

MPLSネットワーク・アーキテクチャー作成における 構成パターンの適用

陳 建和

Pattern Determination for Architecting an MPLS-Based Network

Kenwa Chin

本論文では、実際に企業において導入されたMPLS(Multi-Protocol Label Switching)ネットワークのアーキテクチャー策定経験から得たMPLS適用手法を提案する。この手法は、3つの基本パターンを定義しMPLSを用いた企業ネットワーク構成を鳥瞰する。さらに、お客様の要件を分析した上で、MPLSの導入の可否および適した構成パターンの判断基準を提示する。この手法の狙いは、ますます複雑になり、セキュリティ、パフォーマンスおよび運用管理などの課題を抱える企業ネットワークを、MPLS技術によって解決することである。さらにこのMPLSネットワーク・アーキテクチャーは、基本パターンに含まれたMPLS機能を強化することで将来のグローバル・ネットワーク・バーチャリゼーションの実現も可能であることを示す。

This paper proposes a new design approach for architecting enterprise networks utilizing Multi-Protocol Label Switching (MPLS) technology. Three basic patterns for MPLS-based enterprise network configurations are defined. After analyzing customer requirements on the basis of various decision criteria, whether or not to utilize MPLS and which pattern to be used will be determined. The benefit of this approach is not only its facilitation of solutions for such issues as security, performance and the management of enterprise network environments which are becoming more complicated, but it also provides a way of enhancing the functions of the introduced patterns for the realization of global network virtualization.

Key Words & Phrases : MPLS ,MPLS-VPN ,モビリティ ,グローバル・ネットワーク・バーチャリゼーション
MPLS, MPLS-VPN, mobility, global network virtualization

1 .はじめに

企業の統廃合、中核業務の選択と集中による非主要業務の外部委託などの企業経営変革がネットワーク・インフラストラクチャーに次のような変化をもたらしてきた。

- (1) 一極集中型から、多極分散型あるいは水平分散型に変化したネットワーク構成が増えている[1]。
- (2) 同じ企業の中でも部門別に他の企業との提携が進み、キャンパス・ネットワーク内でのネットワーク・ゾーニングのニーズが高まりつつある[2]。
- (3) オン・デマンド・ビジネスの発展でデータグリッドなどの仮想技術を利用し各地に散在しているリソースを業務ごとに集約利用できるネットワーク技術が必要とされ始めた。

これらの変化に追随するために、VPN(Virtual Private Network - 仮想自営網)が一層着目されている。特に大規模なネットワークでは、最近MPLS(Multi-Protocol Label Switching)技術によるVPN(MPLS-VPN)が、セキュリティ、パフォーマンスおよび運用管理の容易さの観点で注目されている。しかし、業務形態、コストや移行を考慮した場合、MPLSを使ったネットワークの導入は容易ではない。時にはMPLSが適するとも限らない。

本論文では、著者の経験に基づき、企業のネットワーク要件に合わせてMPLS技術の特徴を活かしたアーキテクチャーのパターン化を図り、各パターンを適用する際の判断基準を述べる。

さらに、MPLSのラベル・スイッチング技術の発展にしたがって、これらのアーキテクチャー・パターンの拡張として、LAN/WANをまたがるグローバル・ネットワーク・バーチャリゼーションを実現するネットワー

提出日：2005年8月31日 再提出日：2006年7月4日

ク・インフラストラクチャーの可能性を論じる。

2 . MPLSを使ったVPNの特徴

MPLSは多くのキャリアのサービス・ネットワークとして実績のある、ラベル・スイッチングによるIPネットワーク全体の高速化技術である[3]。また、RFC2547bis (Request for Comment - TCP/IPの技術標準)によるMPLS-VPNのための拡張機能でVPNの情報をラベルに変換することができるようになり、一つのIPネットワークに複数の企業イントラネットを共存させるIP-VPNサービスが可能となった[4][5]。

