SDN ガイドライン

第 1.0 版

NTT コミュニケーションズ株式会社

2016 年 3 月 31 日

改訂履歴

日付	版数	備考
2015 年 3 月 31 日	第 0.1 版	・ 初版を作成。
2016 年 3 月 31 日	第 1.0 版	・ 「第 3 編 運用・監視フェーズ」を追加。 ・ 第 3 編の追加に伴い、整合性等を整えるため全体的に見直し。

目次

第1編 概説

第1章 はじめに

第1節 背景

1. ネットワークの動向と課題

昨今、クラウドサービス利用の拡大、スマートフォンの普及、センサ情報の活用の進展などに伴うネットワーク利活用環境の変化や、これらを活用した情報通信サービスの多様化が進んでいる。ネットワーク上のトラヒック特性が、よりダイナミックに変化するようになったことに伴い、ネットワークへの要求条件も変化している。従来のネットワーク構築、制御技術ではこれに迅速に対応することが困難な状況が生じつつあり、より柔軟なネットワーク設計及び制御を実現する必要性が高まっている。

このため、ネットワーク上の多種多量なデータ（ビッグデータ）の流通を柔軟に制御できるようにするとともに、これらのデータを活用した新たなサービスを支える多種多様なネットワークを迅速に設計・構築・運用できるようにするため、広域ネットワークへの「ネットワーク仮想化技術」の導入が急務である。

ネットワーク仮想化技術の実現には、ネットワークアーキテクチャである「SDN (Software-Defined Networking) 」を基盤とした実用化が進められている。

しかしながら、現段階では SDN を通信事業者のネットワークに適用する明確な指針が存在しない状況である。

2. SDN に対する期待

昨今のデータ通信トラヒックの増加やアプリケーションサービスの高度化、高機能化に伴い、通信事業者に対しては、高速大容量通信をより高品質で低コストに提供するとともに、多種多様な利用目的、利用形態に対し、より柔軟に素早くネットワークサービスを提供するという、2 つの相反する要求が高まっている。

前者に対しては光伝送技術の発展に期待するところが大きいが、この技術分野においては光デバイスレベルのブレークスルーが必要であり、ソフトウェアというよりはハードウェアの進化が必要と思われる。一方、後者に対しては、近年提案され検討が活性化している SDN/OpenFlow の適用が期待されている（図 1-1）。

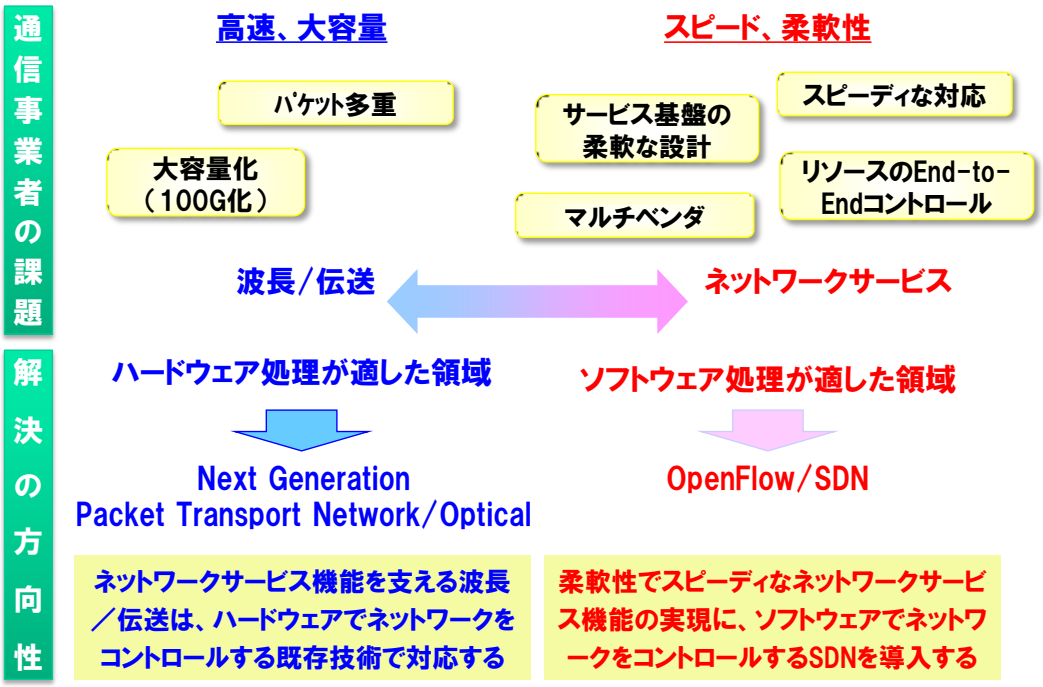


図 1-1　SDN に対する期待

第2節 本ガイドラインの位置付け

1. 概要・目的

本書は、ネットワーク仮想化技術の社会への普及と促進を目指し、SDN 技術を通信事業者のネットワークに適用するための指針や基本的な考え方について、ガイドラインとして体系的にまとめたものである。

- SDN を通信事業者のネットワークに適用するための指針や基本的な考え方を示す。
- 指針や基本的な考え方を解説することを目的とし、技術詳細や具体的な実施手順などを示すものではない。
- 従来のネットワーク技術については他書を参照するものとして最小限の記述に留め、本書では通信事業者のネットワークに SDN を適用するための「特有の事項」に着目して解説する。
- 想定読者は SDN を用いた通信事業者ネットワークの設計者、構築者、運用者とし、従来ネットワークに関する技術や SDN に関する基礎的な知識を有しているものとする。

2. 目次構成

本ガイドラインの目次構成と概要を表 1-1 に示す。

表 1-1　目次構成と概要

目次構成		要旨
第 1 編	概説	本ガイドラインの全体的な説明や前提条件などを示す。
第 1 章	はじめに	本ガイドラインの位置付けを明確にする。
第 2 章	SDN の基礎	SDN 技術を理解するための基礎的な知識として OpenFlow の概要を示す。
第 3 章	ネットワークモデル	本ガイドラインで対象とするネットワーク構成を示す。
第 4 章	ネットワーク・ユースケース	SDN を用いたネットワークのユースケースを示す。
第 2 編	設計・構築フェーズ	通信事業者の業務における設計・構築に関して、ネットワークに SDN を用いるための基本的な考え方を示す。
第 1 章	設計・構築フェーズの基本的な考え方	SDN 適用における設計・構築の基本的な考え方を示す。
第 2 章	SDN NW の設計・構築	ネットワーク階層における「SDN NW」の設計・構築の考え方について示す。
第 3 章	仮想 NW の設計・構築	ネットワーク階層における「仮想 NW」の設計・構築の考え方について示す。
第 4 章	本ガイドラインの基本的なネットワークモデル	第 2 章、第 3 章で示す設計・構築の考え方に基づき、基本的なネットワーク構成をモデルとして定義する。
第 5 章	情報の管理	システム設計等の参考情報として、通信事業者がネットワークサービスを提供するにあたり、管理すべき情報の例を示す。
第 3 編	運用・監視フェーズ	通信事業者の業務における運用・監視に関して、ネットワークに SDN を用いるための基本的な考え方を示す。

第 1 章	運用・監視フェーズの基本的な考え方	SDN 適用における運用・監視の基本的な考え方を示す。
第 2 章	運用・監視フェーズで使用する OAM ツール	ネットワークの効率的な運用・監視に必要となるツールについて、実現例を示す。
第 3 章	Point-to-Point 回線の運用・監視	Point-to-Point 回線の運用・監視として、開通試験・定期監視、異常措置の実施方法例を示す。
第 4 章	Drop 回線の運用･監視	Drop 回線の運用・監視として、開通試験・定期監視、異常措置の実施方法例を示す。
第 5 章	分岐回線の運用・監視	分岐回線の運用・監視として、開通試験・定期監視、異常措置の実施方法例を示す。
第 6 章	コントロールプレーンの運用・監視	コントロールプレーンの運用・監視として、SDN コントローラや監視制御網の、冗長化や定期監視について示す。
第 7 章	統計情報の活用	OpenFlow で取得できる統計情報を、運用・監視に活用するための基本的な考え方を示す。
第 4 編	付属資料	本ガイドラインに関連する補足情報などを示す。
第 1 章	用語の定義	本ガイドラインで定義した用語について整理する。
第 2 章	参照資料の一覧	本ガイドラインで参照した資料を一覧で示す。

第2章 SDN の基礎

第1節 SDN の概要

1. SDN が出てきた背景

近年、クラウド時代といわれるようになってから、インターネットのトラヒックの流れに変化が生じている。以前は PC (Personal Computer) 間においてファイル交換ソフトウェアなどによる Peer-to-Peer トラヒックの増大が課題であったが、最近では情報資源がネットワーク内のクラウドコンピューティング内に蓄積され、スマートフォン、タブレット端末などにより、ネットワークを介して情報資源にアクセスする Cloud-to-End の通信に変わってきている。典型的な例としては「YouTube」などによる映像コンテンツ配信がある。また最近では、企業内の業務システムを仮想サーバ環境で動作させるだけでなく、サービスとして提供されるクラウド上の仮想サーバで動作させる事例も一般的になりつつある。このようにクラウド上の多量な情報資源（ビッグデータ）がネットワークを介して端末に流れることになり、通信事業者としては、トラヒックの大容量化への対応と、変化の速いクラウド時代のトラヒックへの柔軟な対応の両方を同時に実現することが課題となっている。

ネットワーク装置については、従来から装置ベンダが提供するハードウェア／ソフトウェア一体型の市販製品が主流であり、通信事業者が独自にカスタマイズすることは困難であった。そのため通信事業者はベンダが決めた製品仕様に従いサービス展開を行う必要があった。つまり特定ベンダの技術に依存する状態（ベンダロックイン）であり、以下のような課題があった。

- ネットワーク装置で実現できることは、その装置が有している機能のみであるため､新機能が必要であればベンダに要望して機能追加してもらう必要がある。
- 機能追加には時間がかかることが多く、タイムリーなサービス提供ができない。
- 世界中で市販製品であるネットワーク装置を購入できるため、サービスとしての差別化が難しい。
- ネットワーク装置ベンダが異なれば、操作方法も異なり、運用が複雑になる。

このような状況の中で、ネットワーク装置における制御機能（Control Plane：C プレーン）と、パケット転送機能（Data Plane：D プレーン）を分離し、管理や制御機能をソフトウェアで実現することで、新しい機能などをカスタマイズし易いようにするという考えが出てきた。C プレーンと D プレーンの両プレーン間

をOpenFlowのような標準的なインタフェースで接続するという考えが広まってきており、現在ではデータセンタ、企業ネットワークなどを中心にSDN導入の検討が進んでいる。

2. SDNとは

SDN（Software-Defined Networking）とは、「ネットワークの構成、機能、性能などの制御をソフトウェアで動的に設定、変更するためのコンセプト（概念）」である。特徴は、ネットワークのトポロジ管理やルーティング、経路制御などを行うコントロールプレーン（Cプレーン）機能と、パケットフォワーディング（パケット転送）処理を行うデータプレーン（Dプレーン）機能を分離することにより、ネットワークサービスの迅速な提供と高度化をソフトウェアによるアプリケーションによって対応することである（図 1-2）。SDNは当初OpenFlowを中核とするネットワーク技術を表現するために使われ始めたが、現在では拡大解釈され、多様な意味合いで用いられている。

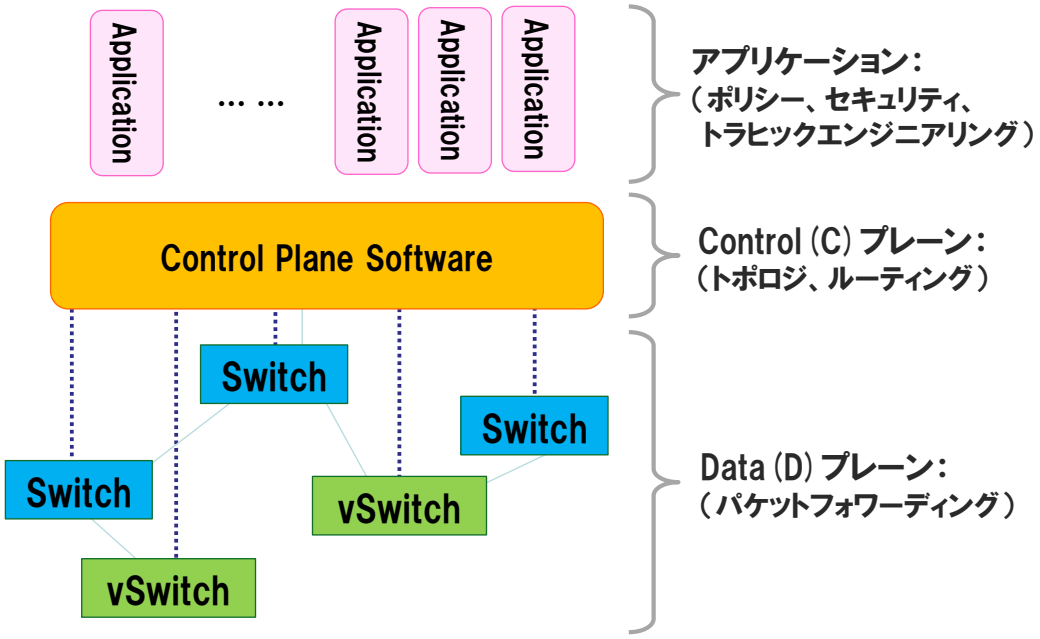


図 1-2　SDNの概念

3. OpenFlow

3.1. OpenFlow とは

OpenFlow は、SDN を実現する技術の 1 つであり、米国スタンフォード大学の研究からスタートし、現在は業界団体である ONF (Open Networking Foundation) が標準化を進めているネットワーク制御技術である。

OpenFlow では、OpenFlow コントローラ（以降は「OFC」と略す）と OpenFlow スイッチ（以降は「OFS」と略す）によりネットワークが構成され、OpenFlow コントローラは複数の OpenFlow スイッチを一元管理し、経路計算や受信したパケットの振る舞いの指示などを行う。この OpenFlow コントローラと OpenFlow スイッチの間で情報をやり取りするためのプロトコルが OpenFlow となる。

OpenFlow スイッチは、受信したパケットをどう処理するかを定義した「フローテーブル」に基づき処理を行う。フローテーブルには、「Match Fields に適合したパケットを Instructions に従い処理する」という内容が記述されている（フローエントリ）。このフローテーブルは、OpenFlow コントローラからの指示で情報の追加、削除、変更が可能である（図 1-3）。

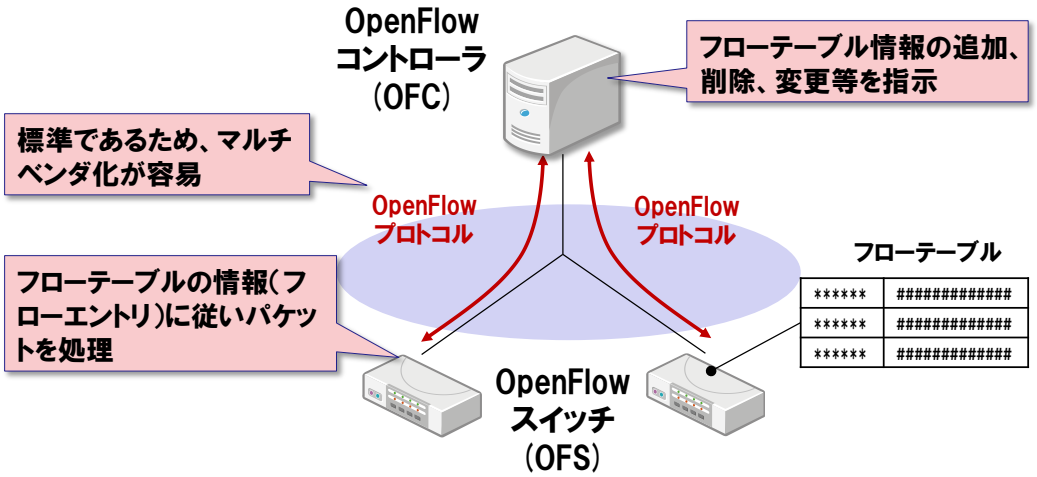


図 1-3　OpenFlow コントローラと OpenFlow スイッチ

フローエントリには、「Match Fields」など 6 種類の情報が含まれており、これらの情報を組み合わせて、受信したパケットの処理方法を決定する。OpenFlow スイッチはパケットを受信した際に、ヘッダ情報を確認してどのフローエントリ

の「Match Fields」に一致するかを判断する（以降は Match Fields で規定された条件を「Match 条件」と略す)。一致した場合に、そのフローエントリの「Instructions」が指定する処理を実行する。フローテーブルを構成するフローエントリの内容を表 1-2 に示す。

表 1-2　フローテーブルを構成するフローエントリの内容

要素	意味
条件 (Match Fields)	パケット受信時にフローテーブルを検索するためのキー。
優先度 (Priority)	Match Fields に合致するフローエントリが複数存在した場合の優先順位。値が大きい方を優先する。
統計情報 (Counters)	同じフローエントリに一致したパケット数、バイト数、フローエントリが書き込まれてからの時間等。
処理 (Instructions)	Match Fields に合致した場合の処理方法を指定する。
有効時間 (Timeouts)	フローエントリが消滅するまでの時間。
クッキー (Cookie)	コントローラがフローエントリを管理するための値。

3.2. パケット処理方法

パケットの処理方法に着目すると、OpenFlow は「プロアクティブ型」と「リアクティブ型」の方式に分類される。

プロアクティブ型は、OpenFlow コントローラは処理すべきパケットのフローエントリを OpenFlow スイッチのフローテーブルに事前に書き込んでおく方式である。OpenFlow スイッチはフローテーブルに該当するパケットを受信した場合にフローエントリに従いパケットの処理を行い、フローテーブルに該当しないパケットを受信した場合にはパケットをそのまま廃棄する（図 1-4)。

本方式では、事前に OpenFlow スイッチにフローエントリを書き込むため、パケット受信の都度、OpenFlow コントローラに処理を問い合わせる必要がなく、

問い合わせによるオーバヘッドの削減というメリットがある。一方で必要なフローエントリを全て登録しておく方式のため、例えば大量のフローエントリを設定する必要がある場合には、フローテーブル数が足りなくなるという課題もある。

リアクティブ型は、フローエントリを事前に登録せず、パケット受信時に OpenFlow コントローラにパケットを転送（Packet-In：パケットイン）して処理方法を問い合わせる方式である。問い合わせを受けた OpenFlow コントローラは、処理すべきパケットであれば該当するフローエントリを OpenFlow スイッチに書き込む。OpenFlow スイッチにフローエントリが書き込まれた後は、同様のパケットを受信した際にはフローエントリに従い処理を行う。また処理すべきパケットでない場合は、OpenFlow コントローラへパケットインされた際にそのまま廃棄される（図 1-5、図 1-6）。

本方式では、OpenFlow コントローラに対する問い合わせが頻繁に発生することになるが、フローエントリを一定時間で消去（エージング）することで、フローテーブルを有効活用できるというメリットがある。

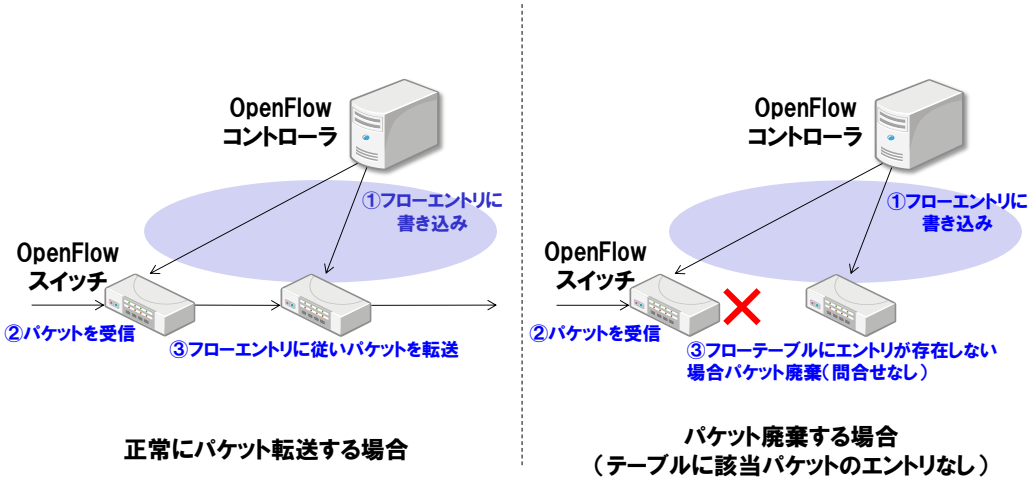


図 1-4　プロアクティブ型動作

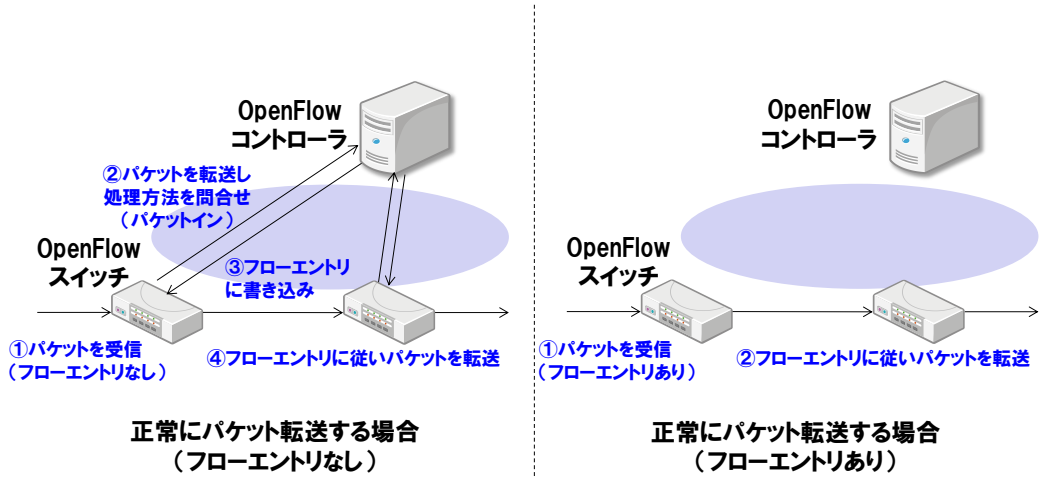


図 1-5　リアクティブ型動作（正常転送）

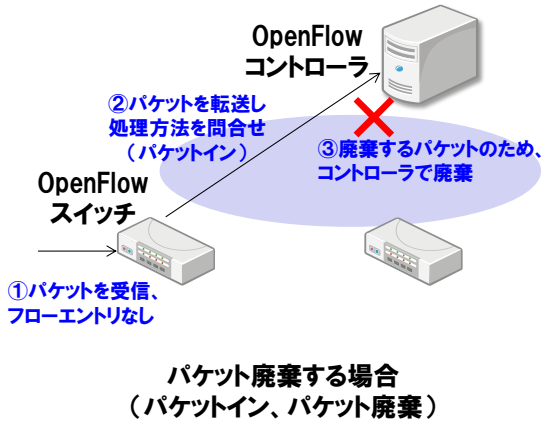


図 1-6　リアクティブ型動作（パケット廃棄）

3.3. パケットの流れる経路

パケットの流れる経路に着目してみると、OpenFlow の動作により、4 つのパタン（A～D）に整理できる（図 1-7）。従来のパケット転送と比べてパケットの流れが複雑になるため、通信事業者にとっては運用の工夫が必要になるが、従来にはないような様々な新しいサービスの可能性が考えられる。

A) Output（指定されたポートからパケットを送出する）によりフローテーブルに指定された経路を流れる

B) Packet-In（パケットイン：コントローラにパケットを送信し処理を問合せる）や Packet-Out（パケットアウト：指定ポートからパケット送出を指示する）によりコントローラを介して流れる

