MPLSネットワークにおけるバックアップLSP疎通確認手法の提案と評価

熊木健二[†1] 長谷川輝之[†1] 阿野茂浩[†1]

MPLS（Multi Protocol Label Switching）技術が普及したため，多くのサービスプロバイダは，本技術を基盤としたネットワークを構築し，様々なサービスを展開してきた．また，高品質サービスを提供するために，MPLS ネットワーク内でのリンクおよびノード障害を最小限にする高速迂回技術（FRR: Fast ReRoute）が導入されてきた．FRR を導入したサービスプロバイダは，迂回用のバックアップ LSP（Link Protection LSP，Node Protection LSP）を運用管理・監視する必要がある．しかし，従来提案されているデータプレーン疎通確認手法では，FRR 動作時のバックアップ LSP データプレーンを介した疎通確認を行うことは不可能である．そこで本論文では，MPLS ネットワークの安定運用に必要なバックアップ LSP データプレーンに対する自動疎通確認手法を提案する．提案した新たな手法は，実ルータでの動作を確認済みである．また，シミュレータによる評価の結果，実運用とほぼ同等の疎通確認時間で完了し十分実用的な手法であることが明らかになった．

Proposal and Evaluation of Verification Method for Connectivity of Backup LSPs in MPLS Networks

Kenji Kumaki,[†1] Teruyuki Hasegawa[†1] and Shigehiro Ano[†1]

Thanks to global dissemination of MPLS technology, various services such as Layer 2 VPN and Layer 3 VPN services have been provided in MPLS (Multi Protocol Label Switching) based networks. FRR (Fast ReRoute) in MPLS technology has been introduced in order to provide high quality services in MPLS production networks. Therefore, Service Providers need to operate and manage backup LSPs (i.e. Link Protection LSPs, Node Protection LSPs). However, the conventional proposed method can not realize connectivity of backup LSPs on the data plane before FRR is active. Consequently, this paper proposes an automatic verification method for connectivity of backup LSPs on the data plane in MPLS networks. Also, this proposed method realizes verification for connectivity of backup LSPs in them. Evaluation results show good performance under certain MPLS networks. Finally, this proposed method could be very useful in MPLS production networks.

1. はじめに

MPLS（Multi Protocol Label Switching）[1] 技術が普及したため，多くのサービスプロバイダは，MPLS 技術を基盤としたネットワークを構築し，その上で Layer 2 Virtual Private Networks（L2VPN）[2]，L3VPN [3]，インターネット等の様々なサービスを展開してきた．具体的には，ルータが，RSVP-TE [4]，LDP [5] を使用して MPLS Label Switched Path（LSP）をルータ間で確立し，その MPLS LSP を利用して様々なサービスを提供する．現在，トラヒック制御，帯域制御，QoS，アベイラビリティ等の観点から RSVP-TE を使用した MPLS Traffic Engineering（TE）LSP がサービスプロバイダネットワークで主に使用されている．

MPLS TE [4] の特徴の 1 つに高速迂回技術（Fast ReRoute: FRR）[6] がある．この技術は，MPLS ネットワーク内でのリンクおよびノード障害を局所的に迂回することでその影響を最小限にすることが可能である．FRR は，高品質サービスを提供するために必須な機能であり，多くのサービスプロバイダで使用されている．

MPLS TE LSP で FRR を使用する場合，提供するサービスの SLA を維持するために，通常の MPLS TE LSP（以下，LSP とする）に加えて局所迂回のための FRR 用バックアップ LSP（以下，バックアップ LSP とする）を管理・監視する必要がある．従来の MPLS

†1 株式会社 KDDI 研究所
KDDI R&D Laboratories Inc.

運用管理・監視技術として，LSP を可視化する手法[7]や LSP のデータプレーン疎通確認手法[8]が提案されており，サービスプロバイダはこれらの手法を用いて LSP およびバックアップ LSP の疎通確認を行ってきた．しかし，文献 8) で提案されている手法では，通常の経路に沿った LSP の疎通確認やバックアップ LSP（Link Protection[6] LSP，Node Protection[6] LSP）単体での疎通確認は可能であるものの，LSP が FRR 動作時にバックアップ LSP を使用することを想定したデータプレーンの疎通確認は不可能である．また，コア間およびエッジ間に確立されている LSP およびそのバックアップ LSP をすべて管理・監視する必要があることから，大規模ネットワークの実運用における LSP 管理・監視作業は非常に負荷の高いものとなっている．運用負荷を軽減するためには，上述の疎通確認を自動化する必要がある．

MPLS ネットワークにおける LSP の疎通確認に関連するその他の取組みとして，Cavendish ら[9]は，ITU-T および IETF における MPLS OAM の問題や MPLS ネットワークにおける OAM の要求について議論している．Aïssaoui ら[10]は，ITU-T および IETF における MPLS OAM 機能の説明およびその分類を行っている．これらの取組みでは，総括的な MPLS OAM に関する議論は行われているが，バックアップ LSP に関する確認手法や評価といった実運用に則したより詳細な議論は行われていない．

そこで，本論文では，MPLS ネットワークにおける FRR 安定運用を支えるためのバックアップ LSP（Link Protection LSP，Node Protection LSP）データプレーン自動疎通確認手法を提案する．本論文で提案する手法は，FRR が動作している場合と同様に，バックアップ LSP に疎通を確認するパケットを送出することを特徴とする．以下，本提案に対して，シミュレータを用いた評価を行い，本提案が想定したネットワークにおいて有意であることを示す．

本論文は，以下の章で構成されている．2 章では，FRR 技術概要とバックアップ LSP の運用課題に関して述べる．3 章では，提案するバックアップ LSP データプレーン自動疎通確認手法に関して説明する．4 章では，バックアップ LSP データプレーン自動疎通確認手法に関する評価および考察を行う．5 章でまとめを述べる．