最近のネットワーク設計手法では、企業ネットワークにおける論理分割の要件に対応するため、VLAN (Virtual LAN - 仮想 LAN)とファイアウォールを組み合わせるだけでなく、VPN技術も取り入れることが普通になっている。さらにWAN回線で多数の拠点を接続する場合、WANの部分まで含めてVPNの構成を考える場合も多くなってきている。このようなWANのVPN構成をする場合の選択肢はいくつかある。

インターネット接続回線と自営のVPN装置で構成されたインターネットVPNという安価でセンター集中型ネットワークに適したパターンがある。一方、より高いセキュリティと信頼性が保たれた、キャリアが提供する閉域網回線サービスであるIP-VPNや広域イーサネットを使い、センター集中型と分散型ネットワークの両方に適するようにしたネットワークのパターンもある。

どの組み合わせにおいても、ネットワークの規模が大きくなるにつれ、管理、パフォーマンス、コストの面から限界に達することが多く見受けられる。これを解決する方法として、LANとWANの両方を自営のMPLSネットワークとして構築することを一つの選択肢として考える企業が増えてきた。このMPLS技術を使ったVPNが論理分割を要件とする企業ネットワークに適している点を次に述べる。

- (1) レイヤー2のVLAN情報、レイヤー3のIPネットワーク情報に加えて、TOS(Type of Service)情報などを反映したラベル値を使い、優先制御を含むフローディング処理の最適化、高速化が可能である。様々な企業ネットワークのLAN/WAN環境に柔軟な対応が可能になる。
- (2) MPLS-VPNによって暗号化を使わずにセキュリティの確保が可能となり、コスト削減にも寄与する。(ATMやフレーム・リレーなどのVirtual Circuitと同等のレベルのセキュリティをIPネットワークで実現できる)
- (3) VPNが異なれば同じIPアドレス体系も使えるためサービス性、運用性が良い。

- (4) VPNを実現するにはルータやスイッチ以外にはVPN装置などの特別な装置は不要である。

しかしながら、MPLSの導入に当たっては、MPLSが可能でかつ高性能なネットワーク機器が必要であり、一時費用がかかる。また、VPN設計を行うための高度なスキルが求められる。さらに、運用管理が普通のIPネットワークより複雑になることなどの課題もある。これらの課題を抱えながらもMPLSを導入する価値があるか否かを検討するためには、MPLSが適したネットワークのパターン化が必須であると考えられる。

ここで、本論文にあらわれるMPLS-VPNの構成要素について説明する[6]。

- (1) CE(Customer Edge)ルータ: 各ユーザー側VPNに置かれるVPNルータ
- (2) PE(Provider Edge)ルータ: MPLSネットワーク側に置かれ、CEルータの対向となるルータ。ユーザーごとに異なるルーティング・テーブルを持ち、ユーザー側から来た経路情報を同じVPNのユーザーグループ内で交換することで、共通のMPLS網でユーザーごとのVPNを実現する。
- (3) P(Provider)ルータ: MPLSバックボーンを構成し、ラベル・スイッチングのみ行う

3 . MPLSを適用するためのネットワーク・パターン

著者のMPLSを使った企業ネットワークの設計の複数の経験に基づいて、MPLSを適用するネットワークのパターンを整理する。この整理に当たって、通信要件、セキュリティ、パフォーマンスといった通常の視点だけではなく、企業の業務形態、運用管理なども重視することが特徴である。このことから、パターン化の視点を次のように置いた。

- (1) 拠点と、その業務機能を接続するバックボーン・ネットワーク
- (2) ネットワークおよび業務形態も含めたセキュリティを考慮するVPN構成
- (3) ユーザーと、業務のためにアクセスするリソースとの関係