C) Drop（パケットを廃棄する）により廃棄される

D) Group テーブル（グループ毎に Actions を指定した情報）により分岐する

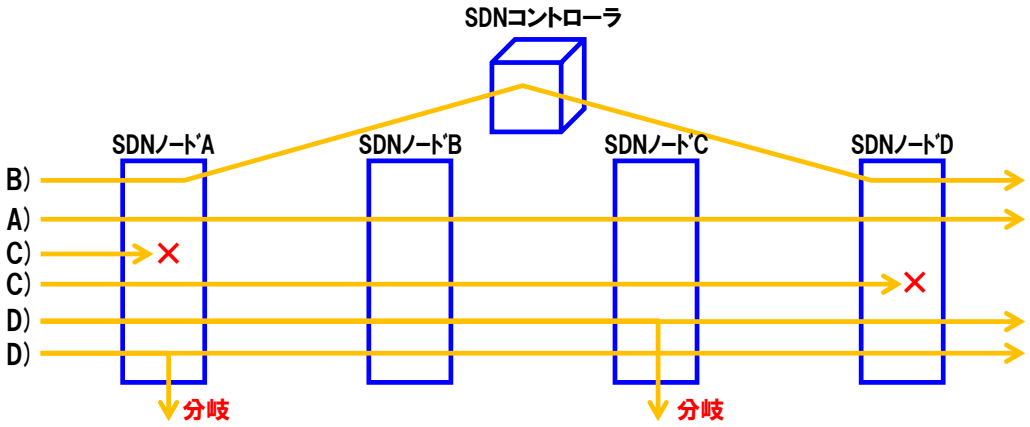


図 1-7　パケットが流れる経路

4. SDN の構成要素

SDN を構成する要素は、大きく 3 つに分類できる（図 1-8）。

1 つめは、パケット転送を担う「SDN ノード」である。SDN ノードは、専用ハードウェアで構成される物理スイッチやソフトウェアで動作する仮想スイッチがある。従来のパケット転送装置との違いは、SDN コントローラからの制御によって動作する点である。2 つめは、SDN ノードの制御や管理を行う「SDN コントローラ」である。3 つめは、SDN コントローラの上位で、ポリシー制御やトラヒック制御など、各種機能を実現する「ネットワークアプリケーション」である。

また、SDN の構成要素の上位には、SDN ネットワークやクラウドネットワーク、既存ネットワークなど、複数のコントローラの管理や制御を行うオーケストレータがあり、各コントローラと連携を行う。

各構成要素の詳細については次節で述べる。

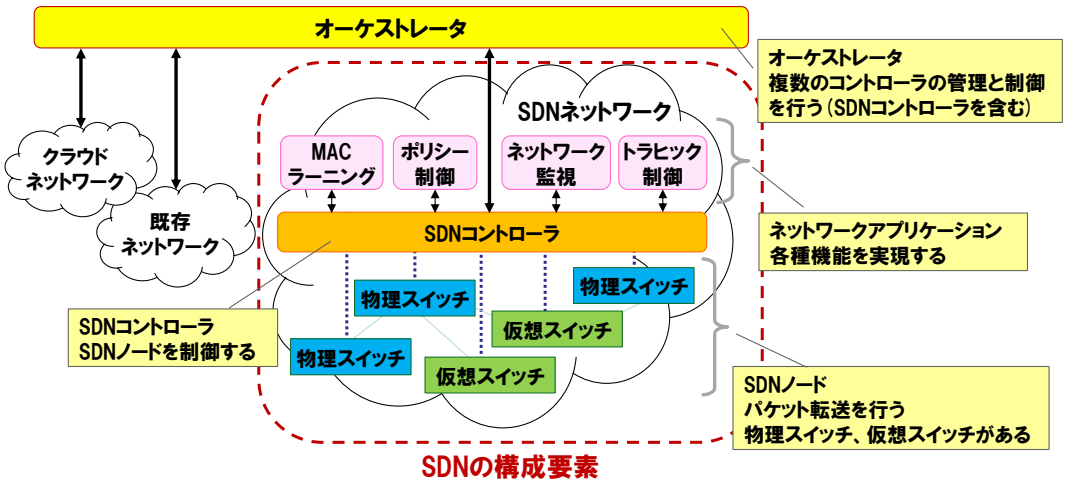


図 1-8　SDN の構成要素

従来ネットワークと SDN を用いたネットワークの運用面での違いは、従来ネットワークでは、ネットワーク技術者がネットワーク全体を見通した上で設計し、それに応じて各装置に個別の設定を行うことで、ネットワーク全体の整合性を保っていた。一方、SDN を用いた場合では、ネットワーク全体を制御するソフトウェアを用意し、そのソフトウェアにより全ての装置を制御するという考

え方である。ソフトウェアを利用してパケット転送を制御し、各装置を集めたネットワーク全体を一つの単位として一括で制御を行う。

第2節 SDN の構成要素

1. SDN ノード

SDN ノードは、実際のパケット転送を担う装置である。この SDN ノードは、専用ハードウェアで構成される物理スイッチと汎用ハードウェア等の上のソフトウェアで動作する仮想スイッチがある。仮想スイッチはサーバ仮想化ソフトウェアの中に含まれていることが多い。この SDN ノードの制御には、OpenFlow やベンダ独自の API (Application Programming Interface) が利用される。

物理スイッチは、NEC などの多数のベンダにより提供されている。

仮想スイッチは OpenFlow 等に対応した仮想スイッチソフトウェアであり、装置構成やカスタマイズに柔軟性がある。この仮想スイッチには「Open vSwitch」や O3 プロジェクト[1]の「Lagopus（ラゴパス)」などがある。Lagopus は、広域ネットワークでの利用を目指し、OpenFlow の最新の安定版仕様である OpenFlow バージョン 1.3.4 に幅広く準拠した高性能な SDN ソフトウェアスイッチであり、オープンソースソフトウェアとして 2014 年 7 月に公開されている。特徴はマルチコア CPU のような近年のサーバアーキテクチャの特徴を効率的に利用するパケット処理の実装と、I/O 性能を高速化する Intel DPDK の技術を利用することで、広域ネットワークで要求される大規模・広帯域な通信処理を可能とする、100 万フロー制御ルールのサポートや 10Gbps の通信性能を実現していることである。

また、最近ではホワイトボックススイッチを利用するケースも増えてきている。従来ネットワーク装置ベンダはハードウェア（筐体や基板）とソフトウェア（OS 等）を一体化した製品を販売してきた。ホワイトボックススイッチとは、スイッチのハードウェア部分のみの製品を指し、スイッチに搭載する OS やアプリケーションといったソフトウェア部分は、スイッチを使うユーザが自ら選んで導入する（Open Network Linux 等）、もしくは自社で開発したものを利用することができる（図 1-9）。

このホワイトボックススイッチの利用例としてはクラウドサービス事業者がある。大規模クラウドサービス事業者は、大量のネットワーク装置を必要としており、装置導入コストは膨大なため、これを抑制する必要がある。そこで

[1]世界初の広域 SDN (Software-Defined Networking) 実現を目指す研究開発プロジェクト。NEC、日本電信電話株式会社、NTT コミュニケーションズ、富士通、日立製作所が参画。（http://www.o3project.org/ja/index.html）

ODM (Original Design Manufacturing)[2] ベンダに自社で利用するホワイトボックススイッチの製造を依頼し、そこに OSS (Open Source Software) 等のソフトウェアを搭載して利用することで、既存スイッチに比べて導入コストを下げつつ、サービスに必要なネットワーク機能を追加して運用を行っている。ホワイトボックススイッチの特徴を以下に挙げる。

- コストが安い
- ベンダロックインの回避が可能
- 迅速なサービス提供
- カスタマイズの柔軟性

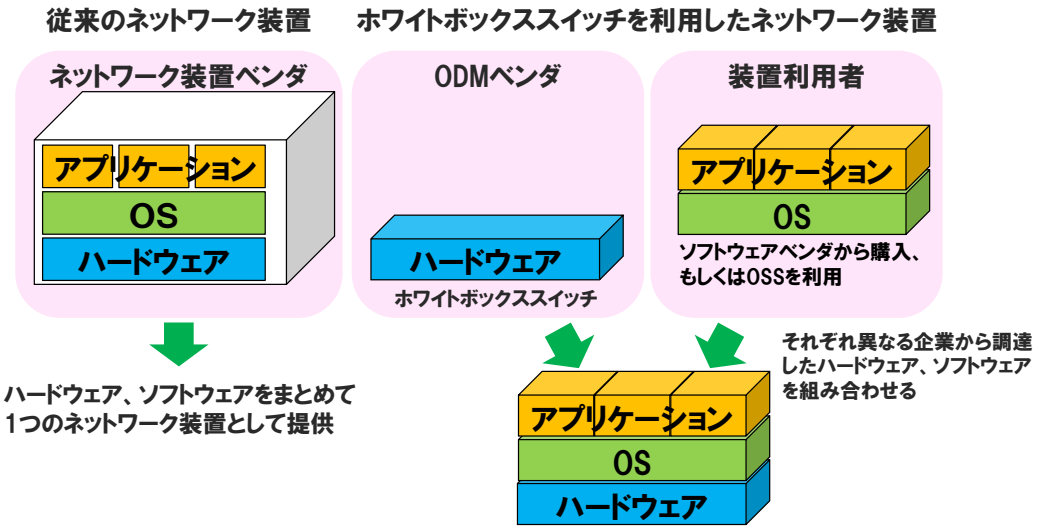


図 1-9　ホワイトボックススイッチを利用したネットワーク装置

[2]汎用部品を組み合わせて設計・製造、販売を行うこと。

2. SDN コントローラ

SDN コントローラは、パケット転送を担う SDN ノードであるスイッチ群が、どのようにパケットを処理するかを管理・制御するソフトウェアである。SDN コントローラは、ベンダや企業が開発を行う商用版と OSS コミュニティ等で開発されるものがある。

SDN コントローラからスイッチ群を制御するための API は、サウスバンド API とも呼ばれており、OpenFlow やベンダ独自の API が使われている。

SDN コントローラには、NTT 研究所が開発したオープンソースコントローラである「Ryu」や、米 Linux ファウンデーションのオープンソースコントローラである「Open Daylight」等がある。

Ryu (Ryu SDN Framework) とは、NTT 研究所開発のオープンソースコントローラであり、OpenStack の開発と同じプログラム言語である Python で書かれている。また、OpenFlow バージョン 1.0、1.2、1.3、1.4 に対応しており、OpenStack との連携が可能である（図 1-10)。

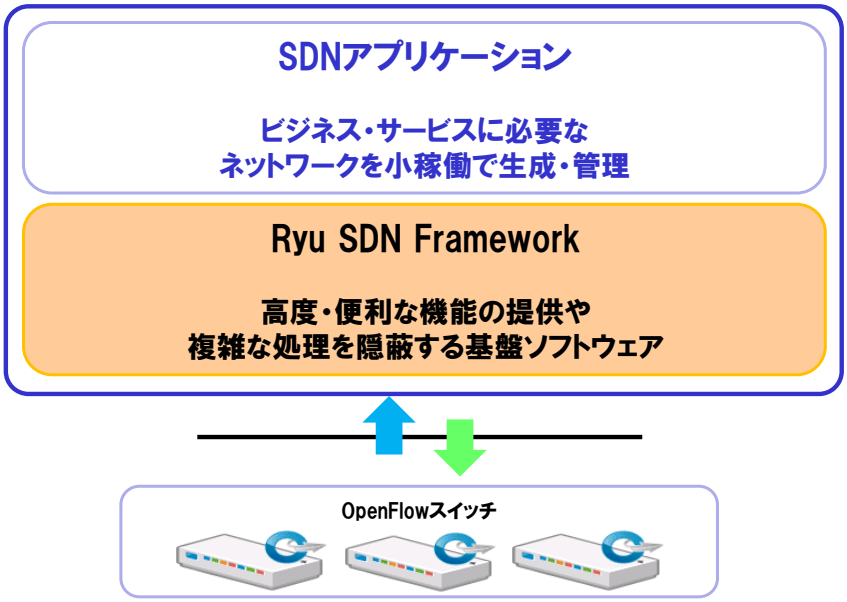


図 1-10　SDN コントローラ「Ryu SDN Framework」

3. ネットワークアプリケーション

ネットワークアプリケーションは、SDN コントローラの上位で動作し、経路計算やネットワーク監視、トラヒック制御などの機能を実現するアプリケーションである。各種制御機能や付加機能を導入する場合、SDN では専用のハードウェアを準備することなく、ネットワークアプリケーションとしてプログラミングを行うことで柔軟に実現できる。その反面、利用者が自らソフトウェアを準備する必要があり、MAC アドレスラーニングやパケット経路計算のような基本的な機能についても、利用者が自らソフトウェアを準備する必要がある。

第3節 オーケストレータ

現在の IT システムは、ネットワークだけでなく、ストレージやサーバなど複数の装置で構成される大規模なシステムとなりつつある。そのため制御対象を分割し、ネットワークを制御する「ネットワークコントローラ」、クラウドを制御する「クラウドコントローラ」など、大規模 IT システムにおいて制御の範囲毎に複数のコントローラが存在することが多い。また冗長化構成のため同一種類で複数のコントローラが存在することもある。そのため、これら複数のコントローラを含むシステム全体を管理し制御するソフトウェアが必要となり、これは「オーケストレータ」と呼ばれている（図 1-11）。

オーケストレータとネットワークアプリケーション、オーケストレータと SDN コントローラとのインタフェースはノースバウンド API とも呼ばれ、現在は各ベンダ等が独自の API を提供していることが多い。

オーケストレータには、仮想サーバと仮想ネットワークを管理・制御することができるオープンソースソフトウェアである OpenStack のオーケストレーション機能である「Heat」や「CloudStack」などがあり、他にもデータセンタ等を運営する事業者が開発するケースもある。

ネットワークを管理するオーケストレータの例としては、O3 プロジェクト等で NEC が提供する SDN プラットフォームである「OdenOS (Object-Defined Network OS) 」があり（図 1-12)、オープンソースソフトウェアとして公開されている[3]。この OdenOS は、既存のネットワークをトポロジー（ノード、ポート、リンク）とフロー（End-to-End の通信）に抽象化したモデルで表現するネットワークを管理する「ネットワークオーケストレータ」であり、パケットトランスポートノードや光トランスポートノードを抽象化して制御することが可能である。また SDN コントローラ機能も有している。

[3] http://www.o3project.org/ja/download/index.html ［O3 プロジェクト ダウンロード］

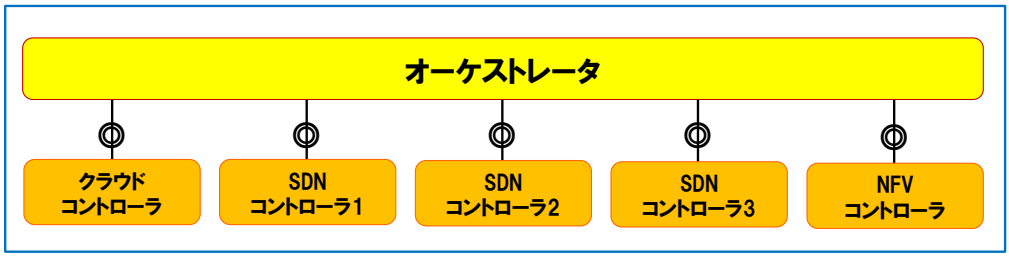


図 1-11　オーケストレータのイメージ

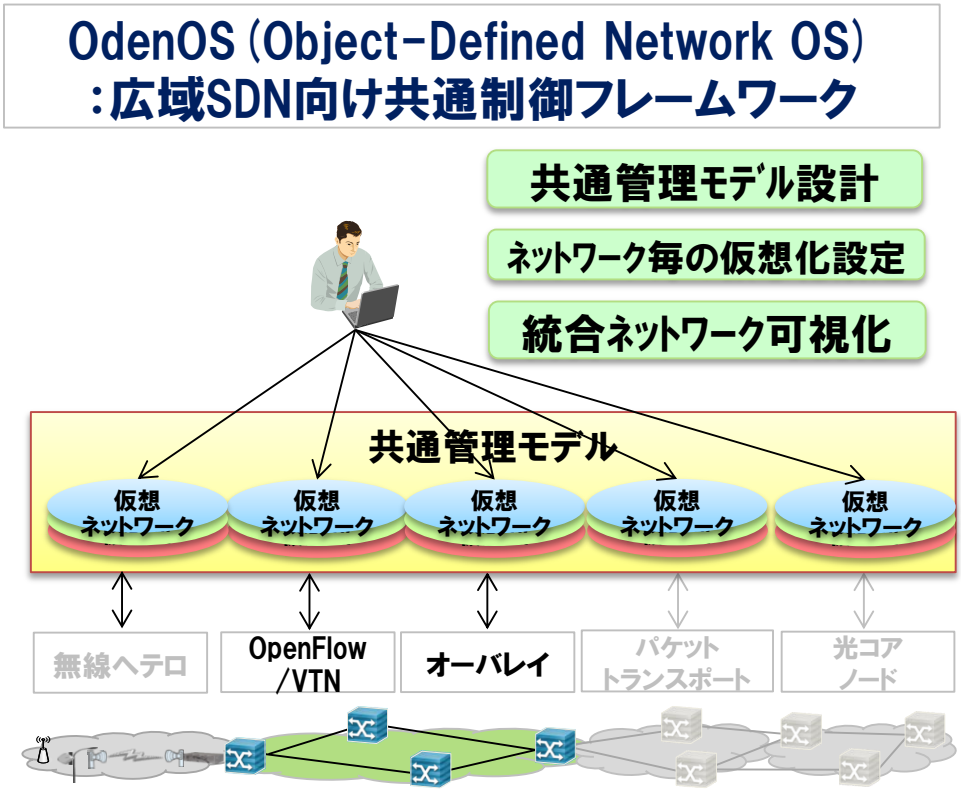


図 1-12　OdenOS イメージ

第4節 SDN の適用方式

1. OpenFlow の適用方式

OpenFlow を前提として SDN を適用する場合には、「ホップ・バイ・ホップ（Hop by Hop）方式」と「オーバレイ（Overlay）方式（トンネル方式)」と呼ばれる二つの方式がある。

2. ホップ・バイ・ホップ（Hop by Hop）方式

ホップ・バイ・ホップ方式は、ネットワーク上の全てのスイッチを OpenFlow 対応とし、コントローラが全てのスイッチを OpenFlow で管理する方式である。OpenFlow コントローラが経路を計算し、OpenFlow プロトコルを利用して各 OpenFlow スイッチに経路情報を配布することで､ネットワークの制御を行う(図 1-13）。

全てのネットワーク機器を OpenFlow に対応させる必要があるため、初期費用の観点等から導入のハードルは高くなるが、OpenFlow によってネットワーク機器毎にきめ細かい制御ができる利点がある。

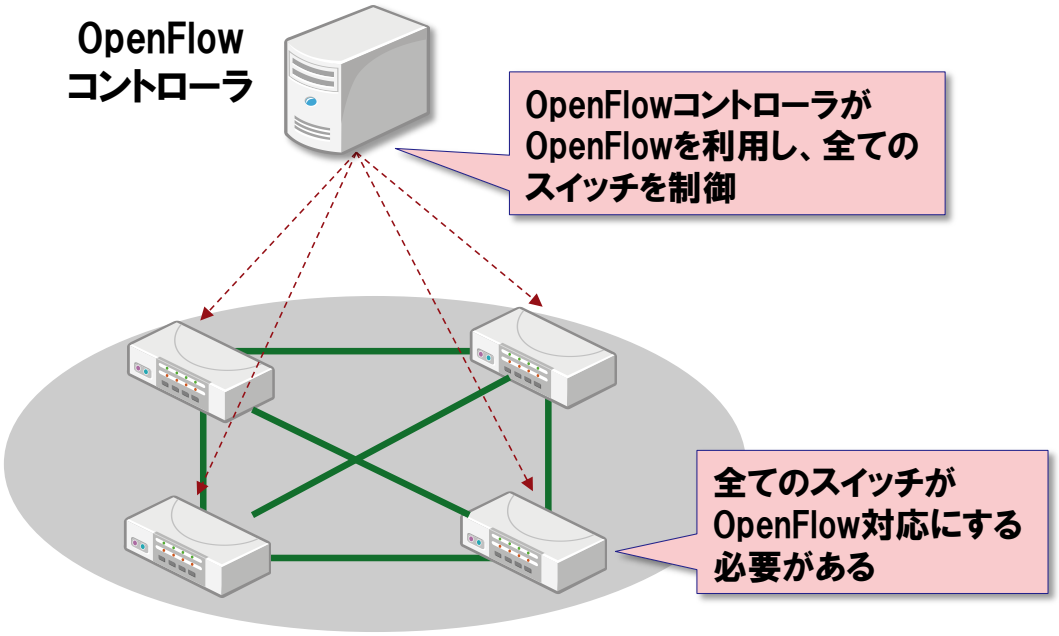


図 1-13　ホップ・バイ・ホップ方式

3. オーバレイ（Overlay）方式（トンネル方式）

オーバレイ方式は、全ての機器を OpenFlow 対応スイッチにするのではなく、ネットワークのエッジに配置されたスイッチ（エッジスイッチ、主に仮想スイッチ）のみを OpenFlow コントローラが OpenFlow で制御し、エッジスイッチ間の通信はトンネリングプロトコル[4]を利用して仮想的に直接接続する（図 1-14）。

既存のネットワーク機器を活かすことができる利点があるが、物理スイッチ側からはトンネル内部のフレームを関知できないため、End-to-End での負荷分散や帯域制御、監視などは難しいという課題がある。

[4] GRE (Generic Routing Encapsulation) 、VXLAN (Virtual Extensible LAN) 、NVGRE (Network Virtualization using GRE) 等がある。

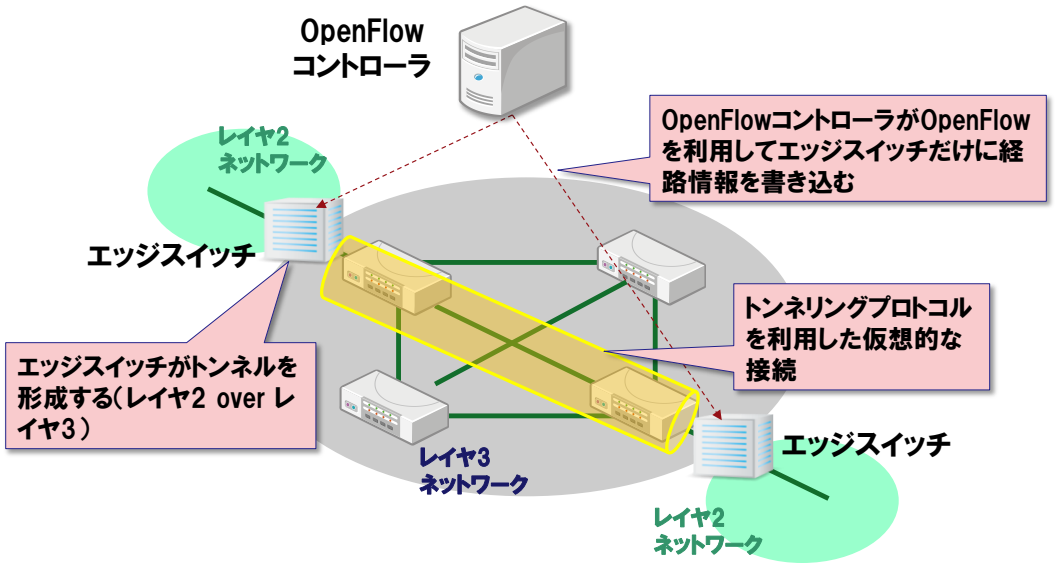


図 1-14　オーバレイ方式

4. 適用方式の比較

ホップ・バイ・ホップ方式とオーバレイ方式の比較を表 1-3 に示す。

表 1-3　ホップ・バイ・ホップ方式とオーバレイ方式の比較

方式	既存スイッチの活用	コントローラによる管理	初期コスト
ホップ・バイ・ホップ	既存スイッチ（OpenFlow 未対応）は使用不可のため、全てを OpenFlow に対応させる必要がある。	・ 全ての OpenFlow スイッチを管理する必要がある。 ・ ネットワーク上で粒度の細かい多様な制御が可能。	大規模ネットワークの場合、全てのスイッチを OpenFlow 対応にする必要があるため、初期コストがかかる場合がある。
オーバレイ	既存ネットワーク装置を利用し、エッジスイッチ（仮想マシン直近スイッチ）のみ OpenFlow に対応させればよい。	仮想スイッチ（エッジスイッチ）と仮想ネットワークの対応関係のみを管理すれば良い。	既存設備を活かし、エッジスイッチのみを OpenFlow 対応とすることで実現可能。