2. FRR 技術とバックアップ LSP の概要

この章では，FRR 技術とバックアップ LSP の運用課題に関する説明を行う．

2.1 リカバリ技術

MPLS ネットワークにおけるリカバリ技術には，ローカルリカバリとグローバルリカバリがある[11]．前者は，障害部分だけを高速に迂回するために，局所的にバックアップ LSP を確立し，障害時にそのバックアップ LSP に迂回をする．後者は，障害を高速に迂回するために，始点ルータ（Head-end ルータ）と終点ルータ（Tail-end ルータ）間にバックアップ LSP を確立し，障害時にそのバックアップ LSP に迂回する[11]．FRR はローカルリカバリの一実施形態であり[11]，1 対 1 で高速迂回を実現する Detour LSP[6] と 1 対 N で高速迂回を実現する Link Protection LSP，Node Protection LSP に分類される．本論文では Link Protection LSP，Node Protection LSP を対象とする．以下，その概要を説明する．

2.2 Link Protection LSP

Link Protection は，ルータ間のリンク障害（たとえば，ファイバ障害，ルータインタフェース障害等）を高速に迂回する技術である．ルータが高速にその障害を検知し，あらかじめ設定された Link Protection LSP にデータ転送を行い，そのリンク障害を高速迂回する．障害検知は様々な方法により行われる．たとえば，POS（Packet-Over-SONET）インタフェースの場合，ルータが AIS（Alarm Indication Signal）を利用して障害検知を行う．また，インタフェースに依存しない方法として，ルータが BFD（Bidirectional Forwarding Detection）[12] を利用して障害検知を行う．そのため，データ転送断時間は，非常に短く数十 msec 以内といわれている[11]．

Link Protection LSP は，**図 1** に示すとおり，R1-R2-R3 を通過する LSP に対して R1-R2 間のリンク障害を守るために，あらかじめ R1 から R2 に対して設

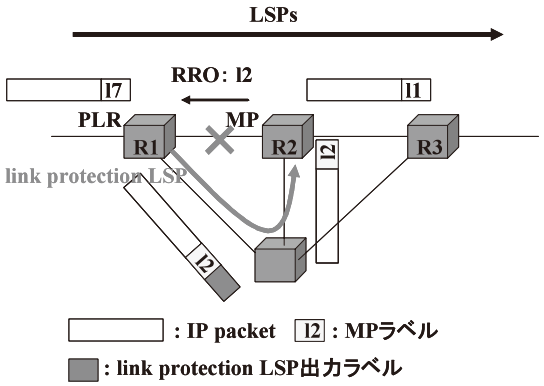

図 1 Link Protection
Fig. 1 Link Protection.

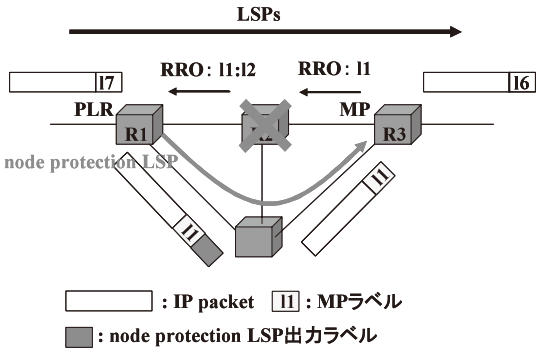

図 2 Node Protection
Fig. 2 Node Protection.

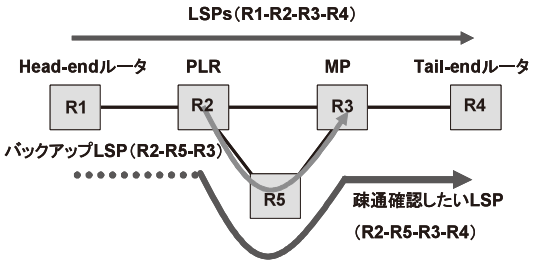

図 3 運用課題
Fig. 3 Operation issues.

定される．図 1 において，R1 は PLR（Point of Local Repair）[6] と呼ばれ，リンクの障害検知を行うとともに R1 に到着するパケットに対して，ラベル（l7）をスワップし，さらに，MP（Merge Point）[6] ラベル（l2）および Link Protection LSP 出力ラベルをプッシュして，Link Protection LSP に対してパケットを転送する役割を持つ．MP ラベルは R1-R2-R3 を通過する LSP の RRO（Record Route Object）[4] から取得する．R2 に到着したパケットは R3 へ転送される．Link Protection LSP は N 本の LSP に対して 1 本の Link Protection LSP を使用してバックアップを行う．

2.3 Node Protection

Node Protection は，ノード障害（たとえば，ルータハードウェア障害等）を高速に迂回する技術である．ルータが高速にその障害を検知し，あらかじめ設定された Node Protection LSP にデータ転送を行い，そのノード障害を高速迂回する．なお，ルータは，ノード自身の障害を検知するのではなく，Link Protection と同じリンク障害を検知して当該ノード迂回を行う．そのため，データ転送断時間は，非常に短く数十 msec 以内といわれている．

Node Protection LSP は，**図 2** に示すとおり，R1-R2-R3 を通過する LSP に対して R2 のノード障害を守るために，あらかじめ R1 から R3 に対して設定される．

図 2 において，R1 は PLR と呼ばれ，リンクの障害検知を行うとともに R1 に到着するパケットに対して，ラベル（l7）をスワップし，さらに，MP ラベル（l1）および Node Protection LSP 出力ラベルをプッシュして，Node Protection LSP に対してパケットを転送する役割を持つ．MP ラベルは R1-R2-R3 を通過する LSP の RRO から取得する．R3 に到着したパケットは R3 の次のルータに転送される．Node Protection LSP は N 本の LSP に対して 1 本の Node Protection LSP を使用してバックアップを行う．

Link Protection LSP と Node Protection LSP は，PLR から見た場合，それぞれの MP が，1 ホップ先（Next-Hop）もしくは 2 ホップ先（Next-Next-Hop）の違いである．

2.4 バックアップ LSP の運用課題

Link Protection LSP および Node Protection LSP（以下，バックアップ LSP とする）を導入した場合，リンクおよびノード障害時に，① PLR で処理されるバックアップ LSP 特有のラベルスタック（ラベルのプッシュ動作）や，② MP でのマージ動作を事前にデータプレーンで確認できないことが，MPLS 実運用上の課題となる．この結果，実際に障害が起こった場合にバックアップ LSP を用いたデータプレーン疎通の保証はできない．これは，FRR の実装上，PLR においてリンクおよびノード障害時のみルータのデータプレーンにバックアップ LSP に転送する情報がインストールされ，ラベルのプッシュ動作が行われるためである．このため，事前に R1-R2-R5-R3-R4（**図 3** 参照）の疎通確認はできない．