これに基づく整理の結果、ネットワーク・パターンを、複数のVPNがリソースをどのようにアクセスするかによって、次の三つに分類する。

3.1 パターン1: 複数VPNが別々のリソースにアクセスする構成

複数VPNが共通バックボーン(図1のMPLSコア)を介して、事業群で別々に運用するデータセンターのり

ソースにアクセスする構成であり、次のような特徴をもつ。

- (1) バックボーンを構成する各拠点の扱いは平等であり、構成を柔軟に考えることを容易にする。例えば、図1に示した本社、データセンター1、データセンター2はバックボーン拠点として同等であり、対等にメッシュ構成を組んでいる。
- (2) バックボーン拠点間のリンク形態はフル・メッシュ型であれば最適だが、リング型の構成も取り得る。
- (3) 事業群ごとに拠点が各地に散在している場合にこれらを事業群単位に論理ネットワークとして構成できる。

図1にこのパターンの標準的ネットワーク構成の例を示す。

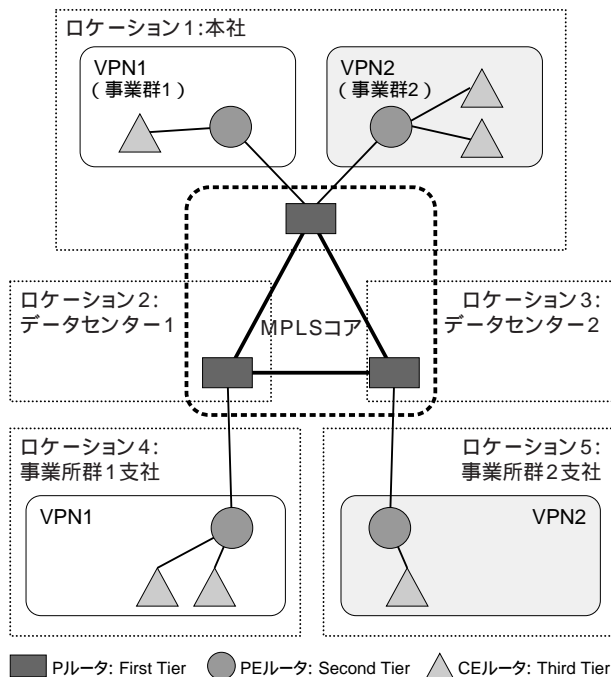


図1. パターン1のネットワーク構成例

このパターンの適用に当たった得失などについての分析結果は次のようになる。

長所:

- (1) MPLS-VPN技術を利用して、各地の拠点に分散している事業群に属するユーザーグループをそれぞれのVPNに収容し、互いに異なるセキュリティ・ドメインとなるように保持できる。
- (2) MPLS技術により、拠点間のデータ・フローが常に最適な経路となるように選ぶことができ、パフォーマンスを確保することができる。
- (3) バックボーン拠点以下にSecond Tier(第2階層)拠点、Third Tier(第3階層)拠点を広げていくといった放射状ネットワークであり、柔軟性と拡張性を保

つことができる。

- (4) バックボーン拠点に置かれるネットワーク機器はラベル・スイッチングのみ行うルータ演算、QoSのためのトラフィックシェーピング、転送レート制限(Rate Limiting)などはSecond Tier以下の機器で行われるため、バックボーン内の処理遅延時間が短くなる。
- (5) 将来技術が進んで、機器やインターフェースの高性能化が行われてもアーキテクチャーを変更する必要がない。

短所・制約:

- (1) ネットワークが論理的に完全分離されているので、保守や運用管理としてVPNが別であることを考慮して行う必要がある。
- (2) バックボーンの拡張や設定変更をする場合にはネットワーク全体への影響は避けられない。
- (3) バックボーンのパターン、構築、運営は事業群が共同で行い、かつそのための利害関係の調整が必要である。関係者がすべて満足することは少ない。
- (4) バックボーンの使用に対する事業群別の課金などが必要な場合は、別途考慮する必要がある。