第3章 ネットワークモデル

第1節 通信事業者の一般的なネットワーク

1. 従来のネットワークモデル

通信事業者の一般的なネットワーク構成を図 1-15 のモデルに示す。

図 1-15 通信事業者の一般的なネットワークモデル

ネットワークの全体構成を区間と機能などで整理し、構内／イントラネット、アクセスネットワーク、中継ネットワーク、DC（データセンタ）内ネットワークで構成されたモデルで表す。通信事業者として直接管理を行うアクセスネットワークと中継ネットワークに加え、ユーザにネットワークサービスを提供するという観点から、構内／イントラネットと DC 内ネットワークを含めて考える。なお、通信事業者のアクセスネットワーク、中継ネットワークは、各々、他社の異なるネットワーク（異なるドメイン）にて構成される場合もある（通信事業者間接続）。

2. 構内／イントラネット

構内／イントラネットはユーザ宅内のネットワークである。基本的には各ユーザにて管理され、通信事業者と契約して広域ネットワークと接続することで、ネットワークサービスの提供を受ける。

3. アクセスネットワーク

アクセスネットワークは中継ネットワークと構内／イントラネットを接続するネットワークである。主な特徴として以下が挙げられる。

- アクセスポイントからユーザ宅内までが該当し、通信事業者のネットワークへユーザを収容する。
- ユーザの利用する各種ネットワークサービスを多重する。
- 有線、無線、インターネットなどの多様な通信手段との相互接続を行う。
- アクセスサーバやルータなどの多様な設備で構築される。

4. 中継ネットワーク

中継ネットワークは通信事業者間やISP（Internet Service Provider）を接続する通信事業者の基幹ネットワークである。主な特徴として以下が挙げられる。

- アクセスネットワークの回線を収容・集線してユーザを多重する。
- 各種ネットワークサービスを多重し、またサービス別のネットワークに振分けを行う。
- 長距離・大容量のパスでトラヒックを集約して高速大容量伝送を行う。
- 地理的に広がった構成をとる。
- 経路冗長や切替え機能を有して高信頼のネットワークを実現する。

5. DC 内ネットワーク

昨今のDC内ネットワークは拡大を続け、サーバ／ストレージの仮想化技術を活用したクラウドデータセンタが主流になり、主にクラウドサービス事業者により管理される。主な特徴として以下が挙げられる。

- １つのサーバ上に多数の仮想サーバが生成できるため、ネットワーク規模が膨大である。

- 仮想サーバのインスタンスが動的にネットワークを移動するため、ネットワークの柔軟な運用が必要である。
- CMS (Cloud Management System) と連携して、各種クラウドサービスを提供する。

第2節 SDN を適用した通信事業者ネットワーク

1. SDN を用いたネットワークモデル

本ガイドラインで想定する SDN を用いた通信事業者のネットワークのモデルを図 1-16 に示す。前提としては既設の L2/L3 ネットワークの存在に捉われず、SDN 技術を適用したネットワークを新規に構築する立場で考えるものとし、SDN の適用方式としてはホップ・バイ・ホップ型と呼ばれる構成に分類される。

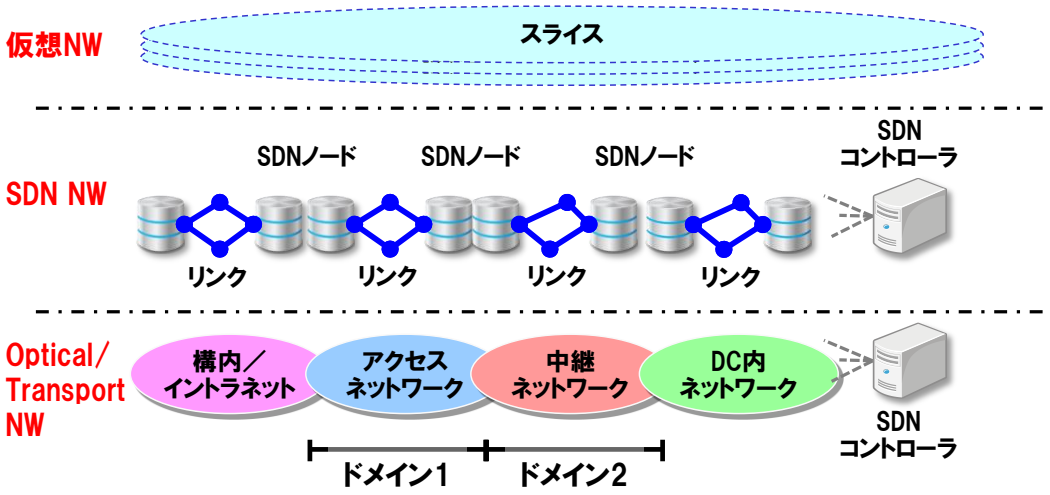


図 1-16　SDN を用いたネットワークモデル

伝送レイヤと SDN ノード及び仮想ネットワークの 3 階層からなる構成で考え、各々を「Optical/Transport NW」、「SDN NW」及び「仮想 NW」と呼ぶネットワーク階層として定義する（表 1-4）。

表 1-4　ネットワーク階層の概要

ネットワーク階層	概要
仮想 NW	SDN NW 上に構成される L2 以上の論理ネットワーク。
SDN NW	SDN ノードと、SDN ノード間のリンクで構成され、SDN コントローラから制御されるネットワーク。
Optical/Transport NW	SDN ノード間にリンクを提供するネットワーク。

「Optical/Transport NW」は、SDN ノード間にリンクを提供するネットワークである。SDN の仕組みを取り入れ、「Optical/Transport NW」リソースを抽象化して SDN コントローラからの制御を可能とした場合を「トランスポート SDN」と呼ぶ。

「SDN NW」は、SDN ノードと、SDN ノード間のリンク（論理リンク）で構成され、SDN コントローラから制御されるネットワークである。

「仮想 NW」は、SDN NW 上に構成される L2 以上の論理ネットワークであり、論理ネットワークで用いるリソースの単位を「スライス」と呼ぶ。

1.1. ネットワークの階層構造

図 1-16 に示す SDN を用いたネットワークモデルについて、ネットワークの階層構造に着目して詳細に示す。

「Optical/Transport NW」は Optical と Packet Transport により伝送レイヤを構成する。Optical は光ノードと物理リンクから構成され、Packet Transport に対して波長パスを提供する。Packet Transport は PTN (Packet Transport Network) ノードと論理リンクから構成され、「SDN NW」に対してパスを提供する。

「SDN NW」は SDN ノードと論理リンクから構成され、論理リンクは「Optical/Transport NW」から提供されるパス／波長パスを用いて（ホップ・バイ・ホップ方式の場合)、「仮想 NW」を構成する（図 1-17)。

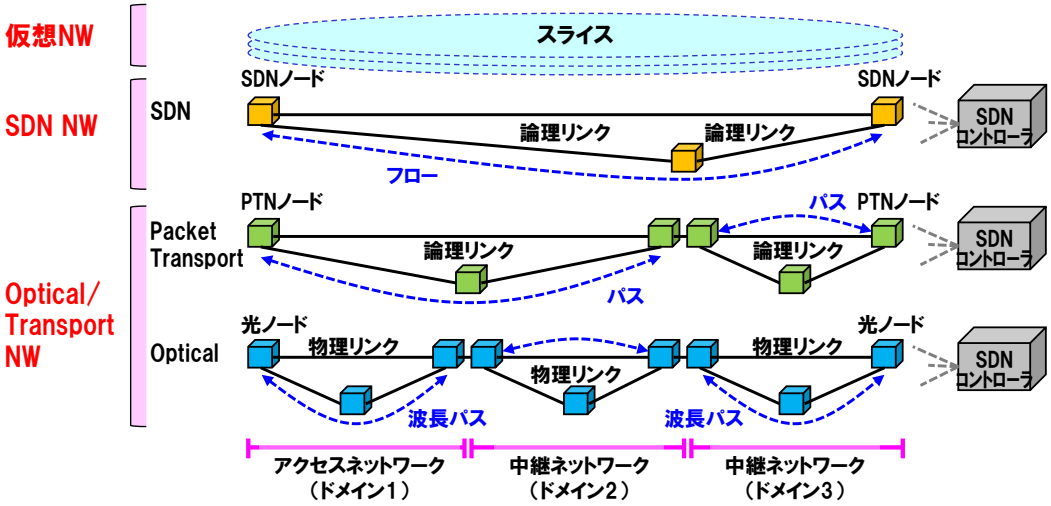


図 1-17　ネットワークの階層構造

リンクの構造に着目すると、SDN ノード-SDN ノード間の SDN 用のリンクは、パケットトランスポート用のリンク、WDM (Wavelength Division Multiplex) 用のリンクの入れ子構造で構成される（図 1-18）。

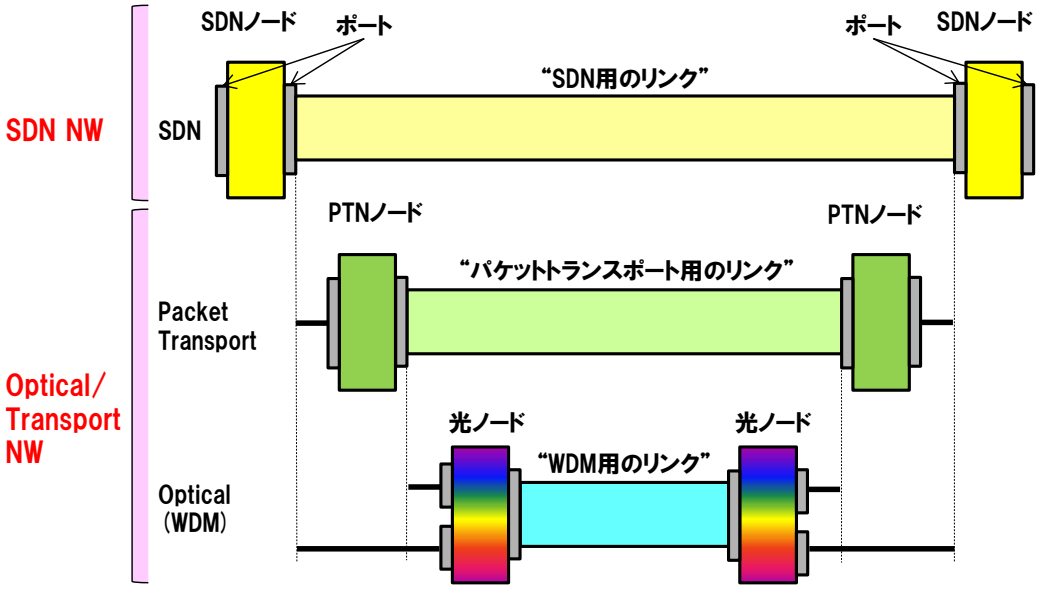


図 1-18　リンクの階層構造

1.2. コントロールプレーンとデータプレーン

「SDN NW」は、ネットワーク制御を担うコントロールプレーンと、パケット転送を担うデータプレーンが分離したアーキテクチャをとる(詳細は第1編第2章 SDNの基礎)。コントロールプレーンはSDNコントローラと監視制御網で構成され、データプレーンはSDNノードと論理リンクで構成される（図 1-19)。

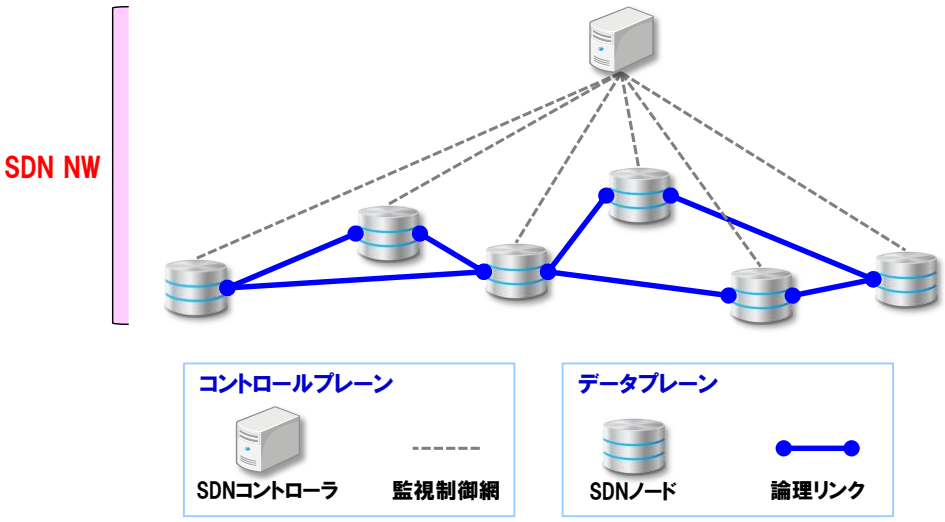


図 1-19　コントロールプレーンとデータプレーン

1.3. スライスの概要

「仮想NW」を構成するスライスは、物理ネットワーク（SDN NW、Optical/Transport NW）のリソースを分割したものであり、各種ネットワークサービスを提供するためのフローは、スライスのリソースを使用して設定される（図 1-20)。スライスは提供するネットワークサービス単位やユーザ単位など、目的や用途、規模などに応じて設定するものである。

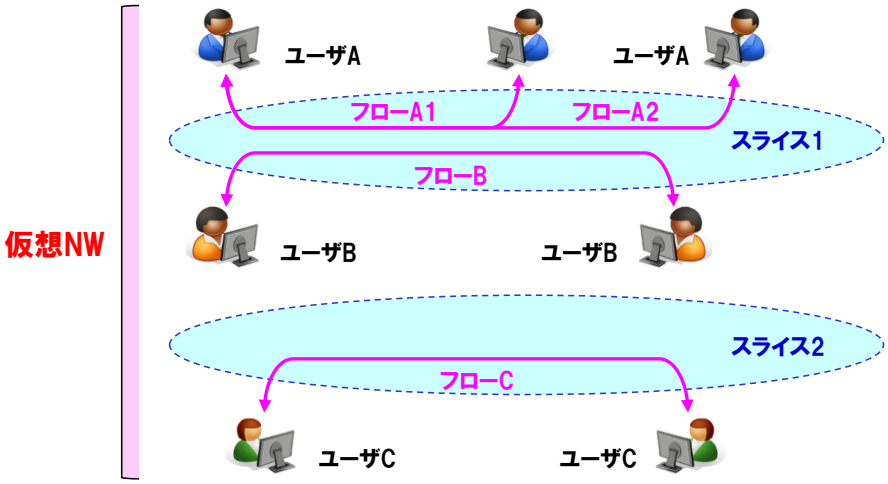


図 1-20　スライスのイメージ

2. ネットワーク管理モデル

SDN を用いた通信事業者のネットワークでは、マルチレイヤ、マルチドメインの多様な構成が想定される。このようなネットワークを制御し、さらにクラウド技術や NFV (Network Functions Virtualization) と組み合わせて新しいサービスを機動的に提供するための管理システムの構成例を図 1-21 に示す。この例では階層毎、ドメイン毎に SDN コントローラを配備し、分散的な制御を行っている。これにより各階層／ドメインで要求される機能、性能を個々のコントローラで個別に開発、維持管理が可能となる。各コントローラを束ねるオーケストレータをその上位に配備することで、ネットワークの End-to-End の制御が可能となる。オーケストレータはクラウド資源や NFV で用いられる網機能資源を提供するアプリケーションを制御するコントローラも束ねて管理している。このような構成では、例えばクラウド資源とネットワーク資源を組み合わせてネットワークサービスを提供する場合、それを実現するアプリケーションはオーケストレータの API (Application Programming Interface) を利用するアプリケーションを実装することになる。

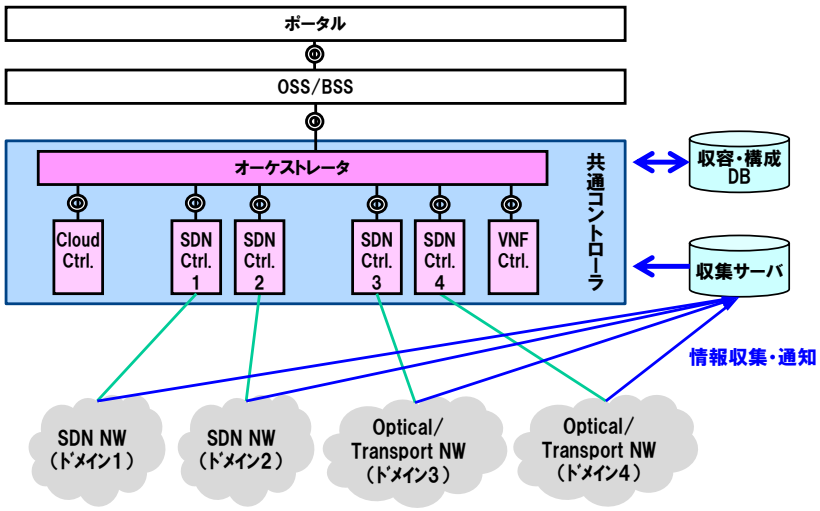


図 1-21　ネットワーク管理モデルの例

この例ではオーケストレータは複数の SDN コントローラを管理することとなり、プログラムが複雑化することが懸念される。それを回避する策として、図 1-22 に示すようなネットワークコントローラを中間に配備し、ネットワーク資源の管理、抽象化、さらには制御用の API 機能を配備することが有効と考えられる。O3 プロジェクトで開発を進めているネットワークコントローラとして「OdenOS」がある。

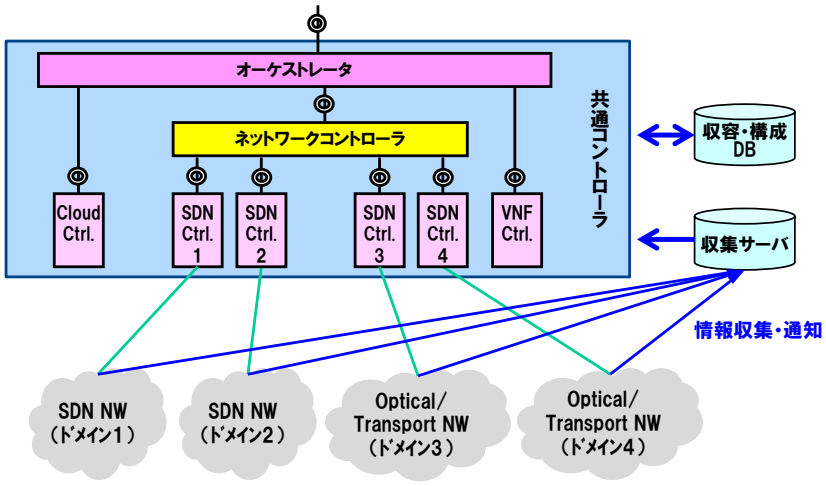


図 1-22　ネットワークコントローラの例

第3節 ネットワークモデルと本ガイドラインの対象

本ガイドラインで対象としている SDN を用いたネットワークについて、図 1-16 のモデルを用いて示す。

本ガイドラインでは通信事業者が管理する中継ネットワーク、アクセスネットワークに関して、「仮想 NW」、「SDN NW」及び「Optical/Transport NW」を制御している SDN コントローラを想定して解説している（図 1-23）。

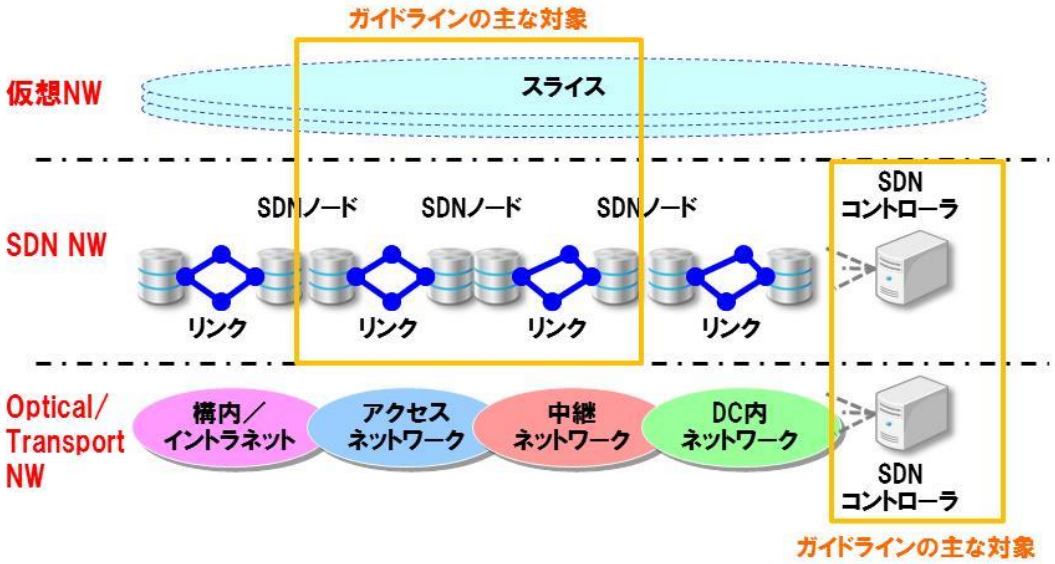


図 1-23　ネットワークモデルと本ガイドラインの対象

第4章 ネットワーク・ユースケース

第1節 ユースケースの概要

本ガイドラインで示すユースケースでは、Point-to-Point の回線サービスを想定する。通信事業者はユーザからネットワークサービスの利用申込を受け、ユーザの 2 ヶ所の拠点間を通信事業者のネットワークで結び、End-to-End の回線接続を提供する。対象とするネットワークは、通信事業者が管理する中継ネットワークとアクセスネットワーク、そしてユーザが管理する構内／イントラネットで構成される（図 1-24）。

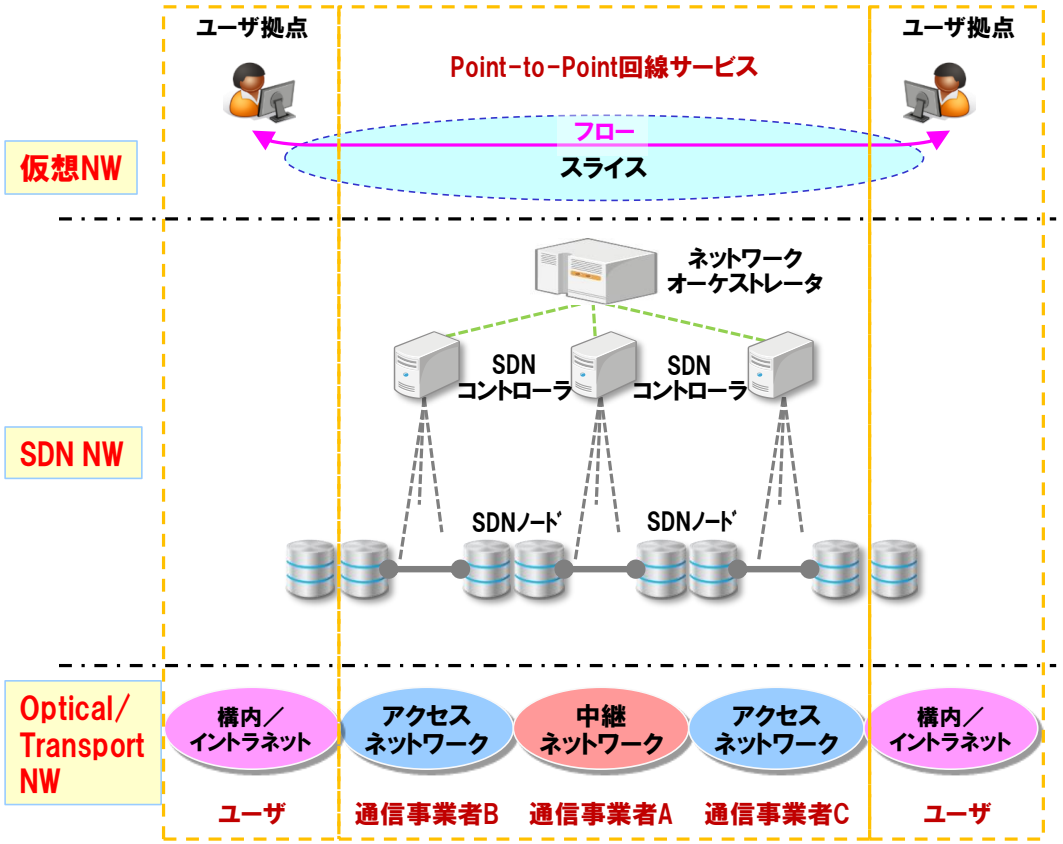


図 1-24 ユースケースの概要

回線サービスを提供する通信事業者 A は、中継ネットワークを管理しているものとする。ユーザの網内／イントラネットを接続するアクセスネットワークは一

方を通信事業者 B、もう一方を通信事業者 C とし、異なる通信事業者（異なるドメイン）によって管理されている。

各通信事業者が管理する中継ネットワーク、アクセスネットワークでは、SDN ノードからなる「SDN NW」が構築され、各通信事業者の SDN コントローラによる制御が可能である。また各通信事業者の SDN コントローラを統合的に制御するネットワークオーケストレータが配備され、通信事業者 A はネットワークオーケストレータを介して、ネットワークの End-to-End の制御が可能な構成とする。