エンド・エンド（R1-R2-R5-R3-R4）での疎通確認実現が実運用の観点からは望ましいが，① については障害が発生しない限り確認ができない．一方，② については障害時に起こるラベルプッシュ動作をエミュレートすることで確認が可能である．そこで，図 3 に示すとおり，LSP が PLR からリンクおよびノード障害時にバックアップ LSP を使用することを想定した終点ルータまでのデータプレーンの疎通確認（R2-R5-R3-R4）を行う手法を提案する．従来の運用では，上記疎通確認作業を行うことができなかったため，コントロールプレーンのラベル情報（MP ラベル情報，バックアップ LSP 出力ラベル情報）確認および LSP ping [8] を使用した LSP（R1-R2-R3-R4）およびバックアップ LSP（R2-R5-R3）単体のデータプレーン疎通確認（図 3 参照）にとどまっていた．

上記運用課題を満たすために，PLR は，FRR が動

作している場合と同様に，バックアップ LSP に疎通を確認するパケットを送出する必要がある．

もう 1 つの運用課題は，バックアップ LSP の数が非常に多いことである．その数は，数百から数千程度となる．運用者が，バックアップ LSP のデータプレーン確認作業を手動で行う場合，非常に時間を費やす．そのため，バックアップ LSP のデータプレーンの疎通を自動で確認する手法が必要である．

3. 提案するバックアップ LSP データプレーン自動疎通確認手法

この章では，2.4 節で述べたバックアップ LSP の運用課題を解決するための手法について提案する．

提案するバックアップ LSP データプレーン疎通確認手法の構成要素は，以下のとおりである．また，下記手法は各 PLR で独立に行われる．

1. 文献 8) で定義される確認パケットに対して，MP ラベルおよびバックアップ LSP の出力ラベルをこの順番にプッシュする機能．
2. PLR を通過する LSP のうち，Local Protection desired flag [4),6)] もしくは Local Protection desired flag および Node Protection desired flag [6)] を送出する LSP の終点ルータに対して，バックアップ LSP インタフェースへラベル化された確認パケット（MPLS echo request）を送出する機能．このとき，ルータのデータベースにあらかじめインストールされている FRR 情報を使用する．
3. 終点ルータから応答パケット（MPLS echo reply）を受信することでバックアップ LSP データプレーンの疎通を確認する機能．

提案する手法のフローチャートを**図 4** に示す．その詳細な手順は以下のとおりである．

手順 1：各 PLR に存在する FRR データベース（ルータが保持するデータベース）からバックアップ LSP を検索する．ここでは，バックアップ LSP に対する出力ラベルおよび出力インタフェースを保持する．

手順 2：手順 1 で選択したバックアップ LSP に対して，そのバックアップ LSP を使用する LSP をすべて検索し，それらの LSP 情報を保持する．

手順 3：手順 2 で記録された LSP の MP ラベルを保持する．

手順 4：手順 1〜3 で得られた情報（バックアップ LSP 出力インタフェース情報，バックアップ LSP 出力ラベル情報，MP ラベル情報，LSP 情報）を使用して，確認パケットを送出する．その情報の例を**表 1** に示す．その後，応答パケットを受信する．

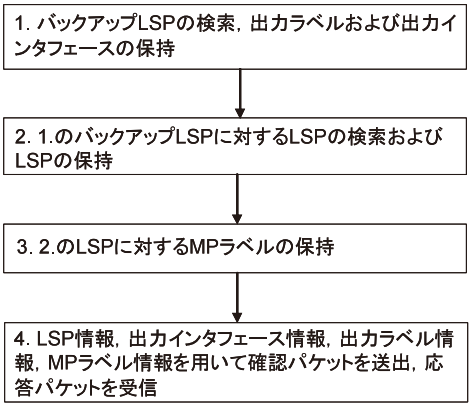

図 4 提案アルゴリズム
Fig. 4 Proposed algorithms.

表 1 バックアップ LSP データプレーン疎通確認
Table 1 Information for verifying connectivity of backup LSPs.

バックアップLSP 出力インタフェース	バックアップLSP 出力ラベル	MPラベル	RSVP TE LSP
interface1	200	100	LSP1
interface1	200	101	LSP2
interface1	200	102	LSP3
interface1	200	103	LSP4
interface2	201	104	LSP5
interface2	201	105	LSP6
interface2	201	106	LSP7
interface3	202	107	LSP8
interface3	202	108	LSP9
interface3	202	109	LSP10
interface3	202	110	LSP11

具体的には，PLR から確認パケットを送出する場合，表 1 に表示されている LSP 情報から文献 8) で定義された Target FEC Stack として Sub-Type = 3, Length = 20（RSVP IPv4 LSP）を設定し，これらの確認パケットに対して，MP ラベルおよびバックアップ LSP 出力ラベルを順番にプッシュする．これらのラベルは 4 byte [13)] である．また，この確認パケットは，文献 8) のパケットフォーマットに従う．

PLR は，確認すべきバックアップ LSP に関連するすべての LSP の終点ルータに対して，バックアップ LSP 出力インタフェースへラベル化された確認パケットを送出する．送出した確認パケットに対して，終点ルータから応答パケットを受信した時点で，バックアップ LSP データプレーンの疎通を確認できる．

4. バックアップ LSP データプレーン自動疎通確認手法の評価

この章では，バックアップ LSP データプレーンの疎通確認手法の評価について，**図 5** および**図 6** に示

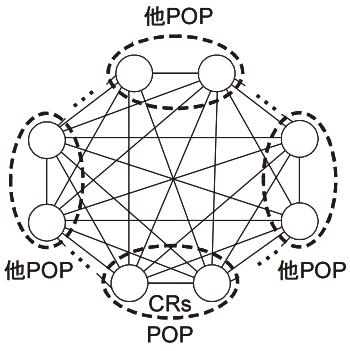

図 5 コアネットワークトポロジ
Fig. 5 Core network topology.