3.2 パターン2: 複数VPNが共有リソースにもアクセスする構成

複数VPNが共通のバックボーンを介して共有リソースにもアクセスする構成であり、共通のバックボーンを使用する点はパターン1と同じである。異なる点は、ユーザーグループごとのVPNからグループ共通に使用するリソースへのアクセスを追加していることである。図2にこのパターンの標準的ネットワーク構成の例を示す。この図中の全社共通リソース(CR)は独立し

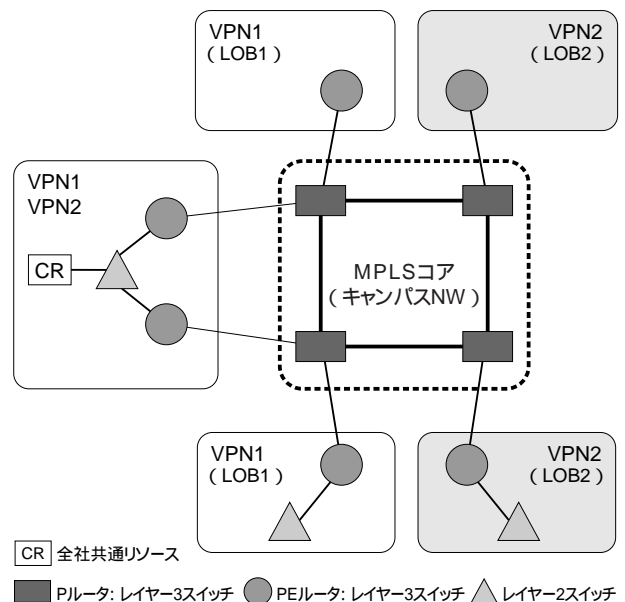


図2. パターン2のネットワーク構成例

た要素として表現してあり、かつ共通に使用されることによる可用性からネットワーク経路冗長化も明示した。このパターン2については次のような特徴がある。

- (1) キャンパス(建屋が複数存在する敷地内)に複数の事業群の拠点が置かれている。これを事業群単位に論理ネットワークとして構成できる。
- (2) ネットワークがキャンパス・スイッチによって構成され、すべてのスイッチ機器をMPLS技術を使って物理的に接続することで対等構成のネットワーク構成となっていて、ビジネス・IT要件を満たすゾーニングに柔軟な対応ができる。
- (3) 図2に示すように各事業群が共通でアクセスするリソースをキャンパス内に配置することができる。共通のリソースの例としては、メールサーバーやグループウェア、インターネットへの接続などが挙げられる。

パターン2の適用に当たっての得失についての分析結果は次のようになる。

長所:

- (1) MPLS-VPN技術を利用して、ネットワーク機器において論理的なVPNを構成することにより、事業群や生産ラインの設立、消去、変更が頻繁に行われるとユーザー要件を満たすことができる。
- (2) MPLS-VPNの論理設定のみでゾーニングが可能であり、ファイアウォールによる煩雑なACL(アクセス制御リスト)などに比べて安価でかつ柔軟にキャンパス・ネットワーク構築することができる。
- (3) 異なるVPNではIPアドレス体系の重複が許されるため、全く同じネットワーク設計を異なる事業群で使用することができる。

短所・制約:

- (1) 共通のリソースにすべての事業群からのユーザーアクセスが集中するため、ネットワーク上のボトルネックになりやすい。
- (2) 部門間のVPNが異なるため、事業群の設立、消去、などに伴う組織変更や異動が多いと、ユーザーモビリティのサポートが煩雑になる。
- (3) MPLSネットワークを構成するネットワーク機器は従来のLANスイッチよりコストが高い。キャンパス・ネットワークのように比較的狭い面積内にネットワーク機器が密度高く配置されていると、コスト面の制約が発生する。
- (4) MPLS-VPNの設計、構築には高いネットワークスキルが求められる。キャンパス・ネットワークの構築としてはやや高いと判断される場合がある。

3.3 パターン3: 複数VPNでアクセスするリソースが多対多の関係にある構成

このパターンは拠点間ネットワークであるパターン1と、キャンパス・ネットワークであるパターン2のネットワークを組み合わせで発展させた、ハイブリッド・ネットワークである。このパターンの標準的ネットワーク構成の例を図3に示す。