「仮想 NW」では回線サービスを提供するための、ユーザ拠点間を結ぶフローが設定される。

第2節 SDN NW の設計・構築

「SDN NW」の設計・構築について示す。通信事業者 A は、通信事業者 B、C 及びユーザ拠点に SDN ノードを設置し、ホップ・バイ・ホップ方式にて「SDN NW」を構成するものとする（図 1-25）。

- 通信事業者 A は、アクセスネットワークを提供する通信事業者 B、C のコロケーションサービスを利用して SDN ノードを設置し、パスを調達する。
- 各ドメインの SDN ノードに対応する SDN コントローラ（コントローラ A、B、C）及びネットワークオーケストレータより、ネットワークの制御を行う。
- ユーザ拠点に SDN ノードを設置する。

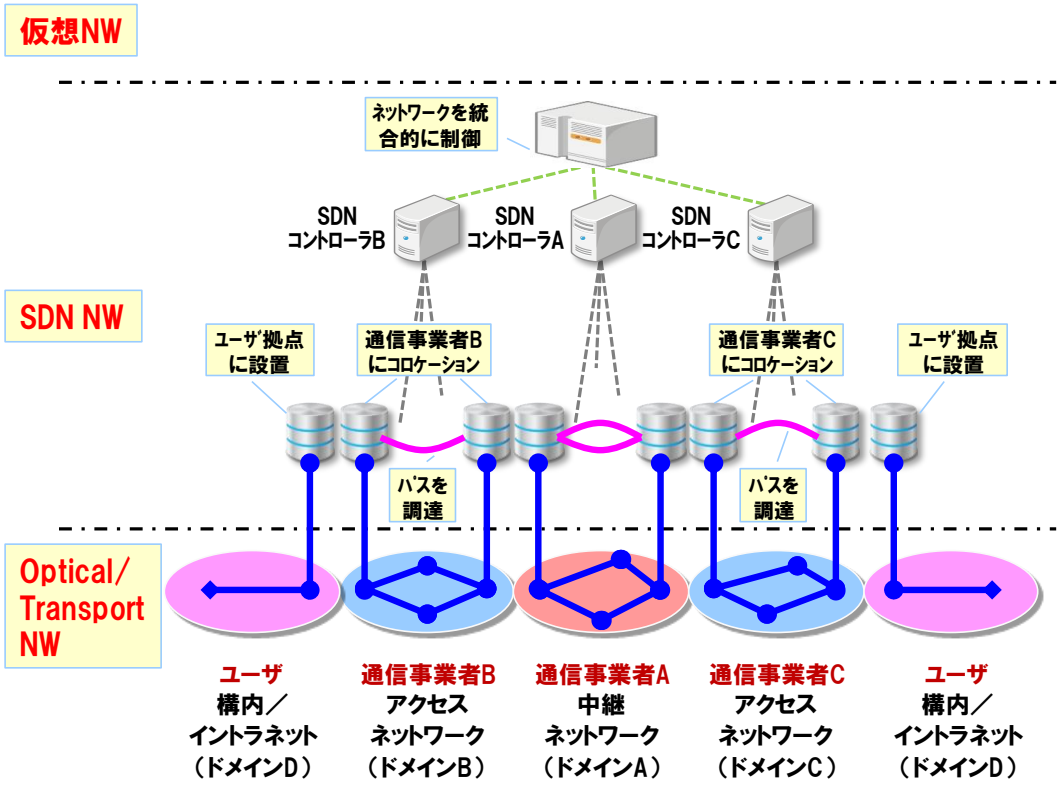


図 1-25　SDN NW の設計・構築

第3節 仮想 NW の設計・構築

「仮想 NW」の設計・構築について示す。通信事業者 A は、ユーザからの回線サービス申込みを受け、ユーザ拠点を結ぶフローを設定して回線サービスを開通する（図 1-26)。

- 通信事業者 A は回線サービスを提供するため、ネットワークリソースを確保する。
- ユーザからのサービス利用申込みを受け、各種条件を確認する。
  - ユーザの拠点
  - 品質条件
  - 信頼性条件
  - 帯域　　など
- ユーザの各種条件に基づきフローを設定して、回線サービスを開通する。

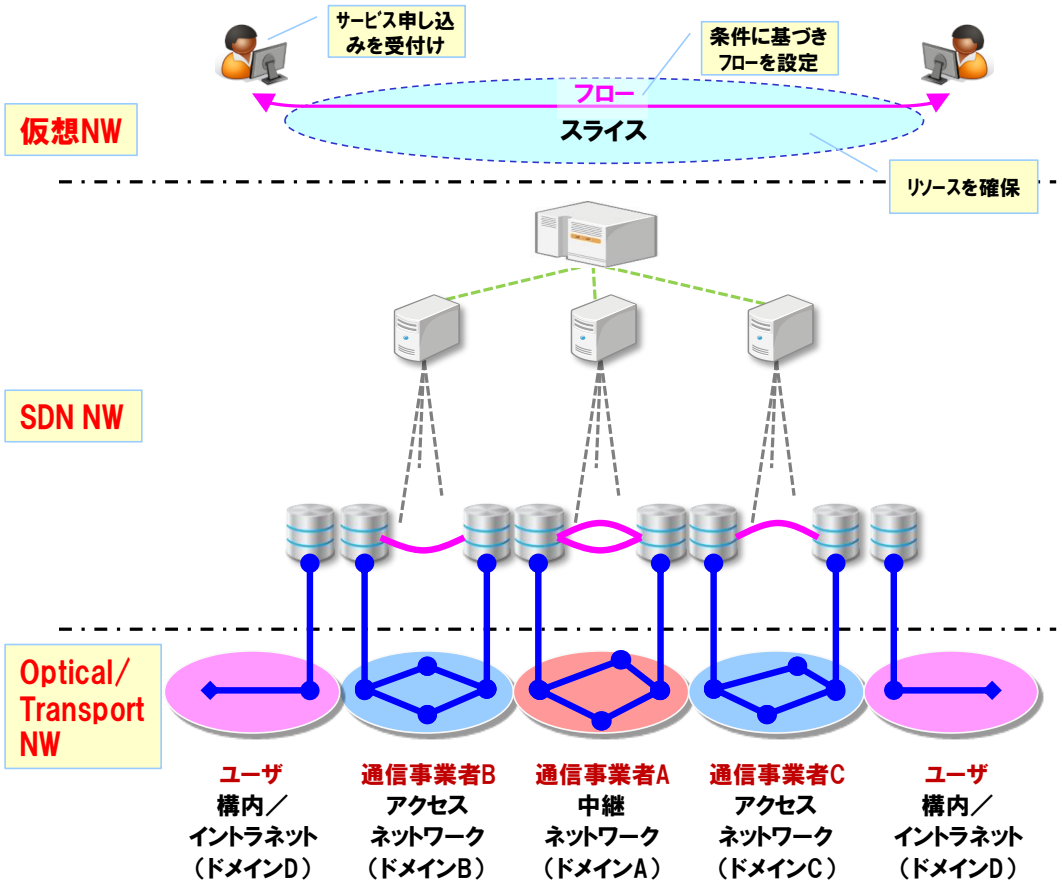


図 1-26　仮想 NW の設計・構築

第4節 通信事業者による運用・監視

通信事業者による運用・監視について示す。通信事業者 A はネットワークオーケストレータを介して、サービス提供状況の確認や、ネットワーク設定情報の変更を行うものとする。またネットワークの状態を常時監視し、異常発生時には、その検出と対処を行う（図 1-27）。

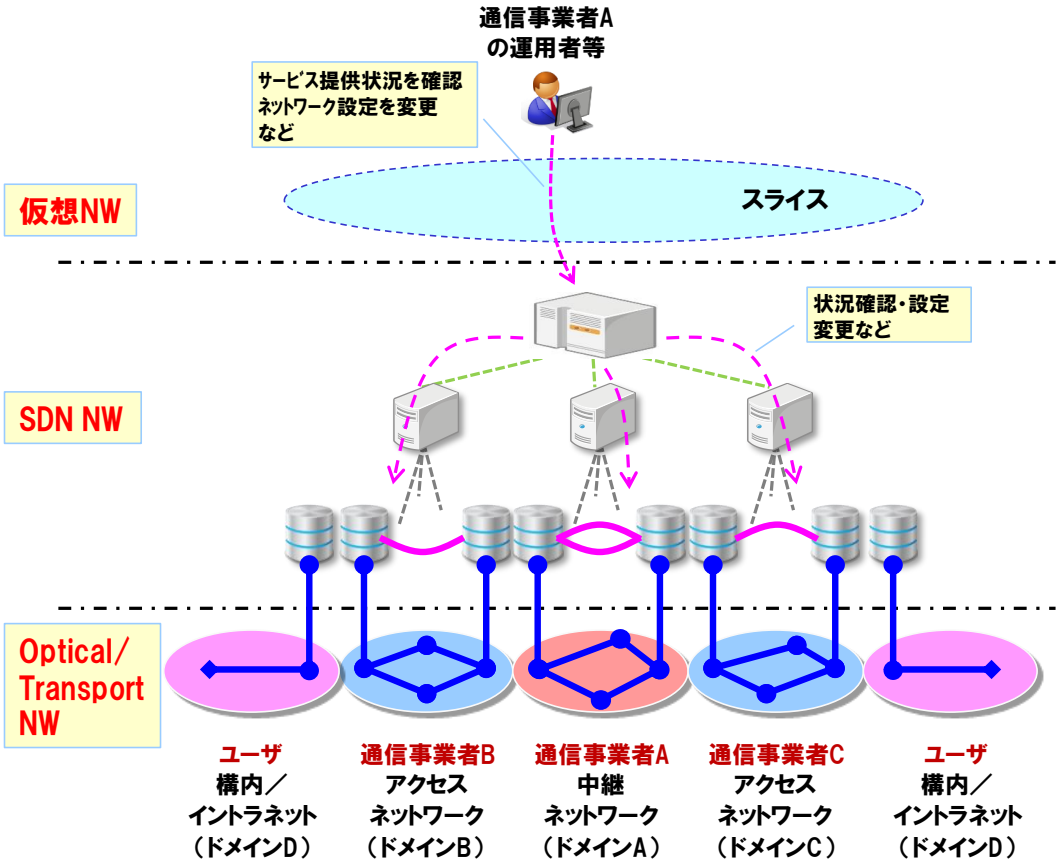


図 1-27　通信事業者による運用・監視

第5節 ユーザによる設定変更

ユーザによる設定変更について示す。回線サービスを利用するユーザは限られた条件においてネットワークの設定変更を行えるものとする。例えば回線の帯域や経路について、利用状況に応じて随時、ユーザに解放されたネットワーク制御用の API を介して変更を行う。また通信事業者においては充分なネットワークのセキュリティ対策（アクセス制限、アカウント管理等）を講じておく必要がある（図 1-28）。

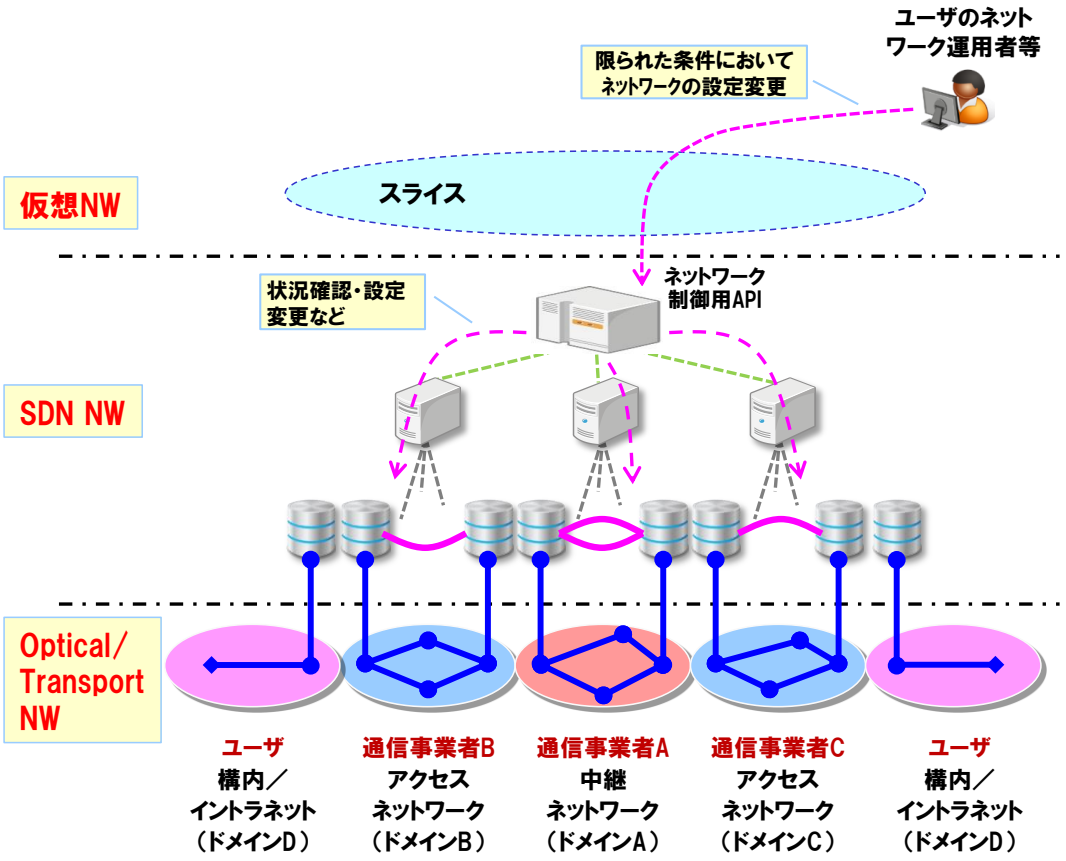


図 1-28　ユーザによる設定変更

第2編 設計・構築フェーズ

通信事業者がネットワークサービスを提供するにあたって、一般的に設計、構築、運用、監視といった業務フェーズがある。本ガイドラインは一般的な業務フェーズに則すものとし、第２編では設計・構築について、第３編では運用・監視について、通信事業者のネットワークにSDNを用いるための基本的な考え方を示す。

- 第２編 設計・構築フェーズ
- 第３編 運用・監視フェーズ

第1章 設計・構築フェーズの基本的な考え方

第1節 設計・構築フェーズの位置付け

設計・構築フェーズでは、提供するネットワークサービスの要求条件を満たすためのネットワーク構成を定め、定めたネットワーク構成に従い「SDN NW」を構成するSDNノードやSDNコントローラを設置・設定する。また「仮想NW」としてスライスやフローの設定を行い、ユーザに対してネットワークサービスを開始する。

第２編 設計・構築フェーズでは、第２章において「SDN NW」の設計・構築について、第３章において「仮想NW」の設計・構築について示した。また第４章では、第２章と第３章で示した設計・構築の考え方を統合し、基本的なネットワークモデルとして整理した。最後の第５章ではシステム設計等の参考情報として情報管理の考え方の一例を示した。

- 第２章 SDN NWの設計・構築
- 第３章 仮想NWの設計・構築
- 第４章 基本的なネットワークモデル
- 第５章 情報の管理

第2節 設計・構築のサイクル

第 2 章において「SDN NW」、第 3 章において「仮想 NW」の設計・構築について示すのに先立ち、ネットワークの階層によって設計・構築を行うサイクルが異なることについて、「Optical/Transport NW」も含めて補足する。

「Optical/Transport NW」はネットワークの基盤を構成する階層であり、光ノードや PTN (Packet Transport Network) ノードの設計・構築を行う。また光ケーブルや各種機器を設置するビルといったレイヤ 0 と呼ばれるような設備を設計・構築する場合は、膨大な期間や費用を要すこともあり頻繁な変更は困難である。これより、数ヶ月から数年先を見据えたサービスの需要予測に基づいて設備を計画的に見直す必要があり、「Optical/Transport NW」の設計・構築サイクルは比較的に長いことが想定される。

「SDN NW」は「Optical/Transport NW」の上位のネットワークとして構成する階層であり、SDN ノードや SDN コントローラの設計・構築を行う。ネットワークの利用状況や機器の使用率などを監視しつつ、必要に応じて機器の見直しを行うことが想定される。ただし、ソフトウェアで機能する機器はソフトウェア更新が頻繁に発生する可能性がある。

「仮想 NW」は「SDN NW」の上位に論理的に構成する階層であり、スライスやフローの設定を行う。ユーザからの日々のサービスオーダ（利用申し込み）を受けて「SDN NW」にフローを設定してユーザに提供することとなり、サービスオーダに応じて随時、フローの設計・構築を行う。またネットワークサービス戦略の見直しや新規ネットワークサービスの提供、ユーザからの要望などに応じて随時、スライスやフローを変更・追加していくことが想定される。

ネットワークの各階層の設計・構築サイクルのイメージを図 2-1 及び表 2-1 に示す。

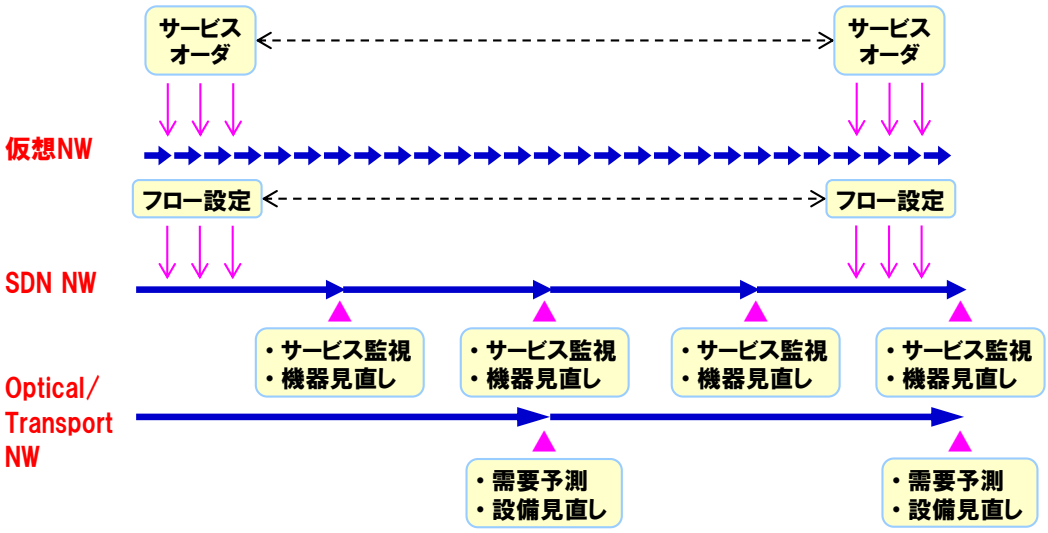


図 2-1　ネットワーク階層と設計・構築サイクル

表 2-1　ネットワーク階層と設計・構築サイクル

ネットワーク階層	設計・構築サイクル	サイクルの目安
仮想 NW	サービスオーダに応じて随時フローやスライスを設定	数時間～数日
SDN NW	サービスの利用状況や機器の使用率に応じて機器を見直し	数ヶ月
Optical/Transport NW	サービスの需要予測に基づき計画的に設備を見直し	数ヶ月～数年

第3節 OpenFlow を用いた設計・構築

SDN を実現する主要な技術として OpenFlow がある。OpenFlow はネットワーク機器のデータプレーンとコントロールプレーンを分離し、データプレーンの機能を OpenFlow スイッチに、コントロールプレーンの機能を OpenFlow コントローラに持たせ、ネットワークの集中制御を行うアーキテクチャを採る（詳細は第 1 編第 2 章 SDN の基礎）。

本ガイドラインでは通信事業者のネットワークにおいて、SDN を実現する技術として OpenFlow を用いることを想定している。そのため SDN ノードは OpenFlow スイッチ、SDN コントローラは OpenFlow コントローラを前提として解説する。

- SDN ノード：OpenFlow スイッチを想定
- SDN コントローラ：OpenFlow コントローラを想定

第2章 SDN NW の設計・構築

『第 2 章 SDN NW の設計・構築』では、第 1 節においてコントロールプレーンについて、第 2 節においてデータプレーンについて基本的な考え方を示す。

- 第 1 節 コントロールプレーン
- 第 2 節 データプレーン

コントロールプレーンの設計・構築では、OpenFlow コントローラの種類や配備の考え方について、データプレーンの設計・構築では、OpenFlow スイッチの種類や配備の考え方について示す。

「SDN NW」の設計・構築の考え方は、基本的には従来ネットワークの設計・構築の考え方を踏襲するものである。本ガイドラインでは OpenFlow の特徴を考慮し、OpenFlow を用いる際に特有の事項に着目して解説するものとし、従来ネットワーク技術の考え方に従う事項については最小限の記述に留める。

第1節 コントロールプレーン

1. OpenFlow コントローラ

1.1. OpenFlow コントローラの種類

SDN コントローラには、商用の OpenFlow 対応のコントローラ製品がいくつかある。コントローラ製品を使用する場合は、製品によって機能や性能条件などが異なるため、適用するネットワークの性質や規模などに応じて適切な機器を選定する必要がある。ただし、現時点では提供される製品種が少なく、また高価である場合が多い。

また、コントローラ製品を使用せずに、自主開発を行う方法もある。自主開発を行う場合は、OpenFlow コントローラのフレームワークを用いて、適用するネットワークに応じた機能や性能条件を備えた OpenFlow コントローラを実現できるが、開発のための技術検討やコストを要する。

1.2. OpenFlow コントローラフレームワークの特徴

OpenFlow コントローラフレームワークには、OSS (Open Source Software) と非 OSS（ソースコードを公開していないソフトウェア（プロプライエタリソフトウェア））がある。OSS を利用することで、効率的な開発が可能となりカスタマイズも容易となる。

OSS については、既に主要な言語に対応したフレームワークが存在しており、開発言語に対する要求条件に応じた選択の自由度が確保されている。例えば、実行効率よりも短期開発という生産性を重視する場合は、少ないコードで実装可能なスクリプト言語 (Ruby、Python 等) に対応したフレームワークを選択したり、また、開発要員や既存のソフトウェア資産の活用、連携などを重視する場合は、C や Java に対応したフレームワークを選択したりすることが考えられる。いくつかのフレームワークには、開発やデバックに便利なツールが提供されている。

OSS のライセンス形態としては、GNU General Public License (GPL v2/GPL v3) 、Apache License (Apache 2.0) 、Eclipse Public License (EPL v1) などがある。GPL v2/GPL v3 は、再配布、二次的著作物についても同じライセンスを適用する必要があるため、商用利用の際は注意が必要となる。

