下に挙げる 2 方式を提案する。

- **擬似的なカット・スルーを用いる方式**

  パケット・フィルタリング機能を提供する LSR に、第 2 層で動作するパケット転送モジュール (PFM) を組み込む。PFM は、入力データグラムに対しフィルタリング・ルールを適用し、この結果転送が許可されればデータグラムを出力する。

  LSR はカット・スルー経路の生成時に、通常のカット・スルー経路を生成するかわりに PFM へ迂回する「擬似カットスルー経路」を生成する。これにより、カット・スルー状態にある全てのデータグラムは PFM を介して転送されることとなる。本方式は、パケットフィルタリング処理を行う LSR のみの変更で実現が可能である。第 3 層でのパケット転送処理では、フィルタリング処理には本来必要としない経路探索等の処理も行う必要がある。しかし、PFM では第 2 層での転送を行うため、これらの処理を短絡した高速な転送処理が可能である。

- **フィルタリング処理をカット・スルー経路の端点となる LSR へ委託する方式**

  ラベルスイッチング・ネットワークにおいて、カット・スルー状態でもカット・スルー経路の端点においては第 3 層でのパケット転送が行われる。本方式は、フィルタリング処理をカット・スルー経路の端点に委託するものである。

  委託に成功した経路については、通常のカットスルーが可能となる。カット・スルー経路内では、パケットの再構成や評価を一切行わないデータグラム転送が可能である。これは、ラベルスイッチング・ネットワークにおける理想状態である。

カットスルー経路の端点となる LSR へフィルタリング処理を委託し、パケット・フィルタリング機能を実現する方式は、完全なカット・スルーが可能である。これは、最も理想的な方式である。しかし、この方式のみでの実現は、多くの LSR をこの方式に対応させ、その全てについて適切な管理に基づくセキュリティー・レベルの維持が必要であるために困難な場合が多い。

そのため、PFM 方式と処理委託方式を組み合わせフィルタリング機能を実現する方法が現実的である。PFM 方式と処理委託方式を組み合わせる事により、ラベルスイッチング・ネットワークの特徴を最大限に生かした、パケット・フィルタリング、延いてはファイヤウォールの構築が実現できる。

また、パケット・フィルタリング以外にも、LSR 上でパケットの情報を用いて処理を行う機能として、NAT 機能やラベルの付け替え機能が挙げられる。本論文で提案した手法は、これらの処理への応用が容易に行える。

本研究では、ラベルスイッチング・ネットワークを用いる事を前提とした。今後の課題は、この制限を緩め、本研究での提案をもとに、ネットワーク一般における分散型ファイヤウォール構築手法への拡張等を検討することである。