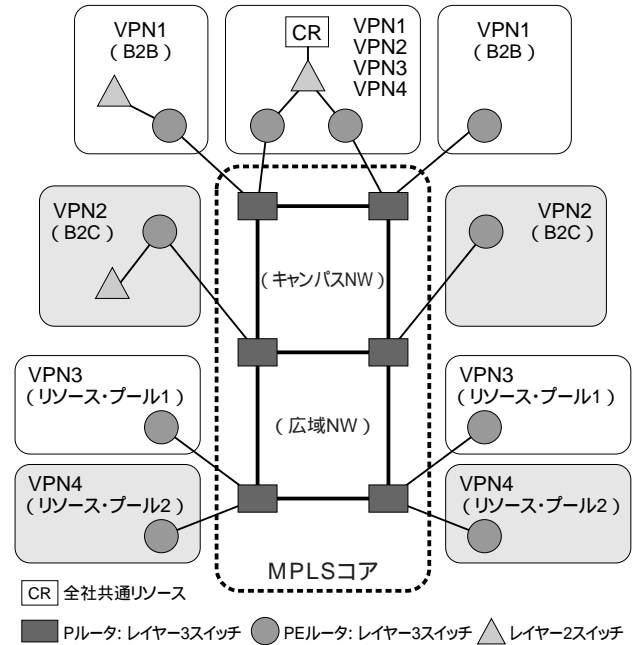


図3. パターン3のネットワーク構成例

このパターン3には次のような特徴がある。

- (1) 図3に示したネットワークのバックエンドには様々なリソースが存在する。これらのリソースは複数のプラットフォーム上で構築されたDBやサーバーであり、仮想化されたリソースとしてサービス要求者に提供されるものである。
- (2) フロントエンドのネットワークから様々なサービス要求が発生する。社内ユーザーが直接アクセスする場合や、インターネットから一般消費者が認証ゲートウェイを通してアクセスして来るケースなども含まれる。

このパターン3は実例として実証されたものではないが、位置付けは、パターン1とパターン2の特徴を集約して生かすことを目標としたLAN/WANハイブリッド型ネットワーク構成である。パターン3の適用に当たっての得失を次のように分析する。

長所:

- (1) パターン1で提示した各バックエンドセンター(事業群)をMPLS-VPNネットワークで接続した形態により、業務別に異なる論理ネットワークとセキュリティレベルを保つことができる。
- (2) パターン2で提供されているキャンパス内MPLS-VPNネットワーク構成を使い、データセンター内の

サーバーファームと各種のアクセスゲートウェイを異なるVPNの設定で分離した構成とし、仮想化したリソースと対応させた組み合わせが可能となる。

- (3) リソースとアクセスの多対多の関係を実現でき、複数の事業部門でネットワークの独立と共用を行うだけでなく、自社のシステムとITインフラストラクチャーを他社に提供するASP(Application Service Provider)のサービスも提供可能となる。

短所・制約:

- (1) LAN/WANをまたがる構成であり、設計上の考慮点が必然的に増える。
- (2) ASPのインフラストラクチャーとして使用した場合、一台の機器が複数の企業ネットワークを構成するケースが多くなる。セキュリティや管理上の課題が必然的に増える。
- (3) パターン3はキャンパスと広域の両方にまたがる点を特徴とし、柔軟なネットワークとリソースの配置を主眼にしている。これを実現するためにはIPプリフィクスおよびVLANを同じMPLSネットワークに格納することが理想であるが標準となるRFCはまだそのレベルにまで達していない。ネットワーク設計を工夫してIPサブネットとVLANのひも付けまで実施すれば異なるMPLSドメインの融合が可能となるが、独自の手法は管理性と拡張性の観点ではお勧めできない。パターン1あるいはパターン2からパターン3への拡張が現時点では現実的な設計・構築方法である。