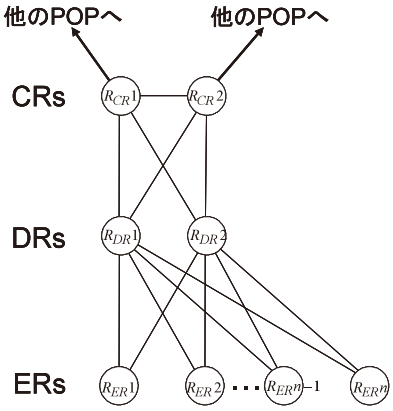

図 6 POP 内ネットワークトポロジ
Fig. 6 Network topology in a POP.

すネットワークトポロジを想定し，バックアップ LSP データプレーンの疎通確認時間を評価する[14),15)]．最初に，ネットワークの規模および確認すべきバックアップ LSP の数に関して述べ，次に，バックアップ LSP データプレーンの疎通確認時間を評価する．

なお，3 章で述べたとおり，各 PLR が，独立にデータプレーンの疎通確認を行うことから，以下では，各 PLR が処理すべき LSP 数について議論する．

4.1 MPLS ネットワークにおけるバックアップ LSP 数の解析的評価

想定するネットワークは，コアルータ，エッジルータを集約する集約ルータおよびエッジルータから構成される．最初に，コアルータの構成を説明する．図 5 は，POP（Points of Presence）にあるコアルータからフルメッシュに他 POP のコアルータに対してリンク[16)]が存在するネットワークトポロジである．この場合，下位レイヤは，オプティカル GMPLS（Generalized MPLS）によりフルメッシュパスを提供することを想定している[14),17),18)]．また，コアルータ間のリンクのコストは，すべて等しいものとする．次に，POP 内の構成を説明する．図 6 は，コアルータ，集約ルータおよびエッジルータからなるネットワークトポロジであり，各 POP 内で同じトポロジとする[15)]．また，コアルータと集約ルータ間および集約ルータとエッジルータ間のリンクのコストは，それぞれのリンク間で等しいものとする．以下のとおり，各ルータの数を定義する．ただし，n（$n \geq 1$）は，POP 内におけるエッジルータの数，x（$x \geq 1$）は，POP の数とする．

コアルータ数： $CR(x) = 2x$ (1)

集約ルータ数： $DR(x) = 2x$ (2)

エッジルータ数：$ER(n, x) = nx$ (3)

実運用に近いネットワーク環境を想定するため，下記の 2 パターンに関して，議論を行う．

パターン 1：コアルータ間でフルメッシュに LSP を確立するケース

パターン 2：エッジルータ間でフルメッシュに LSP を確立するケース

はじめに，パターン 1 の議論を行う．以下の議論は，各コアルータに対し LSP を 1 本ずつ確立することを仮定する．

パターン 1：

図 5 のネットワーク構成から，コアルータが PLR となる．PLR における機能種別は，LSP の始点ルータおよび LSP の終点ルータであり，トランジットルータにはならない．バックアップ LSP データプレーンの疎通確認を評価するには，各 PLR から確立しているバックアップ LSP に対して，そのバックアップ LSP を使用する LSP の数を求める必要がある．そこで，最初に，各 PLR が始点ルータとして LSP を確立する LSP の数を求める．

コアルータ（PLR）間でフルメッシュに LSP を確立する場合，同じ POP 内のもう 1 つのコアルータには LSP を確立する必要がないため，各コアルータから確立する LSP の数は，式 (1) より，以下のとおりとなる．

1 つのコアルータから確立する LSP 数：

$$CR(x) - 2 = 2(x - 1) \quad (4)$$

次に，LSP とバックアップ LSP の関係を述べる．すべてのリンクおよびノードを守るためにバックアップ LSP を確立すると仮定する．図 5 のネットワーク構成から，各 LSP は直接コアルータ間で確立されるため，Node Protection LSP を使用することはない．したがって，各コアルータ間のリンクを守る Link Protection LSP のみが関係する．

以上より，式 (4) のすべての LSP に対して，Link Protection LSP が 1 本存在するため，各 PLR が確

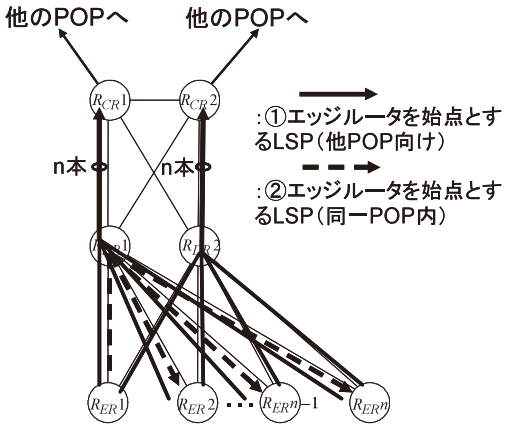

図 7 エッジルータを始点とする LSP
Fig. 7 LSPs originating from edge routers.

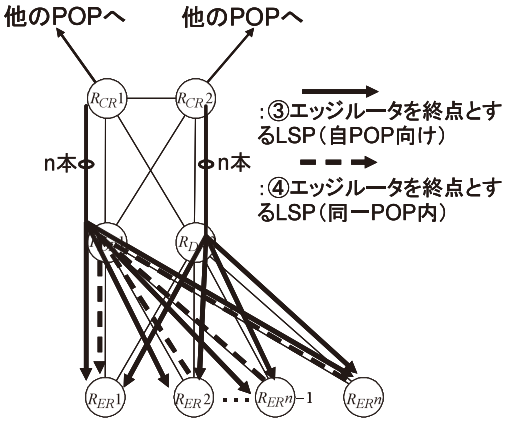

図 8 エッジルータを終点とする LSP
Fig. 8 LSPs terminating to edge routers.