主要な OSS の OpenFlow コントローラのフレームワークを表 2-2 に示す。

表 2-2　主要な OpenFlow コントローラフレームワーク

名称	開発言語	開発元	ライセンス	特徴
Trema	Ruby、C	NEC	GPL v2	・ 日本国内では、非常に良く使われているコントローラ。 ・ 実行速度より開発効率に重点をおいている。 ・ ツール類も豊富。
NOX	C++	スタンフォード大学	GPL v3	・ OpenFlow の登場直後から開発している。 ・ OpenFlow 仕様を作った研究者が関係している。 ・ 歴史が古いため、Web での情報が集めやすい。
POX	Python	UC バークレイ	GPL v3	・ NOX から派生。 ・ Linux/Mac/Windows と OS を問わず動作が可能。 ・ アプリケーションの数は少ない。
Floodlight	Java	Big Switch Networks	Apache 2.0	・ プログラム人口の多い Java を使用。 ・ POX と同じく OS を問わず動作できる。

OpenDaylight	Java	OpenDaylight プロジェクト	EPL v1	・ 主要ベンダが共同で開発。 ・ SDN コントローラ及び Northbound /Southbound API 等の標準化を目指している。
Ryu	Python	NTT 研究所	Apache 2.0	・ OpenFlow バージョンが更新されると即座に最新版が提供される。 ・ 仮想スイッチの Open vSwitch を Ryu で制御可能。

2. SDN コントローラの冗長化

OpenFlow コントローラは監視制御網の OpenFlow チャネルを通して OpenFlow スイッチと接続して制御を実施する。通信事業者の提供する大規模なネットワークでは制御対象となる OpenFlow スイッチが多数となるため、OpenFlow コントローラに異常が発生した場合の影響が大きい。そのため信頼性の確保のために OpenFlow コントローラの冗長化を考慮する必要がある。

OpenFlow では、1 つの OpenFlow スイッチが複数の OpenFlow コントローラへ接続するための仕様が規定されている。冗長構成における OpenFlow コントローラの動作は「Role」と呼ばれる表 2-3 の 3 種類のいずれかの属性の割り当てにより決定される。

この仕組みを利用して OpenFlow コントローラの役割を決定することが可能である。例えば、OpenFlow コントローラ同士が Ping にて死活監視を行い、SLAVE が MASTER の異常を検知した場合、自身の役割を MASTER に変更する方法で冗長性を確保することが可能となる。

表 2-3　OpenFlow コントローラの冗長化

属性	内容
EQUAL	・ OpenFlow スイッチに対してフルアクセスを許可している。 ・ Packet-In 等の全ての非同期メッセージを受け取る。
SLAVE	・ OpenFlow スイッチに対し Read-Only のアクセスが可能。 ・ Packet-In 等の全ての非同期メッセージを受け取らない。
MASTER	・ EQUAL と同様の権限を持つが、OpenFlow スイッチは MASTER を 1 つのみ持つ。

また、OpenFlow コントローラを冗長構成とした場合には、コントローラ間でのデータの同期の方法を定め、故障等でコントローラが切替わった際には、待機系のコントローラが管理・制御を引き継げるような仕組みを用意しておく必要がある。

3. 同一ドメイン内の SDN コントローラの配備

OpenFlow コントローラは、対象とするドメイン内の OpenFlow スイッチを制御する。コントローラはドメイン内でスイッチの集中管理を行うが、処理性能や拡張性などが課題となる場合には、コントローラの集中型と分散型の使い分けを考慮する必要がある（図 2-2）。

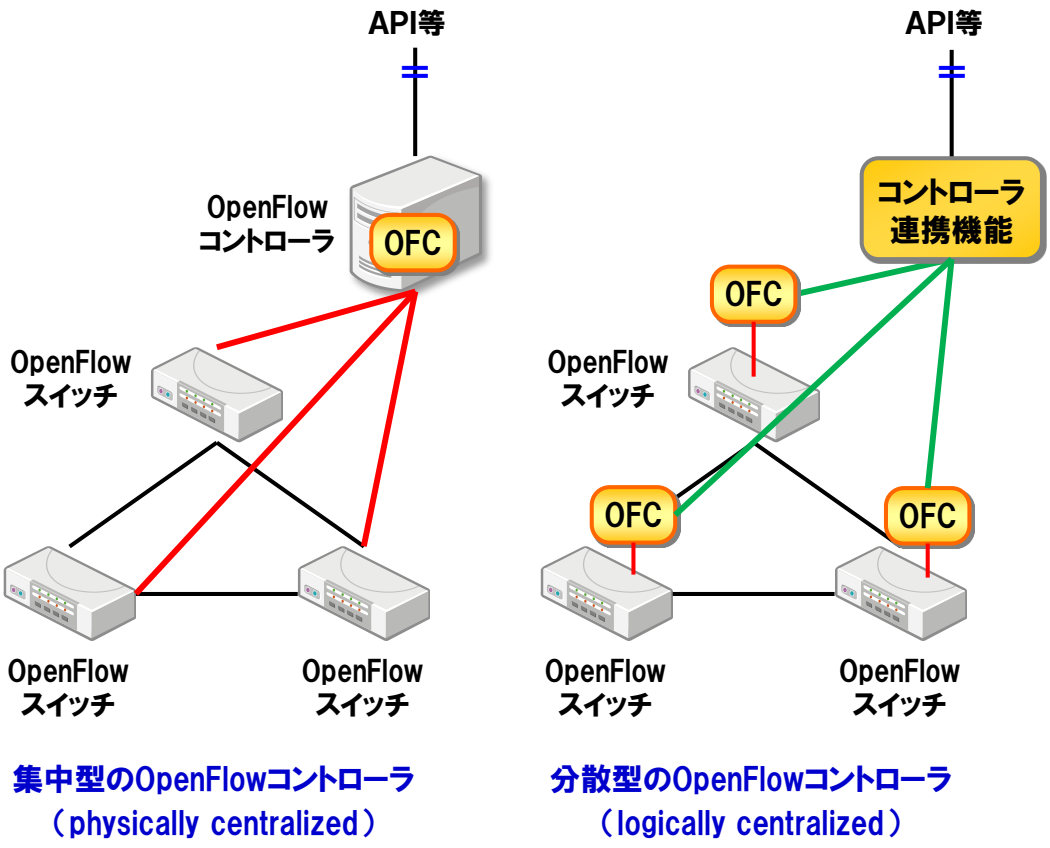


図 2-2　集中型と分散型の OpenFlow コントローラ

3.1. 集中型コントローラ

一つの OpenFlow コントローラで集中的に管理を行う方式である。マクロな視点でのトラヒックエンジニアリングにより、多様なニーズに対する経路探索への対応が可能である。分散型と比較して運用・管理が容易である一方、処理能力や拡張性などがボトルネックとなる場合がある。

3.2. 分散型コントローラ

OpenFlow スイッチに OpenFlow コントローラの機能を分散配備する方法である。また分散配備した機能をコントローラ連携機能などにより階層化する方法も考えられる。

フロー切替え等の、比較的単純であるが短時間に多数の処理を要求される場合など、処理性能の条件が厳しい制御に有効である。

実現例としては、スイッチ内の OS に OpenFlow コントローラをインストールする方法が考えられる。この場合、OpenFlow プロトコルはスイッチ内でやり取りされることになる。ただし、外部のコントローラとの制御情報のやり取りの規定は OpenFlow にはないため、通信方式を検討して OpenFlow コントローラに実装する必要がある。

3.3. 集中型と分散型の使い分け

集中型と分散型の両方式のコントローラの協調制御も考えられる。例えば、隣接ノードの発見などの単純な制御を分散型コントローラで行い、集中型コントローラがその情報を集約して、全体トポロジの作成・管理を担当する方法である。

このように集中型コントローラと分散型コントローラの特性を踏まえ、適用するネットワークの規模や想定される処理負荷、将来の拡張性などを考慮して、設計の段階で適切な方式を選択することが望ましい。

またコントローラの試験などにより実際の処理性能を測定して、要求される条件を満たすかどうかを判断することも重要である。

4. 異なるドメイン間の SDN コントローラの連携

複数の SDN を用いたネットワーク（異なるドメインや OpenFlow 以外の SDN ネットワーク）を接続してサービスを提供する場合、接続先のネットワークを含めた状態管理や制御を行うために、各ネットワークを管理する SDN コントローラ同士の連携が必要となる。

4.1. SDN コントローラ間の連携

各 SDN コントローラが管理するネットワーク構成情報を、SDN コントローラ間で通知することで、相互のネットワーク状態の管理を行う（図 2-3）。ただし、この方法は連携のための SDN コントローラの処理が増大する懸念がある。また SDN コントローラ間での通信方式が標準化されておらず、通信方式を検討して SDN コントローラに実装する必要がある。

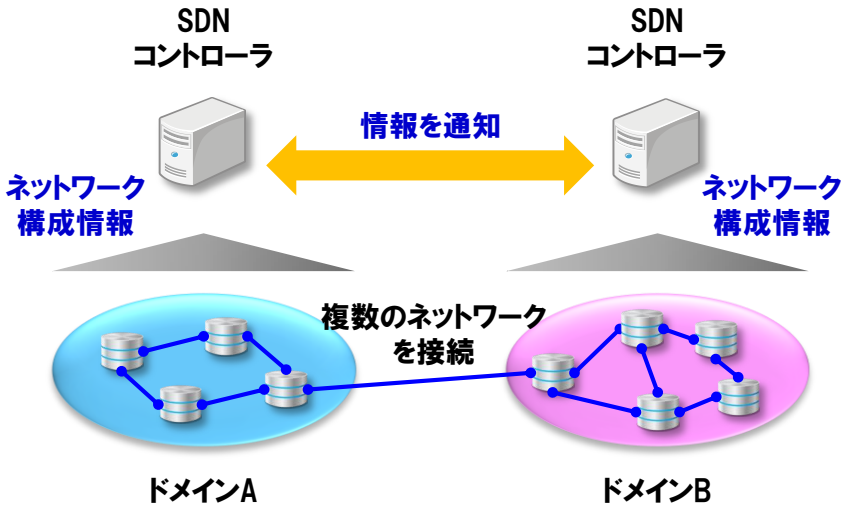


図 2-3　SDN コントローラ間の連携

4.2. オーケストレータを介した連携

各 SDN コントローラが管理するネットワーク構成情報をオーケストレータに集約し、統合管理を行う方法も考えられる（図 2-4）。コントローラ間で連携を行う場合は独自に通信方式を定める必要があるが、オーケストレータを介した連携は SDN コントローラの API を介すことで早期の実現が期待できる。また SDN コントローラの処理の一部をオーケストレータに分散させることにより、SDN コントローラの処理負荷軽減や機能分散の効果も期待できる。

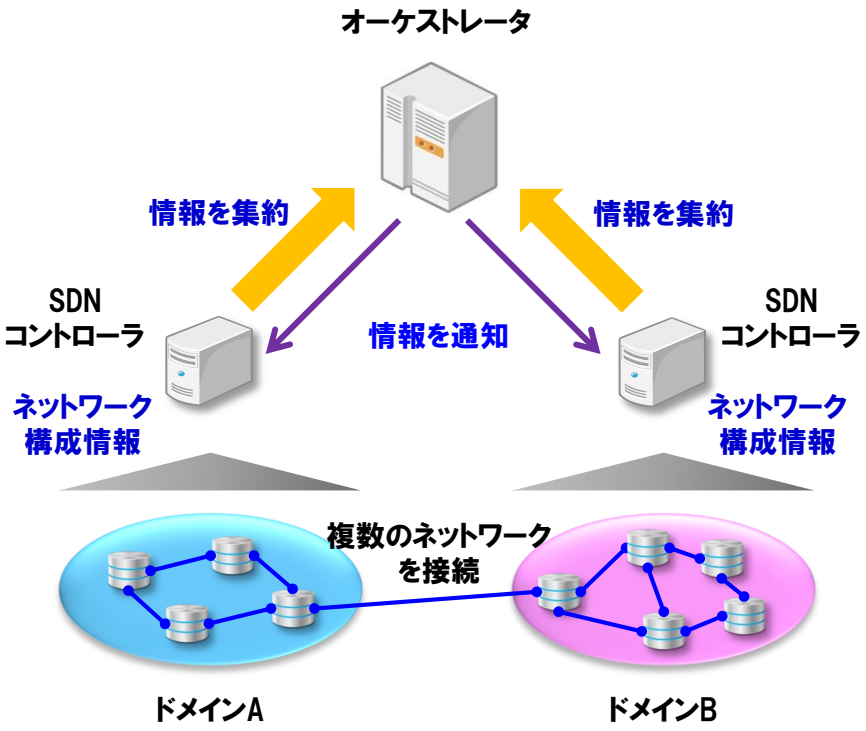


図 2-4　オーケストレータを介した連携

第2節 データプレーン

1. OpenFlow スイッチ

1.1. OpenFlow スイッチの種類

OpenFlow スイッチは、OpenFlow 対応のハードウェアスイッチと、汎用サーバに仮想スイッチのソフトウェアをインストールして使用するソフトウェアスイッチがある。

1.1.1. ハードウェアスイッチ

ハードウェアスイッチは、OpenFlow スイッチとしてのみ動作する機器と、従来の L2/L3 スイッチとしても使用できるハイブリッド型とがある。従来のスイッチの OS やファームウェアをアップグレードすることにより OpenFlow 対応スイッチとするアプローチが主流になってきており、スイッチの選択肢が増えてきている。

ハードウェアスイッチはパケット転送能力に優れ、大規模ネットワークへの適用が期待されるが、一方でフローテーブルのエントリ数の上限が少ないなど機能に制限があったり、チップベンダのリリースタイミングに影響され、新機能や新プロトコルへの対応が遅れたりするなどの懸念もある。

一般的なハードウェアスイッチの主な特徴を以下に整理する。

- パケット転送能力に優れる。
- 大規模ネットワークへの適用に期待。
- 物理ポート数が多い。
- フローテーブルの上限が少ない。
- 新機能や新プロトコルへの対応が遅れる場合がある。

1.1.2. ソフトウェアスイッチ

ソフトウェアスイッチは汎用サーバを用いて安価に、かつ、要求条件や性能要件に応じて幅広い用途で使用することが期待される。ハードウェアスイッチと比べると実装が容易であることから新サービスや新プロトコルへ早期に対応しやすく、機能追加に容易に対応できるため柔軟性に優れている。一方でフローエン

トリ数の増加や Match 条件の複雑化、またショートパケットが多い場合などにパフォーマンスが低下するなど、パケット転送能力に制約が生じる場合がある。

ソフトウェアスイッチの例としては NTT が開発した「Lagopus（ラゴパス）」があり、オープンソースソフトウェア（OSS）として提供されている[5]。

一般的なソフトウェアスイッチの主な特徴を以下に整理する。

- 汎用サーバを用いて実装が容易。
- 機能追加などの柔軟性に優れ適応領域が広い。
- パケット転送能力に制約が生じる場合がある。

1.1.3. 動作条件の考慮事項

OpenFlow には複雑な仕様や数々の Optional があり、OpenFlow に準拠したスイッチであっても対応している動作（Match Fields や Actions など）に制限がある場合がある。OpenFlow に準拠したスイッチに対して、OpenFlow 仕様の実装状況をテストして結果を公開する Ryu Certification があり、スイッチ選定の際には活用することが望ましい[6]。

1.2. ソフトウェアスイッチの利用形態

ソフトウェアスイッチはハードウェアスイッチのように専用機器を購入する必要がなく、様々な用途で使用可能であり導入が容易である。また機能が充実して適用範囲が広いといえる。

ソフトウェアスイッチの利用形態には、物理ハードウェアの汎用 OS 上に実装する方法と仮想環境に実装する方法がある。仮想環境への実装はハイパーバイザと呼ばれる仮想化ソフトウェアを利用する。ソフトウェアスイッチの代表的な利用形態を図 2-5 に示す。

A)　物理ハードウェア上にソフトウェアスイッチを実装（ベアメタル）

B)　ハイパーバイザ内にソフトウェアスイッチを実装

[5] http://www.ntt.co.jp/news2014/1406/140606a.html ［NTT 持株会社ニュースリリース］

[6] http://osrg.github.io/ryu/certification.html ［Ryu SDN Framework Community］

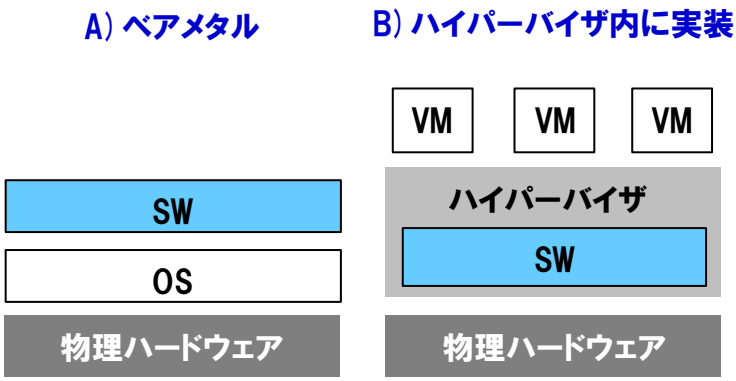


図 2-5　ソフトウェアスイッチの代表的な利用形態

物理ハードウェア上に（ハイパーバイザを介さずに）ソフトウェアスイッチを実装するベアメタル(A)は、物理ハードウェアのリソースを占有できるため高い処理性能が期待できる。一方、多重化ができないため、多数の OpenFlow スイッチを必要とする場合には適さない。(B)は仮想化を実現するためのハイパーバイザにソフトウェアスイッチを組み込む構成であり、仮想化環境において主流となる形態である。

仮想化環境でソフトウェアスイッチのパフォーマンスを安定的に使用するためには、スイッチに割り当てるリソースを固定化する設定を行うことが望ましい。ただし、その場合には制御を行う VM (Virtual Machine) 数などに制限が生じる場合がある。また利用する仮想化ソフトウェアによって機能に違いが生じたり、CPU やボードによって性能が異なることがあるので、事前に十分な検証を行うことが重要である。

いずれの利用形態においても物理ハードウェアのスペックについて考慮が必要である。特に仮想環境にソフトウェアスイッチを実装する場合、1 台の物理ハードウェアで複数の VM のリソースをシェアするため、CPU やメモリ及びディスク容量には充分な余裕があることが望ましい。

2. コントロールプレーンとの接続

コントロールプレーンとデータプレーンの分離に起因する考慮事項について示す。コントロールプレーンとデータプレーン間に通信断が発生した場合（監視制御網に通信断が発生した場合）にはネットワークの制御情報のやり取りができなくなり、データプレーンのパケットのフォワーディング動作に影響を与えることがある。

OpenFlow のプロトコルでは、OpenFlow スイッチと OpenFlow コントローラとの間に通信断が発生した場合の、OpenFlow スイッチのフォワーディング動作を規定している（表 2-4）。通信断時のモードは OpenFlow スイッチの初期設定で定められ、パケット処理方式（プロアクティブ型／リアクティブ型）と合わせて考える必要がある。

表 2-4　OpenFlow プルトコルでのコントローラとの通信断時の動作の規定

モード	動作概要
Emergency Flow Cache	エマージェンシーフローエントリを適用して、フォワーディング動作を継続。
Fail Secure Mode	既に登録されているフローエントリを使用して、フォワーディング動作を継続。
Fail Standalone Mode	通常の（OpenFlow ではない）スイッチまたはルータとして機能。

「Emergency Flow Cache」モードでは、OpenFlow コントローラとの接続が絶たれた場合に、OpenFlow スイッチはエマージェンシーモードに移行する。通常時のフローエントリを削除し、スイッチの初期設定で定められたエマージェンシーフローエントリを適用して、フォワーディング動作を継続する。ただし、OpenFlow 1.1 以降では「Emergency Flow Cache」は削除された。

「Fail Secure Mode」では、OpenFlow コントローラとの接続が絶たれた場合に、OpenFlow スイッチは既に登録されているフローエントリを使用してフォワーディング動作を継続する。フローエントリ登録時に指定した Time Out 値に達してフローエントリが削除されるまでフォワーディング動作が継続されるため、Time Out 値をどの程度に設定するかが重要である。

パケット処理方式がプロアクティブ型の場合はOpenFlowスイッチにフローエントリが予め登録されているため、「Fail Secure Mode」と組み合わせることでOpenFlowコントローラとの接続が絶たれた場合でもフォワーディング動作を継続できる。一方、リアクティブ型の場合はOpenFlowスイッチが宛先不明のパケットを受信した後にフローエントリを登録する方式であり、宛先不明なパケットに対する学習が不可能となりフォワーディング動作が停止する。

「Fail Standalone Mode」では、OpenFlowコントローラとの接続が絶たれた場合に、OpenFlowスイッチはフローエントリによるフォワーディングは行わずに、通常の（OpenFlowではない）スイッチまたはルータとして機能する（ハイブリッド型のスイッチの場合）。ただし、宛先不明のパケットをマルチキャストするモードに移行し、ブロードキャストストームを起こしてバーストするケースがあるため注意が必要である。

3. 冗長化方式

従来ネットワークの信頼性の考え方として、例えばノードではVRRP (Virtual Router Redundancy Protocol）などのプロトコルがあり、各装置はプロトコルに従い自立制御で冗長化を実現している。またリンクではアクティブ／スタンバイなどによる代替リンクを各装置に設定して、冗長化を実現している。

OpenFlowでは、OpenFlowスイッチの冗長化を制御するのはOpenFlowコントローラの役目である。スイッチの異常をコントローラで検出してソフトウェア制御で切替えを実施する必要があり、そのための機能をネットワークアプルケーションとしてコントローラに実装しておく必要がある。ノードやリンクについては必要に応じて冗長化構成を取れるよう設計をしておく必要がある。

切替えにはノード／リンク毎での切替えや，End-to-Endのパスで切替えるなど様々な方法がある（切替え方式の詳細については第3編の運用・監視フェーズで述べるものとし、今後の課題とする。）。

異常検出の観点では、OpenFlowコントローラからOpenFlowスイッチに対して「Echo Request/Reply」メッセージを定期的に送信することで、スイッチの死活監視が可能である。

第3章 仮想 NW の設計・構築

『第 3 章 仮想 NW の設計・構築』では、ネットワークサービスを構成するフローと回線について第 1 節に示す。また多数のユーザが重畳する通信事業者ネットワークにおいて必要となるユーザフローの分離の考え方を第 2 節に、さらにユーザフローの効率的な管理のための中継パスの適用の考え方を第 3 節に示す。

- 第 1 節 フローと回線
- 第 2 節 ユーザフローの分離
- 第 3 節 中継パスの適用

第1節 フローと回線

1. 回線サービスの提供

「仮想 NW」は「SDN NW」の上位の論理ネットワークとして位置付けられ、SDN を用いたネットワークにおいてネットワークサービスを構築して提供する。通信事業者が SDN を用いて提供するネットワークサービスは各種が想定されるが、本ガイドラインでは、各種ネットワークサービスの基本となる Point-to-Point でユーザ拠点間を接続する回線サービスを例として取り上げ、ネットワークサービスの実現方法や考慮事項などについて示す（図 2-6）。

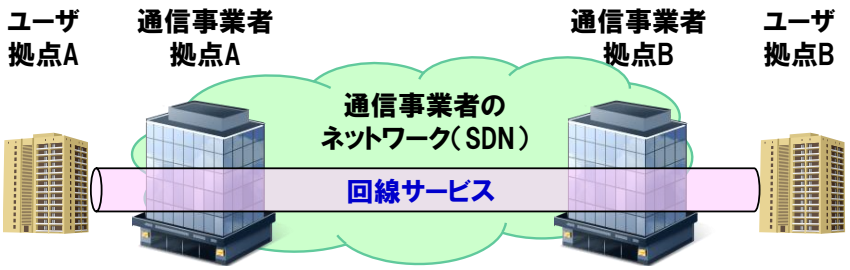


図 2-6　回線サービスの提供

2. フローと回線の定義

フローは、リンク（SDN 用のリンク）及び SDN ノードを通過するパケットの通り道であり、End-to-End のポート間に片方向に設定されるものと定義する。OpenFlow では、OpenFlow コントローラ（SDN コントローラ）から OpenFlow スイッチ（SDN ノード）のフローテーブルに対し、フローエントリとして設定される。

回線とは、1 つ以上のフローで構成され、ユーザに対してネットワークサービスを提供する単位として定義する。End-to-End に Point-to-Point で設定され、ユーザの拠点間を接続する。