4. アーキテクチャー策定における基本パターンの判断基準

前章において、既にそれぞれのパターンのメリット、デメリット、制約などについて述べた。この章では総合的な視点でネットワーク・アーキテクチャーの策定のためのパターン選択基準を論ずる。具体的には、お客様のネットワーク構想に対して、MPLSを適用することが有効か、また有効であるとして三つのパターンのどれを適用するのがよいかという見方で判断の基準を述べる。

4.1 アプリケーション・フロー

- (1) パターン1が適切な場合：拠点間のデータ通信が頻繁に行われるAny-to-Any構成である。
- (2) パターン1とパターン2が共通して適切な場合：別ネットワークに置かれている各部門間の通信はなく、セキュリティを考慮したゾーニングが必要となる構成である。
- (3) パターン3が適切な場合：ビジネス・ロジックやビジネス・データなどのリソースが異なる拠点に散

在していて、サーバー間のデータ通信が頻繁に行われる分散環境である。

- (4) MPLSが有効でない場合：一極集中型、すなわちデータセンターが一つでありアクセスが集中する場合。

4.2 ネットワーク・トポロジー

- (1) パターン1の適用構成：バックボーン・ネットワークを中心において、放射状に第2階層/第3階層以下を拠点から構成し通信リンク数を減らすトポロジーとしたい場合。また、バックボーン拠点間のリンクがIPリンクのようなベストエフォート型の場合、MPLSの適用でコスト・パフォーマンスの改善が図れる〔7〕
- (2) パターン2の適用構成：コア、ディストリビューション、アクセスに分かれたマルチレイヤー型スイッチのキャンパス・ネットワーク構成において、ディストリビューション層以下のスイッチを共用しながらセキュリティ・ゾーニングを形成するトポロジーを実現したい場合。
- (3) パターン3の適用構成：アプリケーション・ノードの配置を構成の主眼とし、それにトポロジーを合わせる必要がある場合。
- (4) MPLSが有効でない場合：アプリケーション・サーバーの配置が一箇所に集中されている場合。

4.3 セキュリティ

- (1) パターン1の適用構成：共通の物理ネットワークを使用しながら、事業群ごとに別々の論理ネットワークを作りたい場合。
- (2) パターン2の適用構成：ファイアウォールを使用する構成との違いを比較する必要がある。ゾーン間の通信制限を細かく設定する必要がある場合、ファイアウォールの適用が妥当であるが、ゾーン間の論理分割で済む場合はMPLS-VPNの適用がより柔軟かつ簡単なゾーニングを提供できる。
- (3) パターン3の適用構成：アプリケーションごとのアクセス制限をネットワークにおいても一貫して行う必要がある場合。
- (4) MPLSが不向きの場合：部門間や業務間ゾーニングの要件に加えて、ゾーン間のデータ・アクセスが頻繁に行われてセキュリティの制限が細かく要求される場合。

4.4 コスト

MPLSを適用するためにネットワーク機器の機能グレードアップが必要となることがある。機種選定の判断基準として一台のPEルータが処理できる仮想ルータの論理数とそれぞれのVPN内の経路数を確保で

きる所要メモリーが最もコストに影響する（メーカー製品によって多少異なるが256MB以上が必要であることが多い）

- (1) パターン1適用構成：PEルータとして使える現行ネットワーク機器がどれくらいあるかがMPLSに移行するか否かの判断基準となる。
- (2) パターン2とパターン3に共通する適用構成：IP電話とデータ端末が同じスイッチに接続されている、VLANベースのMPLS-VPNを柔軟に運用管理できるようにするのであればアクセス、スイッチまでMPLSをサポートする必要がある。バックボーンスイッチのみ新規導入で、PEレイヤー以下のスイッチ構成に既存の機器をいかに活用できるかがコストの判断基準となる。