認すべき LSP の数は，以下のとおりとなる．

各 PLR が確認すべき LSP 数：$2(x-1)$ (5)

式 (5) より，$O(x)$ となる．

次に，パターン 2 に関する議論を行う．パターン 1 同様，以下の議論は，各エッジルータに対し LSP を 1 本ずつ確立することを仮定する．

パターン 2：

図 6 のネットワークトポロジから，エッジルータは，LSP を確立する始点ルータおよび LSP を終端する終点ルータである．コアルータおよび集約ルータは，トランジットルータである．**図 7**，**図 8** に，それぞれ 1 台のエッジルータが始点，終点になる LSP を示す．

バックアップ LSP データプレーンの疎通確認を評価するには，各 PLR から確立しているバックアップ LSP に対して，そのバックアップ LSP を使用する LSP の数を求める必要がある．そこで，最初に，各 PLR が始点ルータとして LSP を確立する LSP の数，終点ルータとして LSP を終端する LSP の数およびトランジットルータとして通過する LSP の数を求める．PLR は，コアルータ，集約ルータおよびエッジルータになるため，各ルータ種別の LSP 数を下記 3 パターンで求める．以下，図 7，図 8 に示す $R_{ER}1$ を中心に議論をする．

1. LSP を確立する始点ルータ（エッジルータ）1 台あたりの LSP 数

エッジルータ（$R_{ER}1$）は，図 7 に示すとおり，他 POP のエッジルータに対して，2 つの集約ルータ（$R_{DR}1$，$R_{DR}2$）を均等に通過するように LSP を確立する（図 7 の ①）ことを仮定する．また，同一 POP 内のエッジルータ（$R_{ER}2, \cdots, R_{ER}n$）に対しては，集約ルータ（$R_{DR}1$）のみを通過するように LSP を確立する（図 7 の ②）ことを仮定する．$R_{ER}1$–$R_{DR}1$，$R_{ER}1$–$R_{DR}2$ における ①，② の LSP 数は，以下のとおり．

$R_{ER}1$–$R_{DR}1$ における ① の LSP 数：

$$\frac{n(x-1)}{2} \tag{6}$$

$R_{ER}1$–$R_{DR}1$ における ② の LSP 数：

$$n-1 \tag{7}$$

$R_{ER}1$–$R_{DR}2$ における ① の LSP 数：

$$\frac{n(x-1)}{2} \tag{8}$$

以上より，エッジルータ（$R_{ER}1$）から確立する LSP 数は，以下のとおりとなる．

エッジルータから確立する LSP 数：

$$\begin{aligned} &R_{ER}1 \rightarrow R_{DR}1\text{: } \frac{n(x-1)}{2} + n - 1 \\ &R_{ER}1 \rightarrow R_{DR}2\text{: } \frac{n(x-1)}{2} \end{aligned} \tag{9}$$

他のエッジルータ（$R_{ER}2, \cdots, R_{ER}n$）も同様となる．

2. LSP を終端する終点ルータ（エッジルータ）1 台あたりの LSP 数

エッジルータ（$R_{ER}1$）は，図 8 に示すとおり，他 POP のエッジルータから，2 つの集約ルータ（$R_{DR}1$，$R_{DR}2$）を均等に通過するように LSP を確立する（図 8 の ③）ことを仮定する．また，POP 内のエッジルータ（$R_{ER}2, \cdots, R_{ER}n$）からエッジルータ（$R_{ER}1$）に対しては，集約ルータ（$R_{DR}1$）のみを通過するように LSP を確立する（図 8 の ④）ことを仮定する．$R_{DR}1$–$R_{ER}1$，$R_{DR}2$–$R_{ER}1$ における ③，④ の LSP 数は，以下のとおり．

$R_{DR}1$–$R_{ER}1$ における ③ の LSP 数：

式 (6) と同じ．

$R_{DR}1$–$R_{ER}1$ における ④ の LSP 数：
式 (7) と同じ．
$R_{DR}2$–$R_{ER}1$ における ③ の LSP 数：
式 (8) と同じ．

以上より，エッジルータ（$R_{ER}1$）で終端する LSP 数は，以下のとおりとなる．
エッジルータで終端する LSP 数：

$$\begin{aligned} &R_{DR}1 \rightarrow R_{ER}1\text{: } \frac{n(x-1)}{2} + n - 1 \\ &R_{DR}2 \rightarrow R_{ER}1\text{: } \frac{n(x-1)}{2} \end{aligned} \tag{10}$$

他のエッジルータ（$R_{ER}2, \cdots, R_{ER}n$）も同様となる．

3. トランジットルータを通過する LSP 数

1 つ目に，集約ルータ（$R_{DR}1$，$R_{DR}2$）からコアルータ方向に通過する LSP の数を求める．

POP 内エッジルータ間の LSP（図 7 の ②）を考慮し，それぞれの集約ルータ（$R_{DR}1$，$R_{DR}2$）からコアルータ（$R_{CR}1$，$R_{CR}2$）方向に通過する LSP の数は，式 (6)，(8) より，以下のとおりとなる．
1 つの集約ルータからコアルータ方向に通過する LSP 数：

$$\begin{aligned} &R_{DR}1 \rightarrow R_{CR}1\text{: } n * \frac{n(x-1)}{2} = \frac{n^2(x-1)}{2} \\ &R_{DR}2 \rightarrow R_{CR}2\text{: } n * \frac{n(x-1)}{2} = \frac{n^2(x-1)}{2} \end{aligned} \tag{11}$$

2 つ目に，コアルータ（$R_{CR}1$，$R_{CR}2$）から他 POP へ通過する LSP の数を求める．式 (11) より，それぞれのコアルータ（$R_{CR}1$，$R_{CR}2$）から他 POP へ通過する LSP の数は，以下のとおり．
1 つのコアルータから他 POP へ通過する LSP 数：

$$\begin{aligned} &R_{CR}1 \rightarrow \text{他 POP}\text{: } \frac{n^2(x-1)}{2} \\ &R_{CR}2 \rightarrow \text{他 POP}\text{: } \frac{n^2(x-1)}{2} \end{aligned} \tag{12}$$

3 つ目に，他 POP からコアルータ（$R_{CR}1$，$R_{CR}2$）を通過する LSP の数を求める．2 つ目と同様に考えると，式 (12) より，他 POP からそれぞれのコアルータ（$R_{CR}1$，$R_{CR}2$）を通過する LSP の数は，以下のとおり．
他 POP から 1 つのコアルータを通過する LSP 数：

$$\begin{aligned} &\text{他 POP} \rightarrow R_{CR}1\text{: } \frac{n^2(x-1)}{2} \\ &\text{他 POP} \rightarrow R_{CR}2\text{: } \frac{n^2(x-1)}{2} \end{aligned} \tag{13}$$