また回線は SDN 以外のドメインを組み合わせてネットワークサービス提供を行う場合がある（表 2-5、 図 2-7）。

表 2-5　フローと回線の定義

	定義
フロー	・ リンク及び SDN ノードを通過するパケットの通り道。 ・ End-to-End のポート間に片方向で設定。
回線	・ ユーザに対してネットワークサービスを提供する単位。 （SDN 以外のドメインを組み合わせてサービス提供を行う場合あり） ・ 1 つ以上のフローで構成。

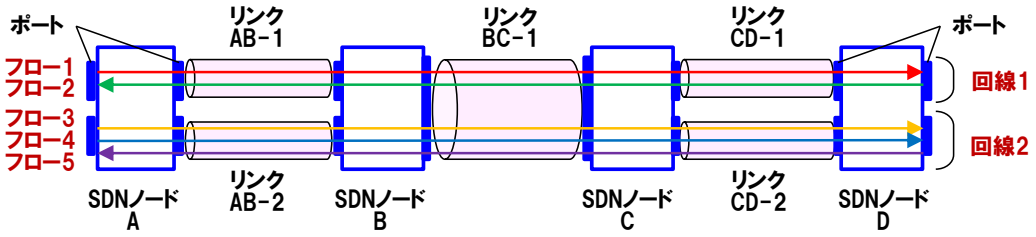


図 2-7　フローと回線の定義

3. プロアクティブとリアクティブ

フローはパケットの処理方法から、プロアクティブとリアクティブに分類される。プロアクティブとリアクティブのフローの特徴を以降に示す。

なお、フローで構成される回線についても同様に、プロアクティブとリアクティブの回線が存在して同様の特徴をもつ。

3.1. プロアクティブのフロー・回線の特徴

プロアクティブの場合は、SDN ノードのフローテーブルにフローエントリが予め設定済みであり、静的な回線設定となる。SDN ノードに到着したパケットはフローエントリに従い転送される。一度設定したフローは回線の廃止オーダまで消えることはない。従来の伝送パスの設定と同じ考え方といえる。

SDN ノードでは必要なフロー数に見合うフローテーブルのサイズが必要となる。

3.2. リアクティブのフロー・回線の特徴

リアクティブは OpenFlow 特有の制御方式である。回線を構成するフローは、ユーザからのサービスオーダ（利用申し込み）を受け、フロー設計の段階で OpenFlow コントローラが経路情報を把握しておくが、その時点では OpenFlow スイッチのフローテーブルへの設定は行わない。

フローテーブルへの設定は、最初のパケットが OpenFlow スイッチに到着した時点で行われる。到着したパケットは「table miss（該当するフローエントリが見つからない)」となり OpenFlow コントローラに対するパケットインが発生する。コントローラは予め保持するフロー情報と照らし合わせ、該当するフローエントリを各スイッチに対して設定する。

また指定された時間を越えてパケットの到着がない場合は、当該のフローエントリは OpenFlow スイッチにより消去される。

リアクティブではフローテーブルの使い回しができるので、フローテーブルのサイズが小さい場合に有効である。

4. フローと回線の種類

4.1. 基本回線と回線オプション

OpenFlow が具備する機能を利用することで複雑なパケット制御が可能となり、従来には無いような様々なネットワークサービスが提供される可能性がある。

本ガイドラインでは OpenFlow で実現可能なパケットの流れる経路に着目し、通信事業者として考えられる回線サービスを整理する。提供する回線サービスを“基本回線”と“回線オプション”として定義し、回線の種類の分類とサービスイメージを示す。

4.1.1. 基本回線

基本回線を以下の通りに定義する（図 2-8、図 2-9）。

- 回線はサービス提供の単位である。
- 回線は 1 つ以上のフローから構成される。
- 回線は 2 つの端点となるポート間で設定される。
- 同じポートに異なる回線が設定できる（多重アクセス回線）。
- 回線の種別として両方向、片方向がある。
- 両方向の回線の場合、両方向の 2 つのフローは同じ経路を通る。

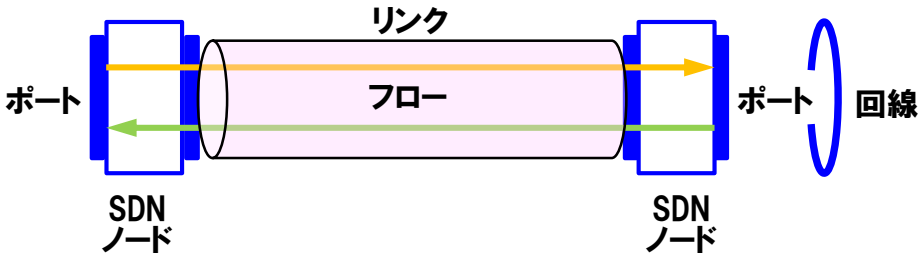


図 2-8　基本回線：両方向通信

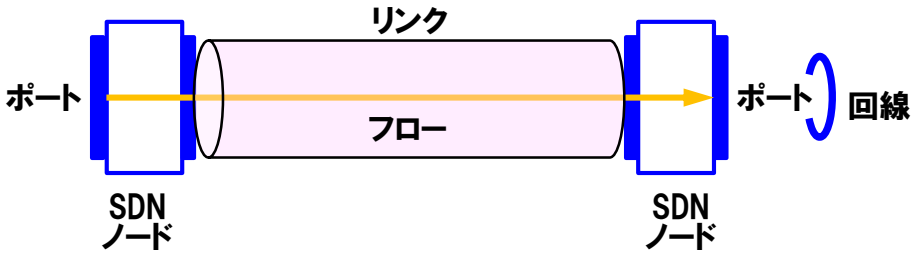


図 2-9　基本回線：片方向通信

4.1.2. 回線オプション

回線オプションを以下の通りに定義する。

- 基本回線に対して機能を追加するもの。
- 基本回線は、複数の回線オプションを選択できる。
  - オプションなし
  - 破棄（パケットは「null」ポートに到達して「Drop」されると考える）
  - 分岐
  - VLAN 付与　　など
- 両方向の回線では、両方向の 2 つのフローは異なる経路の場合がある。

4.2. 回線オプションの種類とサービスイメージ

回線オプションは基本的な回線サービス（基本回線）に対して機能を付加するものである。回線オプションの考え方とサービスイメージを示す。

4.2.1. VLAN を付与

ある SDN ノードにおいて、特定のパケットを Match 条件により識別し、VLAN タグを付与する。あるいは、VLAN タグが付与されたパケットを Match 条件により識別し、VLAN タグを除去する（図 2-10）。

図 2-10　VLAN を付与

4.2.2. パケットの経路を変更

ある SDN ノードにおいて、特定のパケットを Match 条件により識別し、フローが通過する経路を変更する。例えば利用用途による要求遅延を考慮し、遅延要求の高い通信は最短経路となるようパケットを振り分けるといったサービスが可能となる（図 2-11）。

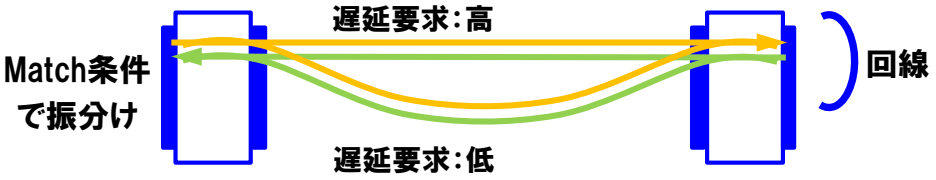


図 2-11　経路を変更

4.2.3. 指定通信のみ許可

ある SDN ノードにおいて、特定のパケットを Match 条件により識別し、条件に合うパケット（または合わないパケット）は廃棄することにより、ACL（Access Control List）のようなサービスが提供可能となる。

OpenFlow の具体的な動作としては、OpenFlow スイッチで受信したパケットが「null」ポートで Drop されると考える。サービス構築のパタンとしては、エッジの SDN ノードで Drop する方法と（図 2-12）、経路の途中に Drop 用の SDN ノードを設ける方法が考えられる（図 2-13）。

図 2-12　特定通信のみ許可（1）

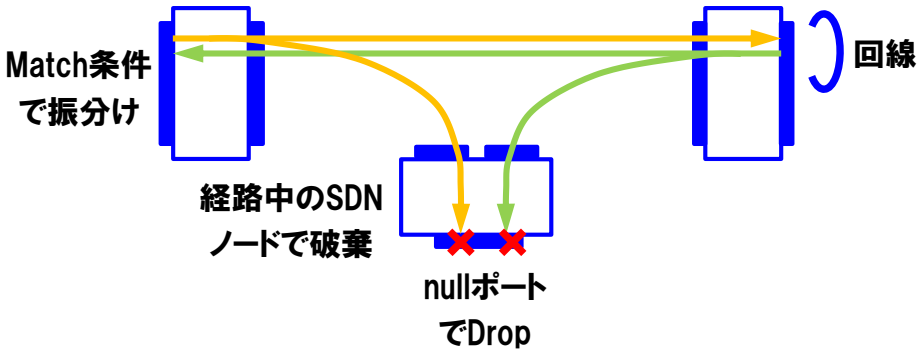


図 2-13　特定通信のみ許可（2）

4.2.4. パケットの宛先を変更

ある SDN ノードにおいて、特定のパケットを Match 条件により識別し、条件に合うパケット（または合わないパケット）の経路を分岐させる（図 2-14）。特定のパケットの宛先を変更することによりロードバランサのようなサービスが提供可能となる（図 2-15）。

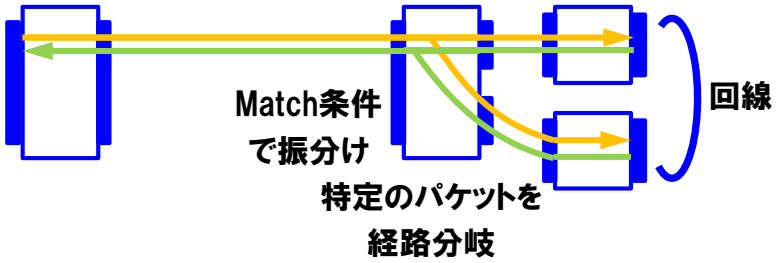


図 2-14　パケットの宛先を変更

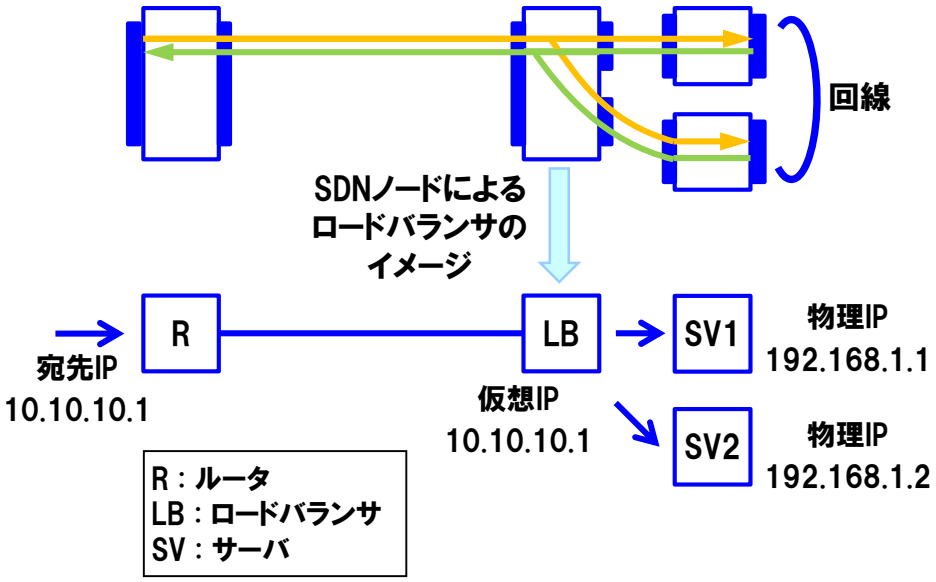


図 2-15　SDN ノードによるロードバランサのイメージ

OpenFlow の具体的な動作としては、OpenFlow スイッチの複数のポートを束ねる「Group」という機能を利用する。グループの処理方法（Type）として「Select」を指定することにより、グループ内からどれか 1 つのポートを選んで転送が可能となり、同じフローエントリのパケットを異なる経路に転送可能となる。

4.2.5. ネットワーク機能の挿入

ある SDN ノードにおいて、特定のパケットを Match 条件により識別し、条件に合うパケット（または合わないパケット）に対してネットワーク機能（DPI: Deep Packet Inspection 等）を付加することで、サービスチェイニングのような利用が可能となる。

サービス構築のパタンとしては、ネットワーク機能を挿入するための SDN ノードをフローの経路の途中に設ける方法と（図 2-16）、エッジの SDN ノードでネットワーク機能を挿入するための SDN ノードに振り分ける方法が考えられる（図 2-17）。

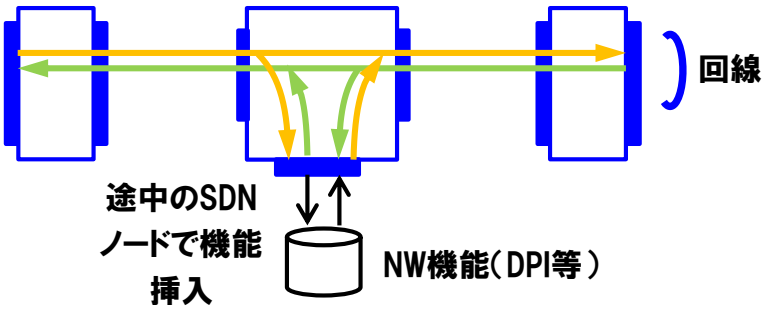


図 2-16　ネットワーク機能の挿入（1）

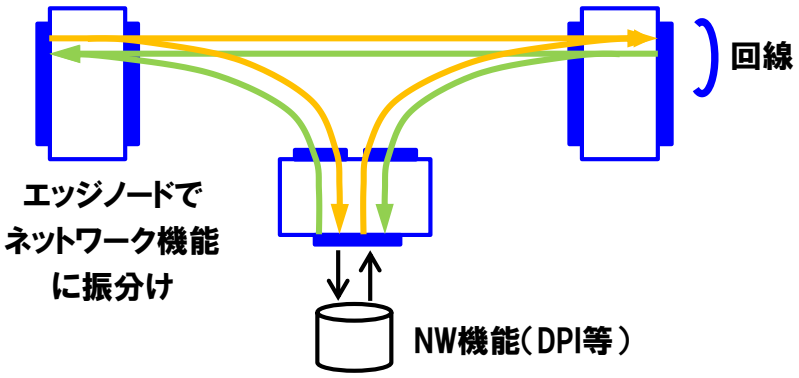


図 2-17　ネットワーク機能の挿入（2）

4.2.6. 冗長あり回線

基本回線に対してオプションとして冗長回線を設定する。以降に冗長回線の例として 3 つの方式を示す。なお、冗長化に関しては双方向で使用するものであるが、図では煩雑になるため片方向のフローのみを示している。

- 冗長あり回線（1:1）
- 冗長あり回線（1+1）
- 冗長あり回線（N:1）

(1) 冗長あり回線（1:1）

平常時に使用する基本回線（Act：アクティブ）に対して、バックアップ用の異経路を通る冗長回線（Sby：スタンバイ）を設定する。平常時は片系のみを使用し、現用系の Act の回線に異常が発生した際に、Act から予備系の Sby に回線を切替えてサービスを継続する（図 2-18）。

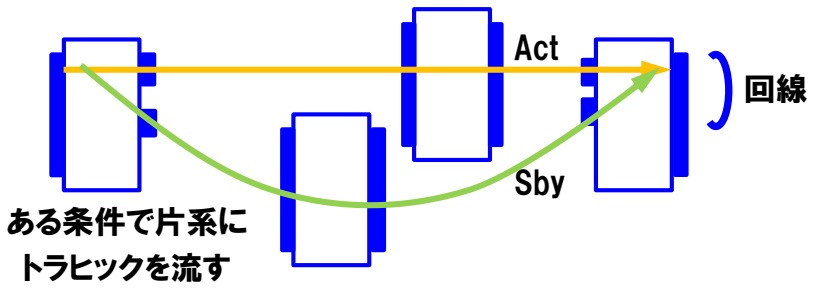


図 2-18　冗長あり回線（1:1）

冗長回線の設定方法としてリアクティブ方式を適用することも可能である（図 2-19）。リアクティブ方式の場合は冗長回線のフローエントリが SDN ノードに事前に設定されておらず、ある条件が発生した後にフローエントリが設定されるため、回線の切替えの際に時間を要する。

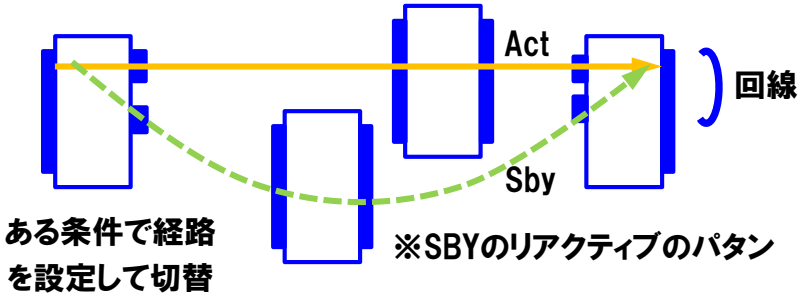


図 2-19　冗長回線がリアクティブのパタン

(2) 冗長あり回線（1+1）

基本回線（Act：アクティブ）に対して、平常時にも使用する異経路を通る冗長回線（Act：アクティブ）を設定する。この場合は平常時から双方の回線を現用系として使用するものとし、トラヒックはある条件で双方の回線に分岐する。通常時から両系の回線を使用することで、どちらか一方の回線に異常が発生した場合でもサービスを継続する（図 2-20）。

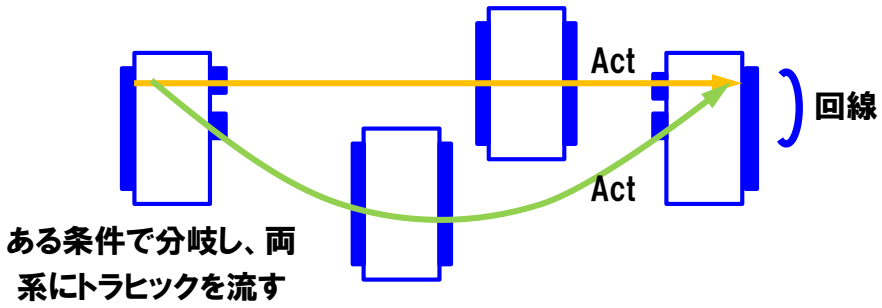


図 2-20　冗長あり回線（1+1）

(3) 冗長あり回線（N:1）

平常時に使用する複数（N 本）の基本回線（Act：アクティブ）に対して、共用となるバックアップ用の異経路を通る冗長回線（Sby：スタンバイ）を設定する。いずれかの回線に異常が発生した際に、現用系の Act から予備系の Sby に回線を切替えてサービスを継続する。図 2-21 は N=2 本のアクティブ回線に対して、スタンバイの冗長回線を設定した例である。

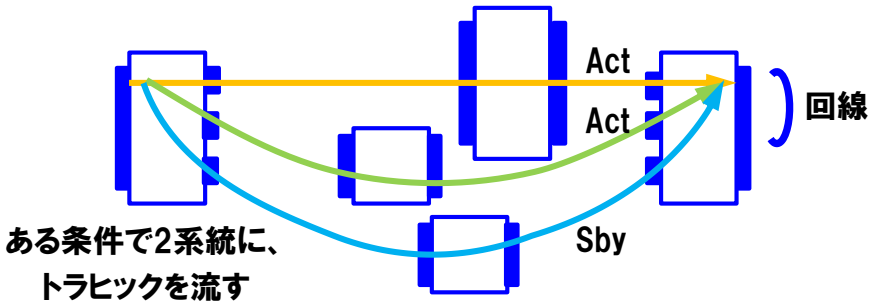


図 2-21　冗長あり回線（N:1）

4.2.7. 3 ポート以上を結ぶ回線

(1) 3 ポート以上を結ぶ回線の基本パタン

これまでの例では 2 ポート（2 拠点）間を Point-to-Point で結ぶ回線の例として解説をしてきた。本項では従来サービスと照らし合わせ、Point-to-Point から Point-to-Multipoint の回線への応用について考える。

3 ポート以上の場合については、2 ポート間の回線の組合せとして同様に考えることができる。具体的には 3 ポートの場合の基本パタンは、6 フロー3 回線の組合せとして考えることができる（図 2-22）。

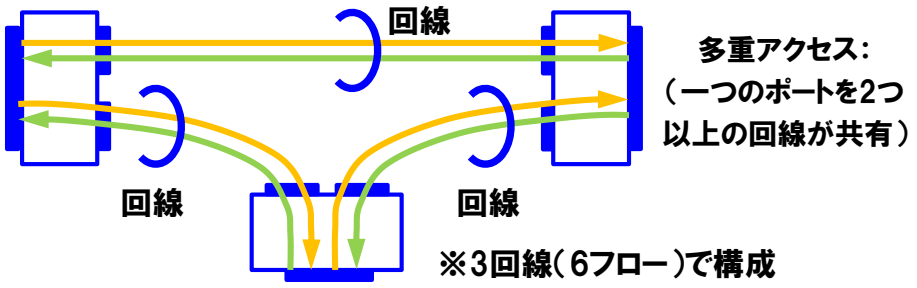


図 2-22　3 ポートを結ぶ 3 つの回線（基本パタン）

(2) 3 ポート以上の場合のマルチキャスト回線の例

3 ポート以上の場合に複数の宛先に対して同じデータを送信するマルチキャスト通信を提供する場合は、片方向の分岐する回線を宛先ポート数分追加することで、特定のパケットをマルチキャストすることができる（図 2-23）。

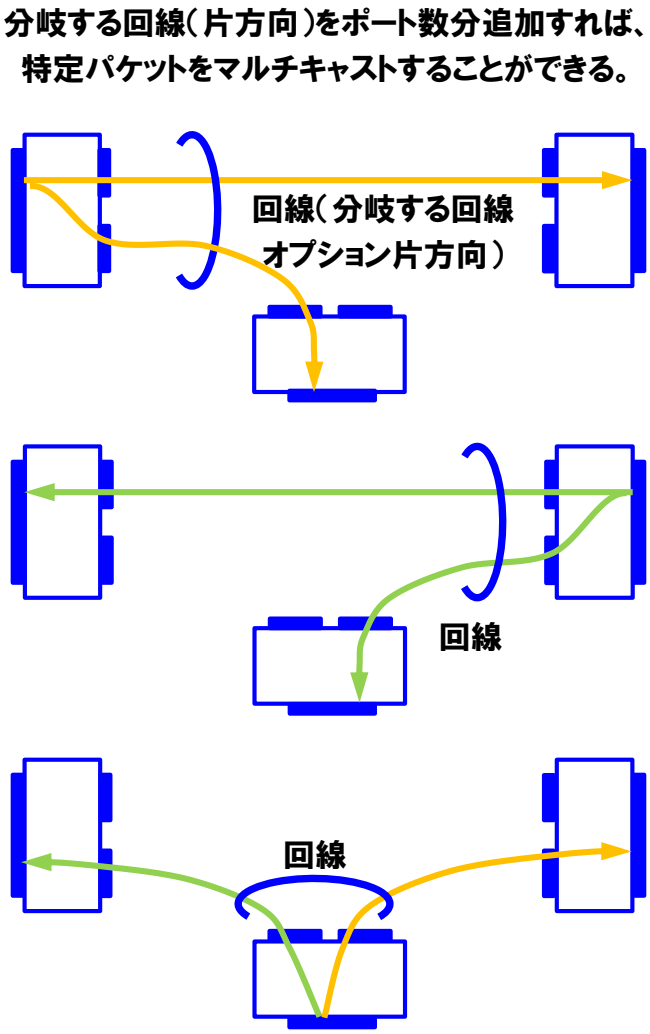


図 2-23　分岐する回線オプションによるマルチキャスト回線の例

第2節 ユーザフローの分離

1. ユーザ多重に関する課題

通信事業者が提供する回線サービスでは、同一のネットワーク上に複数のユーザを多重する利用形態が想定される。ユーザが契約する回線はフローで構成され、OpenFlow では各々のフローは Match 条件で識別されるが、異なるユーザが同じ l2/L3 アドレスや VLAN ID を使用している場合も想定される。異なるユーザが同じ情報を Match 条件として指定した場合や、スイッチのイングレスポート（IN_PORT）のみでフローを識別する場合、それらのフローは同一のパケット転送ルールと見なされ、回線個別のパケット制御が不可となる。またユーザに提供する回線の閉域性という観点からも問題である。