5. 企業MPLSネットワークの将来発展について

MPLS技術を使ったネットワークは、本論文で述べた三つの適用パターンから、さらに発展させた形態が考えられる。また、その発展形態の一つは、MPLSの技術標準の成熟を前提として、より汎用的なネットワーク構成になる。この章ではこれらの将来形態について述べ、今後の発展の示唆としたい。

5.1 それぞれのパターンの応用について

- (1) パターン1ではWANの構築にMPLS技術を自営として適用したが、ISP間接続で使われているMPLS-IX(Internet Exchange)のような仮想経路(バーチャル・トランク、キャリアサービスの一種)を取り入れることで、グローバル企業のバックボーンにまで発展することも考えられる[8]。
- (2) パターン2は製造業のキャンパス・ネットワークから抽出したものであるが、ファイアウォールと組み合わせることにより、従来よりコスト・パフォーマンスの高い、データ・センター・ネットワークのリファレンス構成に発展させることができる。
- (3) パターン3は今の技術でも実現可能であるが、将来より幅広く発展させるため、キャンパスMPLSとWAN-MPLSの組み合わせのための標準化を前提とする。その内容としてはVLANのタグ、IP経路のプレフィックス、TOS、MPLS-VPNタグなどの識別子がラベルとして取り入れ、異質なネットワーク情報の交換が可能な機能が望まれる。これによってサーバーなどのリソースも含めたグローバル・ネットワーク・バーチャリゼーションを実現することができる。これは既にあるDNSなどの技術を使ったリソースのグローバル・バランシングに含まれた仮想化とは異なり、この発展パターンは本論文で論じたネットワーク・アーキテクチャーの将来像である。

この将来像においては、ネットワークとサーバーが一層融合した形態を実現できることになると著者は期待する[9][10]。

5.2 グローバル・ネットワーク・バーチャリゼーションの実現へ

バーチャリゼーション技術は今までサーバーやストレージが中心だったが、ネットワーク機器の技術の革新とMPLSの導入でネットワークも対象に加わり、ITインフラストラクチャーのバーチャリゼーションの範囲と効果を拡大することが期待される。本論文で述べた、MPLS-VPNによる複数の論理ネットワークを物理的なネットワークにオーバーレイする形態はネットワークの仮想化技術である。これをサーバーやストレージの仮想化とより融合させたものとするれば、グローバル・ネットワーク・バーチャリゼーションの一つの実現形態となると考える。

著者はこのようなグローバル・ネットワーク・バーチャリゼーションとして、現時点では次の二つのパターンを捕らえている。

- (1) パターンA：キャンパス・ネットワーク上の複数のスイッチやファイアウォールが一つの機器に集約され仮想化される。このパターンにおいては冗長化を考慮し、スイッチ二台をトランク接続¹でペア構成を組み、可用性を備えたバーチャリゼーションを行うのが普通である
- (2) パターンB：サーバーのようリソースがプール化され、サービス要求ごとに割り振りが行われる。サーバーが異なる場所にあっても、MPLS-VPNの導入でサーバー接続セグメントが同じVLANに属すれば同一サーバープールとして扱うことができる。これを実現するため、互いに離れた拠点にまたがるスイッチ間のトランク接続をMPLSネットワークの介在で実現すると広域でのネットワーク資源の仮想化が可能となる。これは前節で述べた標準化が実現し、レイヤー2/レイヤー3ネットワークの情報などをネットワーク全域に伝播^{でんぱ}することができれば実現可能だと思われる。

パターンAはネットワーク構成のMPLS化は範囲に含まれておらず、スイッチの単体で仮想化を実現することができる。これは既にも実現されたものであり、IBMのネットワーク仮想化ソリューションとなっている。