4 つ目に，コアルータ（$R_{CR}1$，$R_{CR}2$）から集約ルータ方向に通過する LSP の数を求める．式 (13) より，それぞれのコアルータ（$R_{CR}1$，$R_{CR}2$）から集約ルータ（$R_{DR}1$，$R_{DR}2$）方向に通過する LSP の数は，以下のとおり．
1 つのコアルータから集約ルータ方向に通過する LSP 数：

$$\begin{aligned} &R_{CR}1 \rightarrow R_{DR}1\text{: } \frac{n^2(x-1)}{2} \\ &R_{CR}2 \rightarrow R_{DR}2\text{: } \frac{n^2(x-1)}{2} \end{aligned} \tag{14}$$

次に，LSP とバックアップ LSP の関係を述べる．すべてのリンクおよびノードを守るためにバックアップ LSP を確立すると仮定する．図 6 のネットワーク構成から，LSP の始点および終点となるエッジルータに対する Node Protection LSP は確立できない．そのため，リンクを守る Link Protection LSP，コアルータおよび集約ルータを守る Node Protection LSP を考慮する．

実運用では，(I) Link Protection LSP のみを確立する運用，(II) Link Protection LSP および Node Protection LSP を確立する運用がある．後者の運用では，2.3 節で説明したようにノード・リンクいずれの障害においても PLR 自身はリンク断を検出したうえで，Node Protection LSP を優先する[15]．そのため，以下では (I) の運用と (II) の運用についてそれぞれ評価する．

各 PLR が確認すべき LSP の数は，以下のとおりとなる．

エッジルータ：

エッジルータの場合，$R_{ER}1$–$R_{DR}1$，$R_{ER}1$–$R_{DR}2$ のリンク障害および $R_{DR}1$，$R_{DR}2$ のノード障害が関係する．式 (9) より，各 PLR が確認すべきバックアップ LSP の数は，以下のとおりとなる．
各 PLR が確認すべきバックアップ LSP 数（(I) Link Protection LSP が設定されている場合）：

$$\begin{aligned} &\frac{n(x-1)}{2} + n - 1 + \frac{n(x-1)}{2} \\ &= nx - 1 \end{aligned} \tag{15}$$

各 PLR が確認すべきバックアップ LSP 数（(II) Link Protection LSP および Node Protection LSP が設定されている場合）：

$$\begin{aligned} &\frac{n(x-1)}{2} + n - 1 + \frac{n(x-1)}{2} \\ &= nx - 1 \end{aligned} \tag{16}$$

式 (15)，(16) より，$O(nx)$ となる．

集約ルータ：

集約ルータの場合，$R_{DR}1$–$R_{CR}1$，$R_{DR}1$–$R_{CR}2$

のリンク障害，エッジルータへのリンク障害および $R_{CR}1$，$R_{CR}2$ のノード障害が関係するが，LSP は，$R_{DR}1$–$R_{CR}2$ を通過しないため，$R_{DR}1$–$R_{CR}2$ のリンクおよび $R_{CR}2$ のノードを除くリンクおよびノード障害を考慮する．エッジルータと同様の評価を行うと，式 (10)，(11) より，PLR（$R_{DR}1$）が確認すべきバックアップ LSP の数は，以下のとおりとなる．

PLR が確認すべきバックアップ LSP 数（（I）Link Protection LSP が設定されている場合）：

$$\frac{n^2(x-1)}{2} + n\left\{n-1+\frac{n(x-1)}{2}\right\} = n^2x - n \quad (17)$$

PLR が確認すべきバックアップ LSP 数（（II）Link Protection LSP および Node Protection LSP が設定されている場合）：

$$\frac{n^2(x-1)}{2} + n\left\{n-1+\frac{n(x-1)}{2}\right\} = n^2x - n \quad (18)$$

式 (17)，(18) より，$O(x*n^2)$ となる．なお，$R_{DR}2$ の確認する LSP 数は，POP 内で始点および終点となる LSP が通過しない理由により，式 (17)，(18) より少なくなる．このため評価には，式 (17)，(18) を用いる．

コアルータ：

コアルータの場合，他 POP コアルータでのリンク障害，ノード障害，POP 内における $R_{CR}1$–$R_{DR}1$，$R_{CR}1$–$R_{DR}2$，$R_{CR}1$–$R_{CR}2$ のリンク障害および $R_{CR}2$，$R_{DR}1$，$R_{DR}2$ のノード障害が関係するが，LSP が $R_{CR}1$–$R_{CR}2$，$R_{CR}1$–$R_{DR}2$ を通過しないことから，$R_{CR}1$–$R_{CR}2$，$R_{CR}1$–$R_{DR}2$ のリンクおよび $R_{CR}2$，$R_{DR}2$ のノードを除くリンクおよびノード障害を考慮する．エッジルータと同様の評価を行うと，式 (12)，(14) より，PLR（$R_{CR}1$）が確認すべきバックアップ LSP の数は，以下のとおりとなる．

PLR が確認すべきバックアップ LSP 数（（I）Link Protection LSP が設定されている場合）：

$$\frac{n^2(x-1)}{2} + \frac{n^2(x-1)}{2} = n^2(x-1) \quad (19)$$

PLR が確認すべきバックアップ LSP 数（（II）Link Protection LSP および Node Protection LSP が設定されている場合）：

$$\frac{n^2(x-1)}{2} + \frac{n^2(x-1)}{2} = n^2(x-1) \quad (20)$$

式 (19)，(20) より，$O(x*n^2)$ となる．コアルータ（$R_{CR}2$）も同様となる．

4.2 提案手法のシミュレータによる評価と考察

4.1 節で議論した各パターンでの解析結果に基づき，以下の手法を用いて，バックアップ LSP データプレーン疎通確認時間を評価する．数台程度の実環境での動作確認も行っているが，評価するルータの台数の関係から実ルータの処理時間を反映可能なシミュレータを用いて行った．シミュレータの CPU は，UltraSPARC T1 × 8（個）程度の能力を有する．

