

# 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



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。

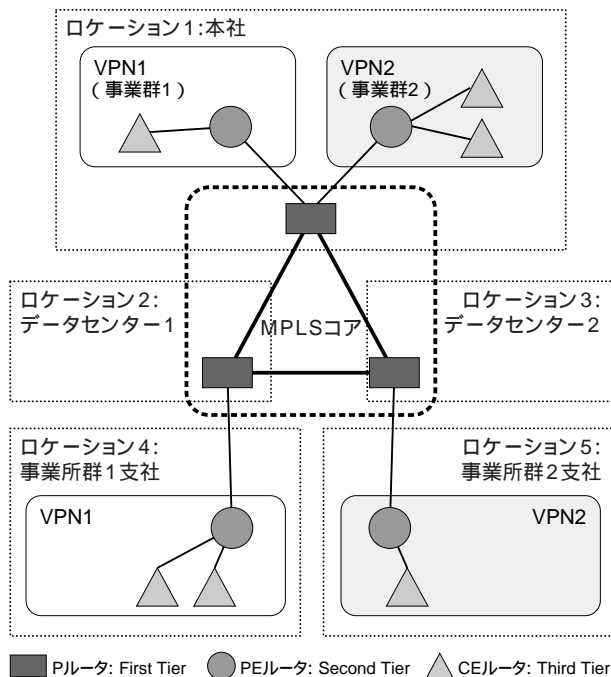


図1. パターン1のネットワーク構成例

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ティング演算、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

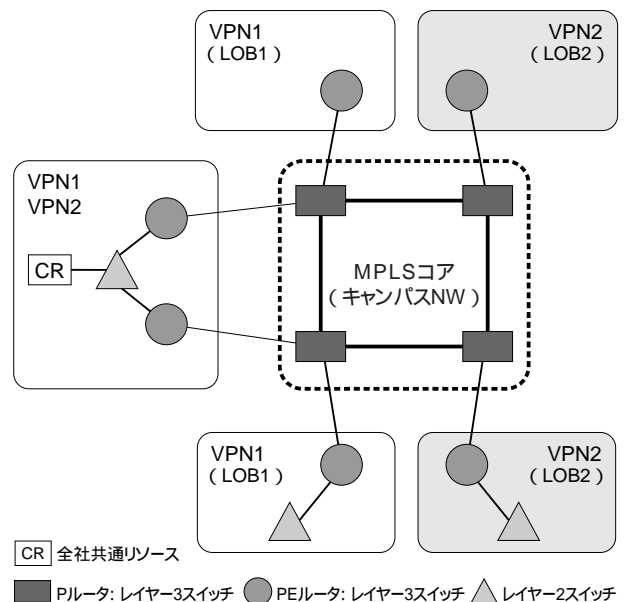


図2. パターン2のネットワーク構成例

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。

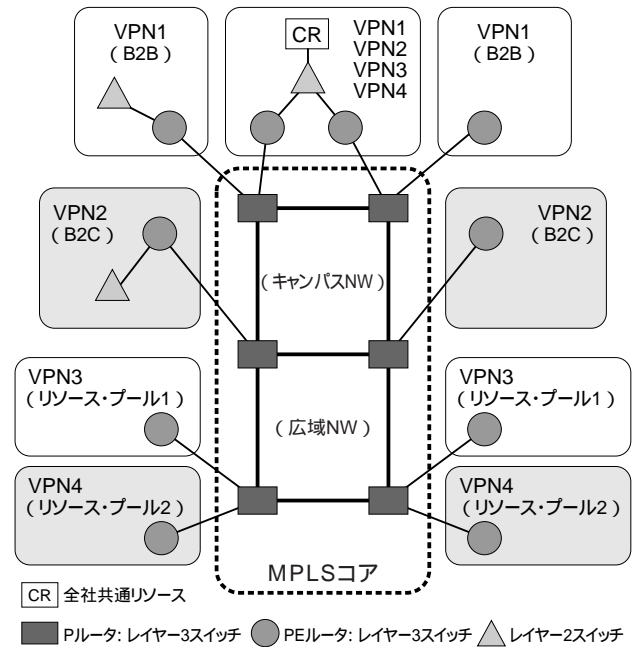


図3. パターン3のネットワーク構成例

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





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。

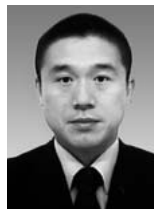
## 6. おわりに

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/mp1s01.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](mailto:kchin@jp.ibm.com)