パターンBが今回提示した、MPLSネットワークが将来のシステム資源の分散化と仮想化のサポート役となるグローバル・ネットワーク・バーチャリゼーション

1 トランク接続：機器間を物理的に複数の通信経路で接続し、論理的には一つの太くかつ可用性のある通信経路とする接続形態

である。仮想化されたリソースの一部としてネットワーク資源を異なるロケーションへの広げることが実現される。すなわちグローバル・ネットワーク・バーチャリゼーションの実現である。今までのDNSを使ったグローバル・ロードバランスやURLリダイレクションなどによるリソースの分散化と比較した場合、より多くのネットワーク要件に対応することが可能となる。また、MPLSを使ったネットワークリソースのProvisioningについてもツールで管理するようにすることができる。

将来IPv6やMPLSのIXサービスを取り入れたネットワークの多様化は既に予想されており、MPLSの上でバーチャリゼーションをさらに発展させる可能性が充分にあると考えるが、別の機会に論じたいと思う。

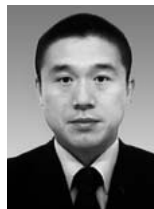
6. おわりに

高速でありながらセキュリティとアーキテクチャーの柔軟性を重視するネットワークに適したMPLS技術は、キャリアのサービス・ネットワークにおいて実証され、企業ネットワークにも浸透し始めた。コストと移行の制約から、すべての企業ネットワークに適用することは当面は難しい面もある。しかしながら、本論文で述べたように、パターンと判断基準の組み合わせを使って、これから頻繁に業務と組織の変革が行われる企業に適したネットワークをMPLS技術で構築できると考える。

また、サーバーやストレージのバーチャリゼーション技術が林立している現在、ネットワークのバーチャリゼーションもMPLS技術を導入することによりローカルからグローバルのバーチャリゼーションへと広げていき、一層成熟したものとするよう実現に努力したい。

参考文献

- [1] 北澤 治郎：“ITインフラのパラダイムシフトとは、” ProVISION, No.47, pp.38-42 (2005)
- [2] 佐藤 修二：“セキュア地域イントラネットデザイン、” ProVISION No.42, pp.73-74 (2004)
- [3] B.Davis and Y.Rekhter, トップスタジオ訳, 池尻 雄一 監修：MPLS入門, 翔泳社, ISBN4-7981-0139-7 (2002)
- [4] J. Guichard and I. Pepelnjak: *MPLS and VPN Architectures*, Cisco Press, ISBN1-58705-002-1 (2000)
- [5] S. Halabi and D. McPherso: *Internet Routing Architectures 2nd Edition*, Cisco Press, ISBN1-57870-233-X (2000)
- [6] 特集：MPLS技術とその最新動向を知る, ”アットマーク・アイティ, <http://www.atmarkit.co.jp/fnetwork/tokusyuu/11mpls/mp101.html> (2002)
- [7] A.A. Shaikh: *Efficient Dynamic Routing in Wide-Area Networks*, University Michigan (1999)
- [8] 中川 郁夫：“MPLSを用いた広域分散IXの技術とインパクト、”日本学術振興会産学協力研究委員会発表資料 (2004)
- [9] A. Acharya, A. Shaikh, R. Tewari, and D. Verma: “Scalable Web Request Routing with MPLS,” *IBM Research Report RC 22275* (2001)
- [10] R. Chadha, Y.-H. Cheng, T. Cheng, S. Gadgil, A. Hafid, K. Kim, G. Levin, N. Natarajan, K. Parmeswaran, A. Poylisher, and J. Unger: “PECAN: Policy-Enabled Configuration Across Networks,” *Proc. IEEE Policy* (2003)



日本アイ・ビー・エム株式会社
ネットワーク&インフラ・サービス事業部
テクニカル・サポート
ICP-アドバイザーITアーキテクト

陳 建和 Kenwa Chin

[プロフィール]

1993年、日本IBM入社。1994年から数多くの大規模ネットワーク構築プロジェクトを経験。その後、グローバル・プロジェクトの支援活動としてネットワークの提案、企画、コンサルティングなどにも従事する。現在、ネットワークを中心としたインフラストラクチャー構築の複数プロジェクトにおいてITアーキテクトとして活動している。
kchin@jp.ibm.com