本シミュレータは，1 台のサーバ内に仮想的に複数のルータを作成しそのルータ間でパケット処理を行う．そのため，下記の結果はサーバ内の仮想ルータにおけるパケット処理時間の総和を表す．

4.2.1 コアルータ間でフルメッシュに LSP を確立するケース（パターン 1）

このケースでは，4.1 節式 (5) に示すように，確認すべきバックアップ LSP の数が，コアルータの数に依存するため，以下の条件に従い，評価を行う．

以下に，想定するネットワーク構成条件および評価条件を示す．

ネットワーク構成条件：

1. 式 (1) において，x を 5 から 25 まで 5 POP ごとに増加させる．つまり，全体のコアルータ数を 10 台から 50 台まで変化させる．
2. 図 5 に示すフルメッシュを構成する．また，コアルータ間のリンクのコストは，すべて等しい．

評価条件：

1. コアルータ間でフルメッシュの LSP を確立する．ただし，同じ POP 内のコアルータには LSP を確立しない．各ルータに対して LSP を 1 本ずつ確立する．
2. すべての始点ルータは，LSP に対して Local Protection desired flag および Node Protection desired flag を送信する．
3. すべてのリンクおよびノードを守るためのバックアップ LSP を確立する．
4. インタフェースは 10G Ethernet，インタフェース間の伝送遅延は 0 とする．
5. バックアップ LSP データプレーンのパケット処理時間は，各 PLR が，3 章で提案した手法を用いて確認パケットを生成し，各 PLR が，確認すべきバックアップ LSP を通過する全 LSP に対して確認パケットを送出し，応答パケットを受信した時点での実行時間を測定する．
6. 取得データは，1,000 回取得したデータの平均とする．

図 9 は，コアルータ間でフルメッシュに LSP を確立

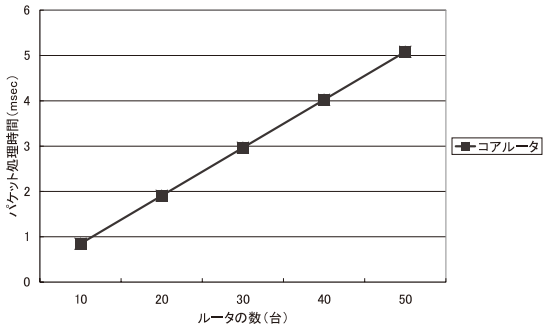

図 9 評価結果（1）
Fig. 9 Evaluation results (1).

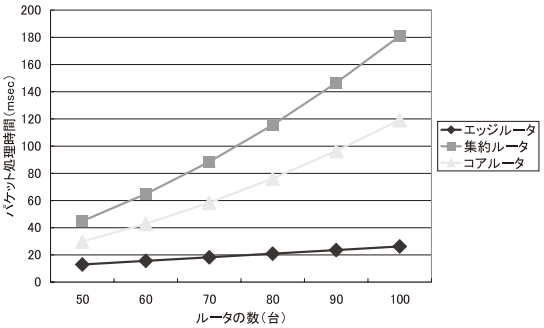

図 10 評価結果（2）
Fig. 10 Evaluation results (2).

した場合，PLR 1 台あたりのバックアップ LSP データプレーンのパケット処理時間を示す．

図 9 では，ルータの台数の増加に対して，ほぼ比例をしてパケット処理時間が増加している．これは，式 (5) で示したオーダ（$O(x)$）と一致する．

また，PLR であるコアルータが，独立にこの処理を行っているため，ネットワーク全体のバックアップ LSP データプレーンのパケット処理時間は，図 9 に示す時間に等しくなる．

シミュレータを用いた評価結果から，バックアップ LSP 1 本あたりのパケット処理時間は，ルータの数に関係なく平均で 106 μsec 程度であった．実際の MPLS ネットワークにおいて，たとえば東阪の往復伝送遅延時間（理論値）が 7 msec 程度であるため，実際の 1 本あたりのバックアップ LSP の疎通確認時間は，本提案のパケット処理時間に往復伝送遅延時間を加えても 7 msec 程度となり，現状の運用における 1 本あたりの MPLS パスデータプレーン疎通確認時間とほぼ一致する．

以上の結果からパターン 1 のトポロジにおいて，バックアップ LSP 疎通確認が実用的な処理負荷で実現できる見込みを得た．

4.2.2 エッジルータ間でフルメッシュに LSP を確立するケース（パターン 2）

このケースでは，4.1 節式 (15)〜(20) で評価したように，エッジルータの数に依存するため，以下の条件に従い，評価を行う．

ネットワーク構成条件：

1. 式 (3) において，x を 10 に固定し，n を 5 から 10 に変化させる．つまり，全体のエッジルータを 50 台から 100 台に変化させる．
2. 図 6 に示すネットワーク構成とする．コアルータと集約ルータ間および集約ルータとコアルータ間のリンクのコストは，それぞれのリンク間で等しい．また，POP 間のネットワークは，4.2.1 項のネットワークを使用する．

評価条件：

4.2.1 項と同じとする．

図 10 は，エッジルータ間でフルメッシュに LSP を確立した場合，PLR 1 台あたりのバックアップ LSP データプレーンの正常性確認時間を示す．

図 10 では，ルータの台数の増加に対して，ほぼ比例してエッジルータでのバックアップ LSP のパケット処理時間が増加している．また，コアルータおよび集約ルータでは，ルータの台数の増加に対して，ほぼ 2 乗でバックアップ LSP のパケット処理時間が増加している．エッジルータに関しては，式 (16) において，POP 数（x）を固定した場合のオーダ（$O(n)$）と一致する．コアルータおよび集約ルータに関しては，式 (18)，(20) において，POP 数（x）を固定した場合のオーダ（$O(n^2)$）と一致する．この 2 つのパケット処理時間の差は，エッジルータが POP 内で折り返す LSP 数およびホップするルータ数の差に相当する．

なお，PLR であるエッジルータ，集約ルータおよびコアルータが，独立にこの処理を行っているため，ネットワーク全体のバックアップ LSP データプレーンのパケット処理時間は，最も時間を費やした集約ルータのパケット処理時間に等しくなる．