そのため通信事業者のネットワーク内では、Match 条件によるフローの識別の他に、ユーザのフローをネットワーク内でユニークに識別するための仕組みが必要となる。

2. ユーザフローの識別

通信事業者のネットワーク内でユーザのフローを識別するための仕組みとして、ユーザのフロー毎にネットワーク内でユニークとなるタグを付与する方法が考えられる。以降ではユーザフローの識別のために付与するタグを「網内タグ」と呼ぶ。

通信事業者のネットワークの入口（エッジノード）においてユーザのパケットを識別・分類し、別途管理するユーザのフローと網内タグの対応関係に従い、エッジノードにてパケットに網内タグの付与を行う。通信事業者のネットワーク内では網内タグに従い転送制御を行い、出口のエッジノードにおいて付与した網内タグの除去を行う。

OpenFlow ではタグの付加／削除は Actions における Push/Pop で制御が可能であり、使用するタグの種類としては、Ethernet（VLAN ID、PBB I-SID）、MPLS（Label）などが考えられる。ただし、使用する OpenFlow スイッチによって対応しているタグが異なる場合があるため注意が必要である。

3. 網内タグの考え方

使用する網内タグのビット数（アドレス空間）がネットワーク内に設定できるフロー数に影響するため、収容するフロー数を考慮して適切なタグを選定する必要がある。参考として網内タグと設定可能フロー数の関係を表 2-6 に示す。

表 2-6　網内タグと設定可能フロー数（参考）

タグ	ビット数	設定フロー数
VLAN ID	12 ビット	4,096 フロー
Label (MPLS)	20 ビット	1,048,576 フロー
PBB I-SID	24 ビット	16,777,216 フロー

ユーザのフローをユニークに識別するための網内タグの付与の方法はいくつか考えられる。

図 2-24 は管理するネットワーク全体でユニークとなるよう、ユーザのフロー毎に網内タグを設定する方法である。ネットワーク内の 6 つのフローに対してユニークとなるよう、網内タグも 6 つの ID を付与して識別する。

この方法はネットワーク内で網内タグが一意に定まるため網内タグの管理は容易であるが、多数のフローを収容する場合は多数の網内タグを使用することになるため、設定可能フロー数に制約が生じる場合がある。

図 2-25 はリンク内でユニークとなるよう、ユーザのフロー毎に網内タグを設定する方法である。この場合は各 SDN ノードの IN_PORT の情報と合わせて網内タグの ID を付与して識別する。

この方法は各リンクで網内タグの ID の使い回しができるため、タグのアドレス空間を有効に活用することができるが、リンクを通過する毎に各ノードで網内タグの付け替え（Pop/Push）が発生するとともに、各リンク別にフローと網内タグの対応を制御する必要があり管理が複雑となる。

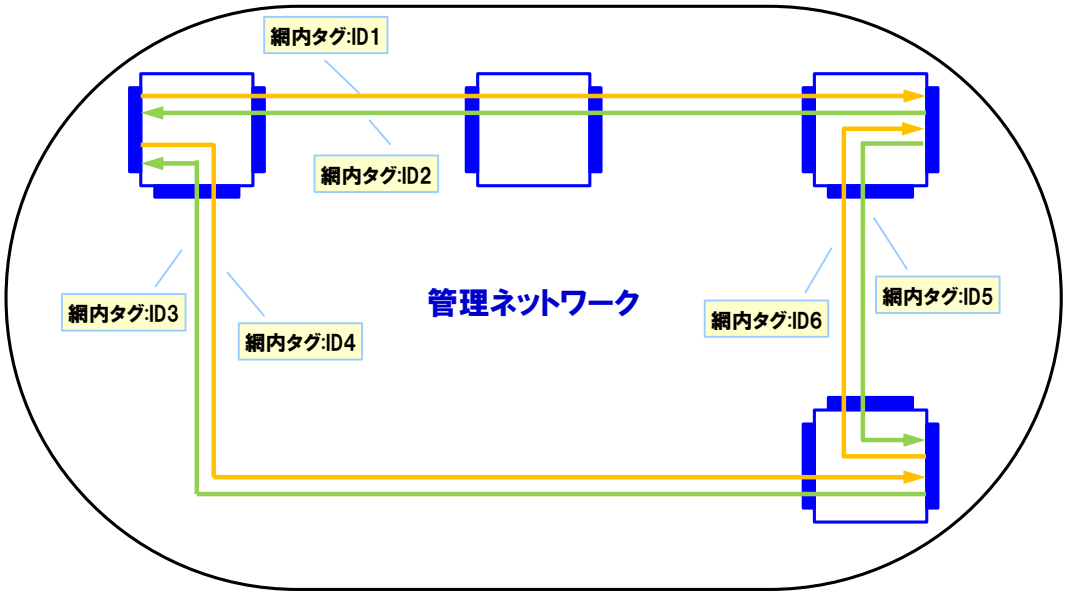


図 2-24　網内タグをネットワーク全体でユニークに付与

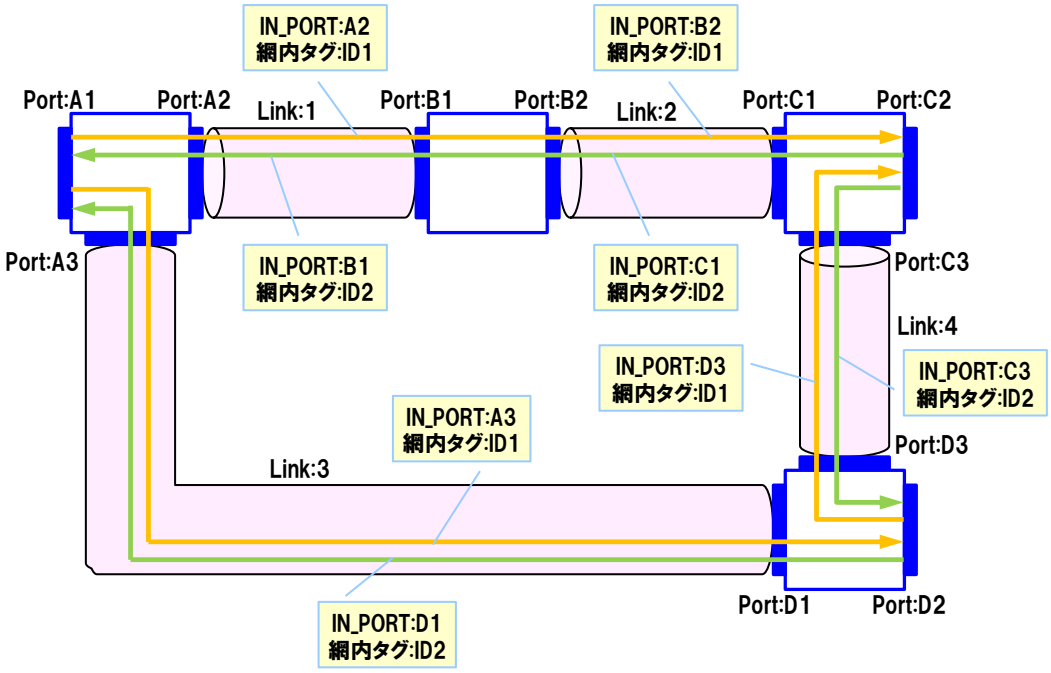


図 2-25　網内タグをリンク内でユニークに付与

第3節 中継パスの適用

1. 中継パスの基本的な考え方

ネットワークに多数のユーザを収容した場合、多数の回線やフローを管理する必要があり、大量のパケットが通過するネットワーク内のコアノードでは、処理負荷の増加やフローエントリ数の制限が課題となる懸念がある。そのため、第 2 節に示すユーザフローの分離の考え方を応用して、複数の回線を集約して中継パスとして管理し、設計や運用の効率化を図る方法を考える。

具体的には宛先に応じて複数の回線を束ね、束ねた回線を中継パスとして管理し、中継パス単位に網内タグを再設定する。SDN ノードをエッジとコアで機能分担し、エッジノードは回線を識別して宛先に応じた中継パスに収容する（中継パス用の網内タグを付与する）。コアノードは中継パスを識別する網内タグのみをみて宛先のエッジノードまでパケットを転送する。

中継パスのイメージを図 2-26、図 2-27 に示す。

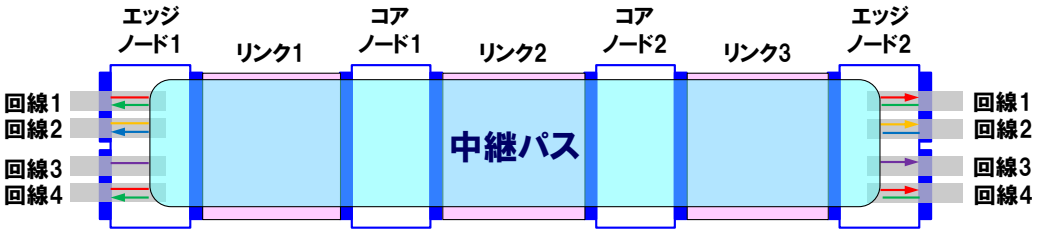


図 2-26　中継パスに回線を集約

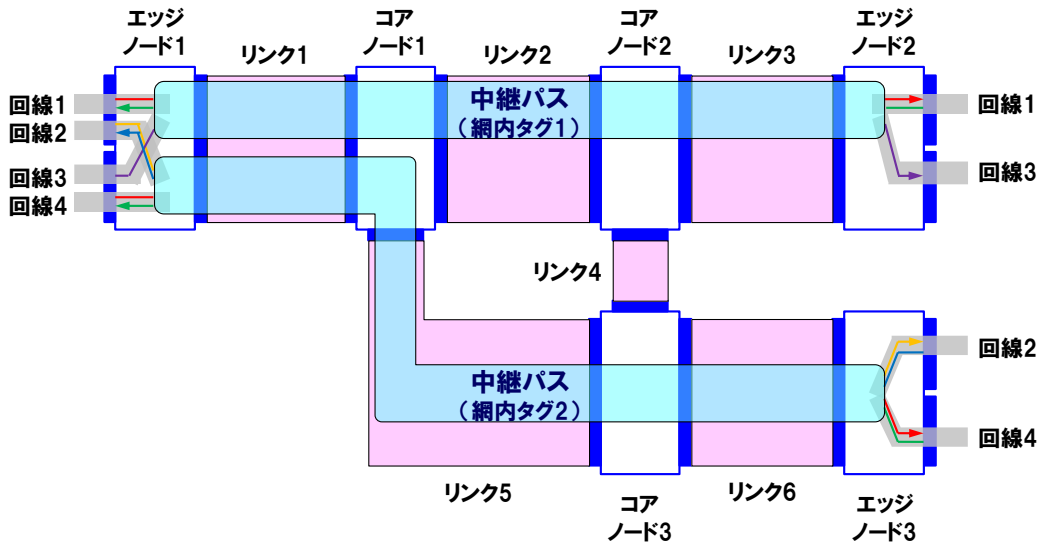


図 2-27　宛先別の中継パスを設定

2. 中継パス適用の効果

中継パスを適用した場合、コアノードは中継パスのみをハンドリングすればよく、コアノードの負荷軽減が期待できる。中継パスを適用した際のコアノードに対する効果を以下に示す。

- 中継パスを識別するタグのみをみて中継。
  - ➢ ノード装置の負荷軽減
- フロー集約によるフローエントリ節減。
- 中継パス単位の監視、保守、切替えが可能。
  - ➢ 運用の効率化
- 処理が単純でありハードウェアスイッチに向く。

第4章 本ガイドラインの基本的なネットワークモデル

第1節 基本的なネットワークモデルの定義

「第２編第２章 SDN NW の設計・構築」及び「第３章 仮想 NW の設計・構築」において示した設計・構築の考え方に基づき、本ガイドラインにおける基本的なネットワークの構成を図 2-28 のモデルで定義する（以降は「ネットワーク基本モデル」と呼ぶ)。以降では本章に示すネットワーク基本モデルを想定して解説を行うものとする。

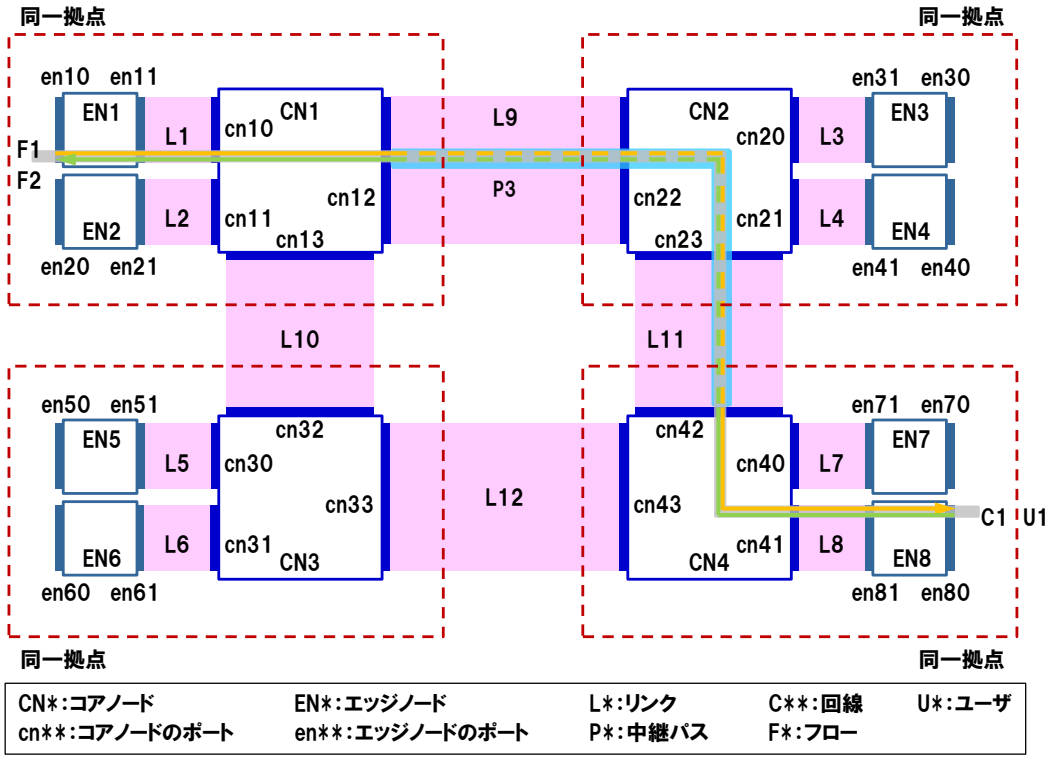


図 2-28　基本的なネットワークモデル（ネットワーク基本モデル）

ネットワーク基本モデルは、SDN ノード及び SDN ノード間のリンクで構成される「SDN NW」、その上位階層として、フローと回線及び中継パスで構成される「仮想 NW」として考える。

SDN ノードは機能分担を考慮し、エッジノードとコアノードを区別して考える。エッジノードはユーザの回線を収容し、回線に応じた網内タグの管理を行う機

能を有する。コアノードは複数の回線を束ねて中継パスに収容し、コアノード間は網内タグを利用してパケット転送を効率的に行う機能を有する。基本的にはコアノードの配下に複数のエッジノードが接続され、各々のノードは同一の拠点に設置されているものと考える。

第2節 中継パスの設定

ネットワーク基本モデルは、コアノード間に中継パスが設定されると考える。図 2-29 ではコアノード（CN1、CN2、CN3、CN4）に対して、中継パス（P1、P2、P3、P6）が設定されている例である。

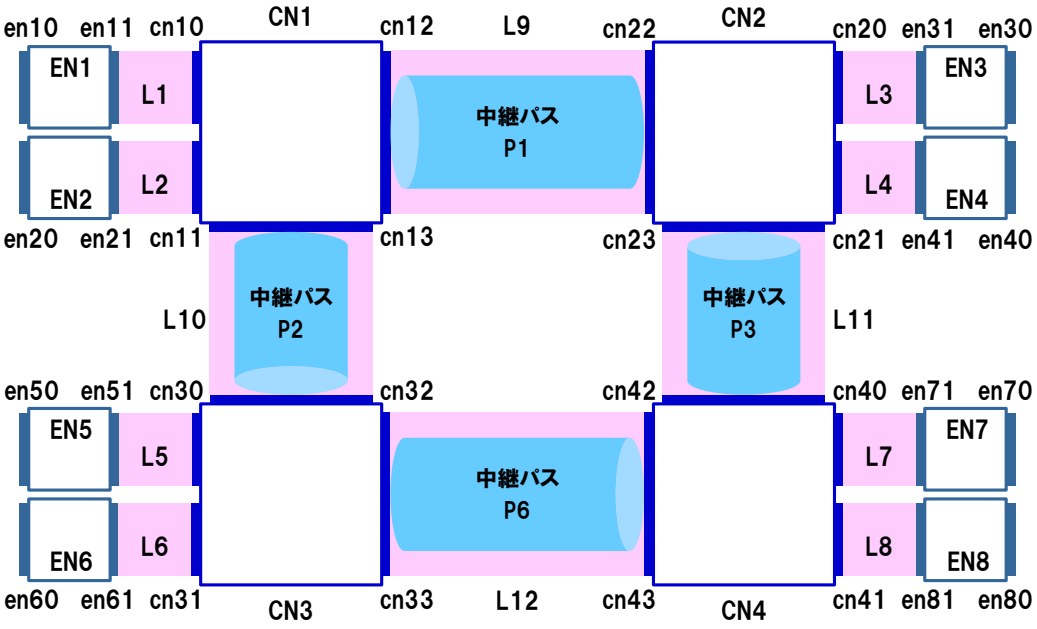


図 2-29　中継パスの設定

図 2-30 は全てのコアノード間に直通となる中継パスを 1 本ずつ設定した例である。例えばコアノード CN1 と CN2 の間の通信は中継パス P1 を使用するが、CN1 と CN4 の間の通信は中継パス P3 を使用することになり、宛先のコアノードに応じた中継パスを選択して使用する。この構成の場合、中継パスに異常が発生した際に迂回するための中継パスが設定されていないため、中継パスの切替えを行うことができない。

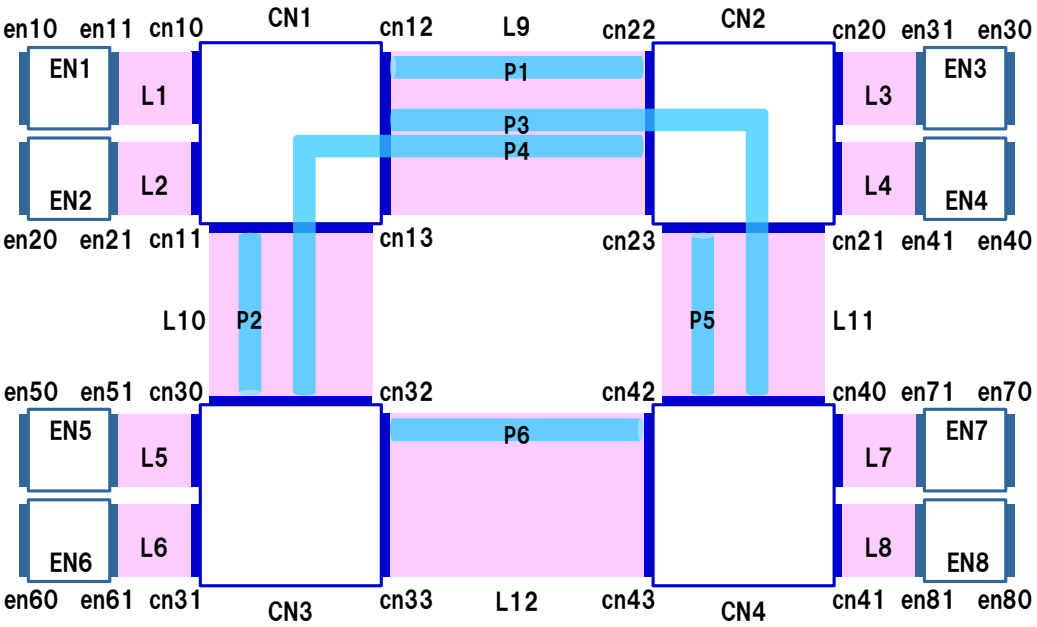


図 2-30　中継パスの設定（冗長構成なし）

図 2-31 は、図 2-30 の構成に対して中継パスの冗長化を行った例である。例えばコアノード CN1 と CN4 の間には現用系の中継パス P3 と、P3 とは逆方向となる予備系の P9 の 2 本の中継パスが設定されている。コアノード間の 2 本の中継パスは重複しない予備の経路を持つことになり、中継パスの異常が発生した際には中継パス単位での切替えが可能となり、ネットワークの信頼性が向上している。

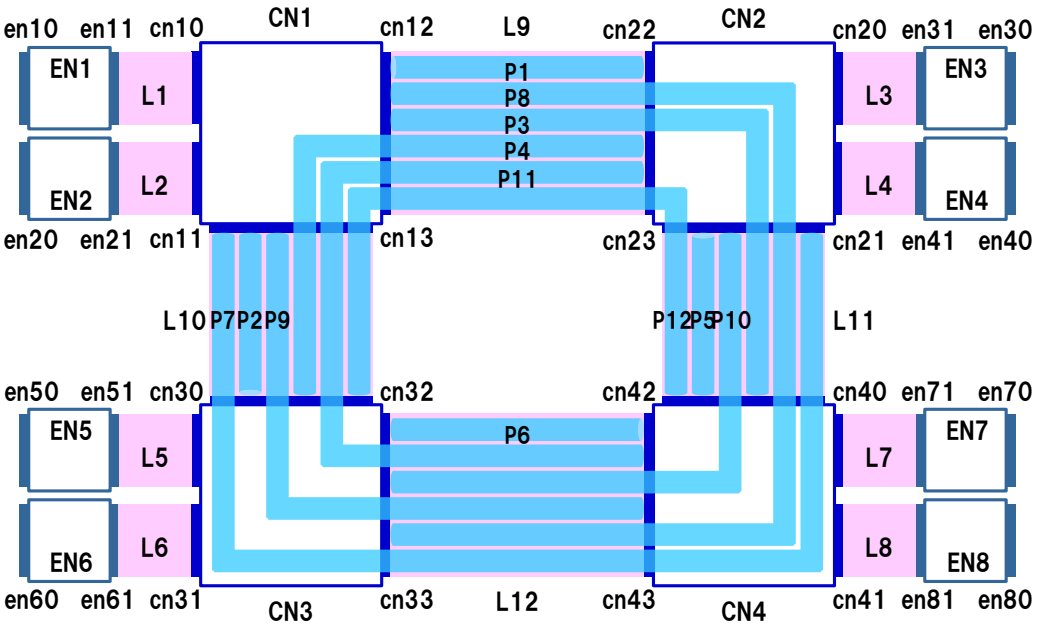


図 2-31　中継パスの設定（冗長構成あり）

第3節 回線の設定

ネットワーク基本モデルは、ユーザにネットワークサービスを提供するにあたり、回線及び回線を構成するフローが設定されると考える。図 2-32 ではエッジノード EN1 のポート en10 と、エッジノード EN7 のポート en72 間に、両方向の基本回線 C1 を設定した例である。基本回線 C1 は方向の異なる 2 つのフロー（F1、F2）で構成されている。

エッジノード EN1 からは、コアノード CN1、CN2、CN4 を経由してエッジノード EN7 に到達する。コアノード間は、CN1 と CN4 の間に設定された中継パスを使用してパケットが転送される。