シミュレータを用いた評価結果から，バックアップ LSP 1 本あたりのパケット処理時間は，ルータの台数に関係なく平均でエッジルータ，集約ルータ，コアルータ，それぞれ 265 μsec，183 μsec，132 μsec 程度であった．4.2.1 項と同様の議論により，現状の運用における 1 本あたりの MPLS パスデータプレーン疎通確認時間とほぼ一致する．

以上の結果からバックアップ LSP 疎通確認がパターン 2 のトポロジにおいても実用的な処理負荷で実現できる見込みを得た．

5. ま と め

本論文では，MPLS ネットワークにおける，バックアップ LSP（Link Protection LSP，Node Protection LSP）データプレーン自動疎通確認手法を提案した．また，バックアップ LSP データプレーン自動疎通確認手法を示し，その提案手法を評価した．

従来の MPLS ネットワークの実運用では，LSP が FRR 動作時にバックアップ LSP を使用することを想定したデータプレーンの疎通確認は不可能であり，コントロールプレーンのラベル情報（MP ラベル情報，バックアップ LSP 出力ラベル情報）確認および LSP ping を使用した LSP およびバックアップ LSP 単体のデータプレーン疎通確認にとどまっていた．しかし，提案した新たな手法により，従来の MPLS ネットワークの実運用において確認できなかったバックアップ LSP データプレーン疎通確認を実現した．

提案手法の評価において，実ネットワークを想定し，バックアップ LSP データプレーン疎通確認は，実運用とほぼ同等の疎通確認時間で行えることが分かり，MPLS ネットワークの実運用に適用できる見込みを得た．なお，プロトタイプによる数台の実環境での動作についても確認済みである．

以上の結果から，実現機能およびその処理オーバヘッドの観点で，本提案手法は，MPLS ネットワークの実運用安定化に資する有益な手法である．

参 考 文 献

1) Rosen, E., Viswanathan, A. and Callon, R.: Multiprotocol Label Switching Architecture, IETF RFC3031 (Jan. 2001).
2) Andersson, L. and Rosen, E.: A framework for layer 2 virtual private networks (L2VPNs), IETF RFC4664 (Sep. 2006).
3) Callon, R. and Suzuki, M.: Framework for layer 3 provider provisioned virtual private networks, IETF RFC4110 (July 2005).
4) Awduche, D., et al.: RSVP-TE: Extensions to RSVP for LSP Tunnels, IETF RFC3209 (Dec. 2001).
5) Andersson, L., et al.: LDP Specification, IETF RFC3036 (Jan. 2001).
6) Pan, P., Swallow, G. and Atlas, A.: Fast Reroute Extensions to RSVP-TE for LSP Tunnels, IETF RFC4090 (May 2005).
7) Nakagawa, I.: MPLS Path Management, *Apricot2005* (Feb. 2005).
8) Kompella, K. and Swallow, G.: Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures, IETF RFC4379 (Feb. 2006).
9) Cavendish, D., Ohta, H. and Rakotoranto, H.: Operation, administration, and maintenance in MPLS networks, *IEEE Communications Magazine*, Vol.42, Issue 10, pp.91–99 (Oct. 2004).
10) Aïssaoui, M., Watkinson, D. and Bocci, M.: OA&M in a converged IP/MPLS network, technology white paper, Alcatel Telecommunications Review (2004).
11) Vasseur, J.-P., Pickavet, M. and Demeester, P.: *Network Recovery*, pp.309–310, pp.314–324, p.336, Morgan Kaufmann Pub. (Aug. 2004).
12) Katz, D. and Ward, D.: Bidirectional Forwarding Detection, IETF Internet-Draft, draft-ietf-bfd-base-06.txt (Mar. 2007).
13) Rosen, E., et al.: MPLS Label Stack Encoding, IETF RFC3032 (Jan. 2001).
14) Yagi, T., et al.: A Distributed Traffic Monitoring Scheme for Scalable IP-over-Optical Networks, p.21 (2006). http://www.wtc2006.hu/present/1568973530_X_Takeshi_yagi_ohp.ppt
15) Osborne, E. and Simha, A.: *Traffic Engineering with MPLS*, p.332, pp.392–394, Cisco Press (2003).
16) Kumaki, K., et al.: Interworking Requirements to Support operation of MPLS-TE over GMPLS networks, IETF Internet Draft (Dec. 2006). draft-ietf-ccamp-mpls-gmpls-interwork-reqts-00.txt
17) Berger, L., et al.: Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description, IETF RFC3471 (Jan. 2003).
18) Berger, L., et al.: Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions, IETF RFC3473 (Jan. 2003).

(平成 19 年 6 月 7 日受付)
(平成 19 年 12 月 4 日採録)

熊木 健二（正会員）

1996 年名古屋大学大学院工学研究科修了．同年国際電信電話株式会社（現 KDDI 株式会社）入社．同社にて internet KDD の設計・開発・運用を経たのち，1999 年より MPLS に関わる技術開発から IP-VPN サービス立上げを行い，設計・開発・運用支援に携わる．現在 KDDI 研究所にて，次世代ネットワークアーキテクチャおよびそのプロトコルに関する研究に従事．IETF CCAMP，L3VPN，MPLS，PCE 等の WG で標準化活動を行い，多数の RFC，I-D を提出している．現在，PCE WG design team のメンバ．

長谷川輝之（正会員）

1991 年京都大学工学部電気第二工学科卒業．1993 年同大学大学院修士課程修了．同年 KDD（株）入社．以来，研究所にて，高速通信プロトコル，次世代インターネットの研究に従事．現在，（株）KDDI 研究所 IP 品質制御システムグループ主任研究員．平成 15 年度電波産業会電波功績賞受賞．

阿野 茂浩（正会員）

1987 年早稲田大学理工学部電子通信工学科卒業．1989 年同大学大学院修士課程修了．同年国際電信電話株式会社入社．以来，研究所にて，ATM 交換方式，IP ネットワーク管理・制御，次世代インターネットの研究に従事．現在，（株）KDDI 研究所 IP 品質制御システムグループリーダ．1995 年度情報処理学会学術奨励賞受賞．電子情報通信学会会員．