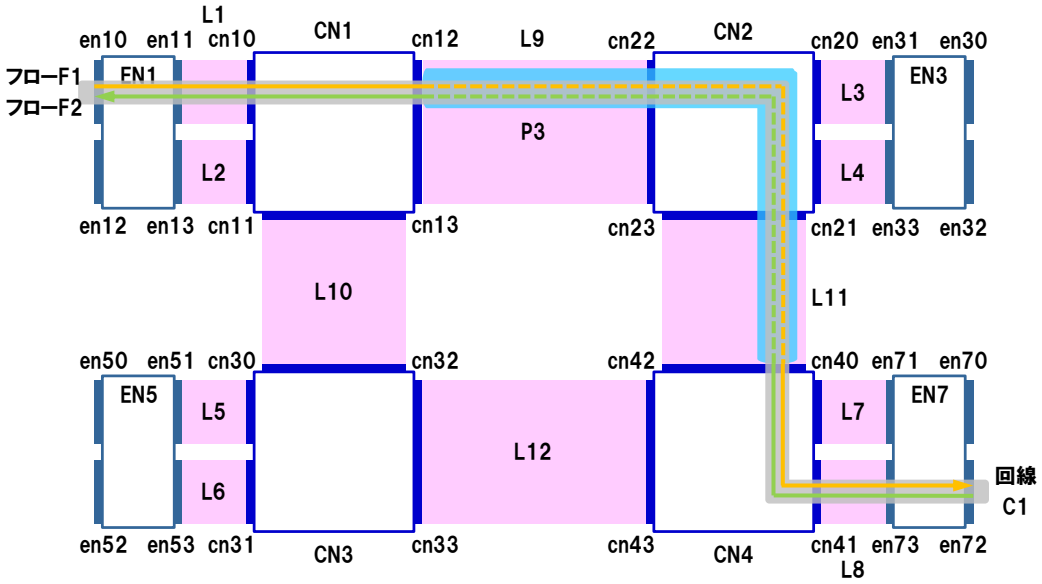


図 2-32　回線の設定

第4節 ネットワークの多面構成

ネットワークの高信頼化の対策のひとつとして、従来の伝送系ネットワークでは「多面構成」があり、SDN を用いたネットワークにおいても同様に考えることができる。「SDN NW」階層において複数の「面」を構築し、「仮想 NW」階層において各面へ分散させることで冗長化を図る考え方である。以降ではネットワーク基本モデルにおける多面構成の考え方を示す。

1. 2 面構成

「SDN NW」階層を 2 面構成とし、エッジノードを双方の面のコアノードに収容することで、ネットワークの高信頼化が図れる。図 2-33 はコアノード CN1～CN4 で構成する「A 面」と、コアノード CN5～CN8 で構成する「B 面」を構築した「2 面構成」の例である。

ユーザ U1 がエッジノード EN1～EN2 間で冗長ありの回線 C11 を契約した場合、平常時に使用する基本回線（Act：アクティブ）を A 面に設定し、バックアップ用の異経路を通る冗長回線（Sby：スタンバイ）を B 面に設定する。現用系の A 面に異常が発生した際には、予備系の B 面に切替えることでネットワークサービスを継続できる。

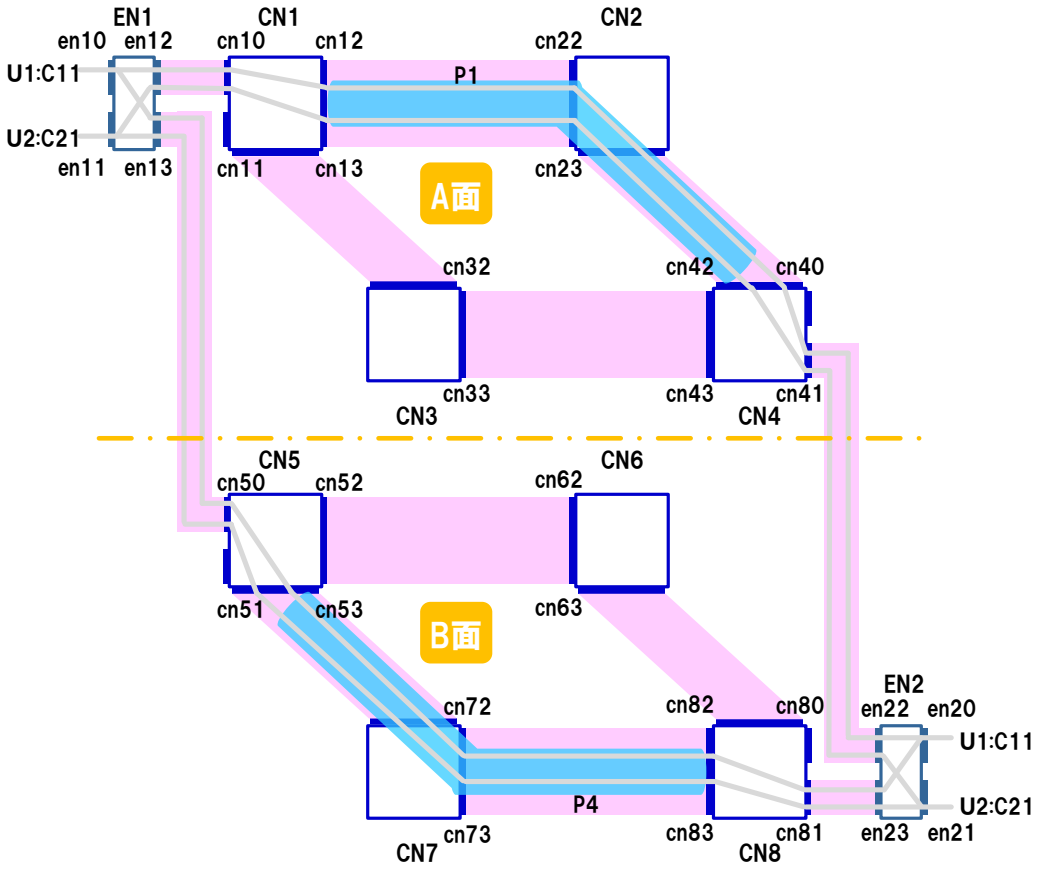


図 2-33　2 面構成の例

2. n+1 面構成

ネットワークの多面構成では、面単位で設備の増設を行うことでネットワークの拡張が可能である。例えばネットワークの設備が収容限界に達した場合に、新たな面を追加構築することで、ネットワーク全体の収容量の向上を図る。

図 2-34 は A 面、B 面の「2 面構成」のネットワークに対して、C 面を増設した例である。この場合、A 面を、B 面と C 面の共通の予備設備と考え、B 面と C 面のバックアップ回線を A 面に設定することで、ネットワークの「n+1 面構成」が実現できる。

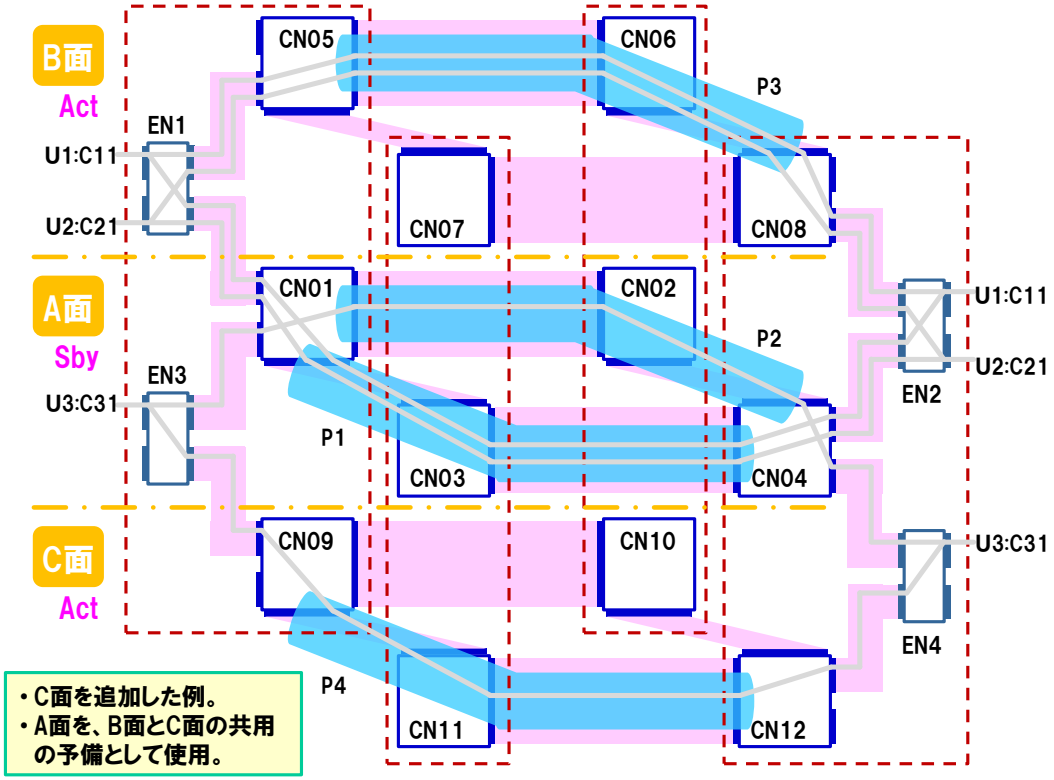


図 2-34　n+1 面構成の例

3. 多面構成における中継パスの設定

図 2-35 は A 面／B 面の 2 面構成において、各面のコアノード間に冗長なしの中継パスを設定した例である。中継パスに異常が発生した際には、他方の面に切替えることでサービスの継続を図る。

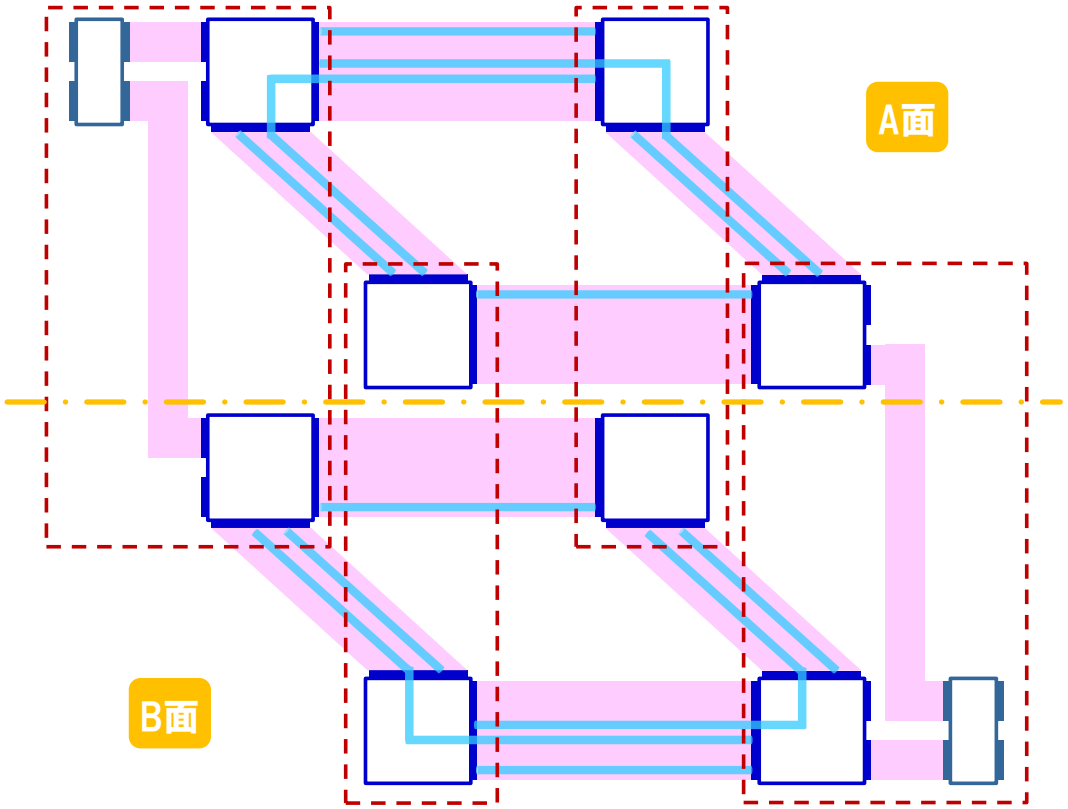


図 2-35　多面構成における中継パスの設定（冗長構成なし）

図 2-36 は、図 2-35 の構成に対して各面で中継パスの冗長化を行った例である。中継パスに異常が発生した際には、面内での切替えと面間での切替えが可能となり、ネットワークの信頼性がより向上している。

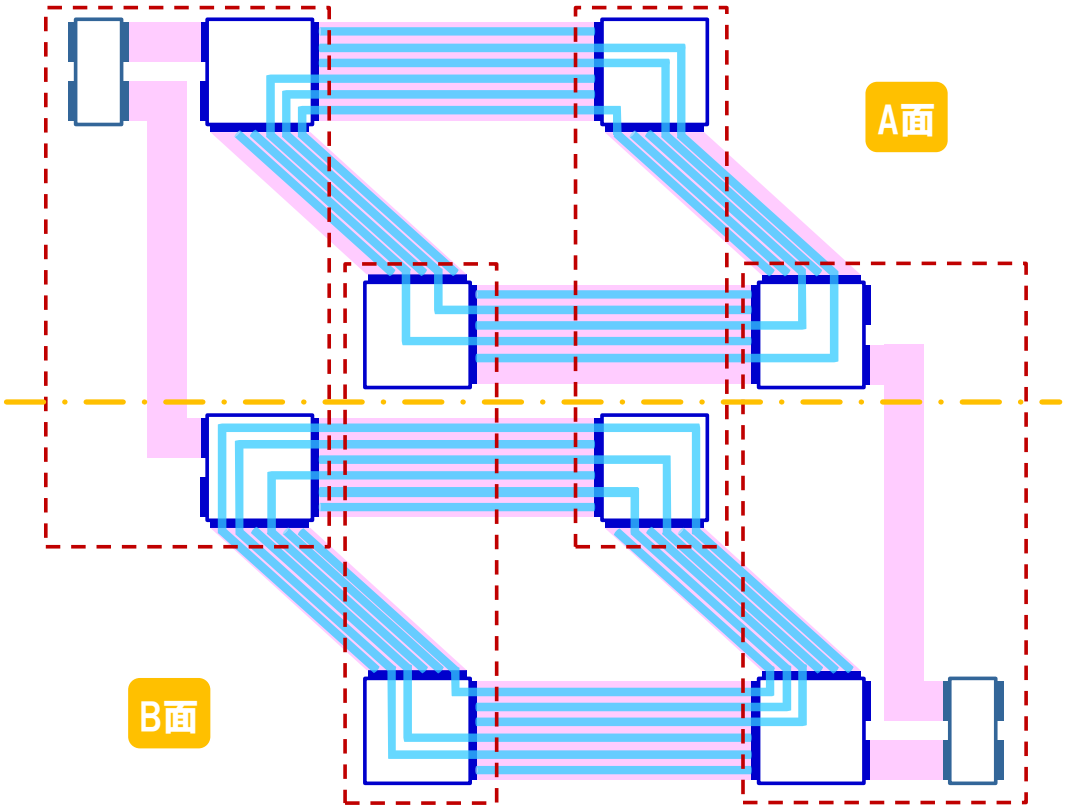


図 2-36　多面構成における中継パスの設定（冗長構成あり）

表 2-7 に示すように、方式 1（図 2-35）では、中継パス数が少なく、必要となる帯域も少ないが、中継パスに異常が発生した際には、A 面に迂回のための中継パスが設定されていないため、回線単位で A 面から B 面への切替えが必要になる。一方、方式 2（図 2-36）では、中継パス数が多くなり、必要となる帯域も増えるが、中継パスに異常が発生した際には、A 面内での中継パス単位での切替えのほか、A 面から B 面への面間での切替えも可能な構成となる。

異常発生時のネットワークサービスへの影響を極力少なくする場合には、方式 2 が望ましい。

表 2-7　中継パス設定方式の比較

	方式 1（図 2-35）	方式 2（図 2-36）
中継パスの数	・ A 面：6 本 ・ B 面：6 本	・ A 面：12 本 ・ B 面：12 本
中継パスの帯域（契約帯域を「1」とした場合の比較）	・ 面内で最大 1 倍の帯域。 ・ 面間での切替えを考慮し、ネットワーク全体では最大 2 倍の帯域。	・ 中継パスの切替えを考慮し、面内で最大 2 倍の帯域。 ・ 面間での切替えを考慮し、ネットワーク全体では最大 4 倍の帯域。
中継パス異常時の切替え	・ A 面内での中継パスの切替えは不可。 ・ 回線単位で A 面から B 面への切替えが必要。	・ A 面内での中継パスの切替えが可能。 ・ 回線単位での A 面から B 面への切替えも可能。

第5章 情報の管理

第1節 情報モデル

通信事業者が回線サービスを提供するにあたり、必要となる情報の管理の考え方について例を用いて示す。

通信事業者が管理する情報を、「ユーザ」「契約」「回線」「フロー」「ポート」「リンク」「ノード」のオブジェクトで構成されるモデルとして表現する（図 2-37）。「ユーザ」「契約」「回線」についてはサービスを管理するために必要な情報、「フロー」「ポート」「リンク」「ノード」についてはネットワークを管理するために必要な情報である。なお、本モデルはユーザに提供する回線を管理するための情報を示し、通信事業者が内部で使用する回線（管理用など）は考慮していない。

次項からは各オブジェクトについて解説する。

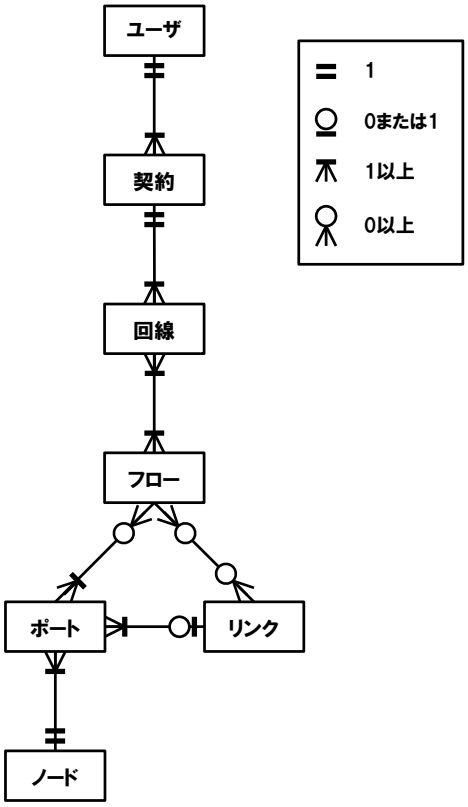


図 2-37　情報モデル

第2節 ユーザオブジェクト

ユーザは回線サービスの利用者である。契約のオブジェクトで構成される（図2-38）。

1ユーザに対して複数の契約情報が取り得る。

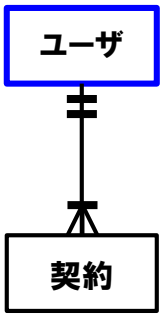


図 2-38　ユーザオブジェクト

第3節 契約オブジェクト

ユーザは回線サービスを利用するために通信事業者と契約を結ぶ。ユーザ、回線のオブジェクトで構成される（図 2-39)。

1 契約に対して複数の回線情報が取り得る。

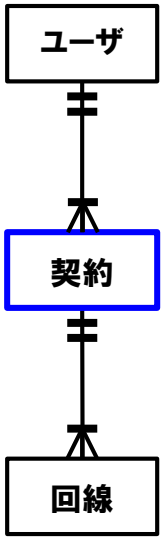


図 2-39　契約オブジェクト

第4節 回線オブジェクト

回線は 1 つ以上のフローで構成される Point-to-Point の通信であり、通信事業者のサービスの提供単位である。契約、フローのオブジェクトで構成される（図 2-40）。

1 回線は複数のフロー情報で構成される場合がある。また 1 フローは複数の回線で使用する場合がある。

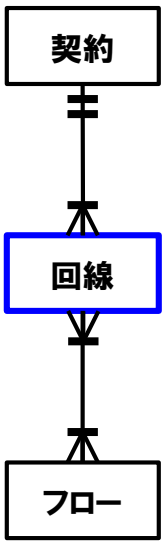


図 2-40　回線オブジェクト

回線オブジェクトがもつデータ属性の例を表 2-8 に示す。

表 2-8　回線オブジェクトのデータ属性の例

データ属性	概要
回線-ID	・ 回線にユニークに割り振られた識別子。
ロケーション	・ 回線の始点と終点を示すユーザの拠点を示す情報。
関連フロー	・ 回線を構成するフローを示す情報。
回線オプション	・ 回線オプションの有無や、オプションの内容を示す情報。
帯域	・ ユーザが契約した回線の帯域を示す情報。
関連契約	・ 回線情報と契約情報を紐付けるための情報。

第5節 フローオブジェクト

フローは回線を構成するノードとリンクを通過するパケットの通り道であり、End-to-End で片方向に設定される。回線、ポート、リンクのオブジェクトで構成される（図 2-41）。

フローと回線の関係は、1 フローは複数の回線で使用する場合がある。また 1 回線は複数のフローで構成される場合がある。

フローとポートの関係は、1 フローは複数のポートの情報で構成される。また 1 ポートには複数のフローが設定される場合があるが、フローが設定されていないポートも取り得る。

フローとリンクの関係は、1 フローはリンクなし、または複数のリンクの情報で構成される。リンクのないフローとは、ネットワーク間のタグの付け替え処理のみのフローなど、フローがノード内の IN_PORT と OUT_PORT で終端するような場合である（図 2-42）。また 1 リンクには複数のフローが設定される場合があるが、フローが設定されていないリンクも取り得る。

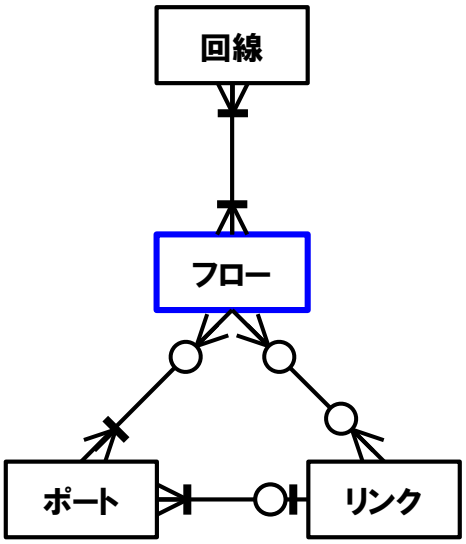


図 2-41　フローオブジェクト

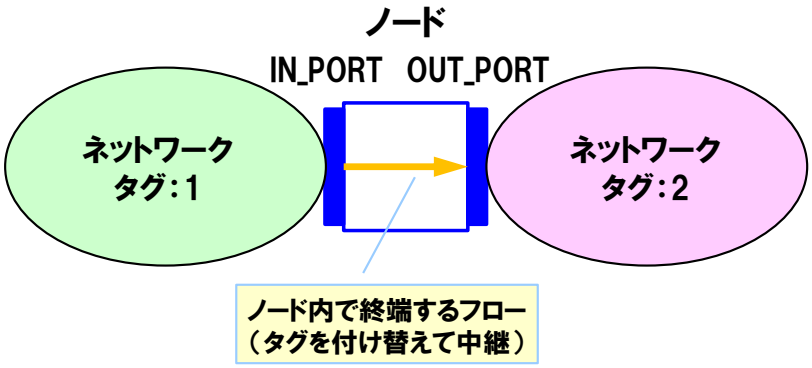


図 2-42　リンクのないフローの例

フローオブジェクトがもつデータ属性の例を表 2-9 に示す。

表 2-9　フローオブジェクトのデータ属性の例

データ属性	概要
フロー-ID	・ フローにユニークに割り振られた識別子。
経路情報	・ フローが通る経路を示す情報。 ・ 経由するノード、ポート、リンクで構成される。
Match 条件	・ パケットを識別するための Match 条件を示す情報。 ・ 条件と該当ノードの情報で構成される。
Meter 情報	・ フローの統計情報や、統計量に応じた制御方法を示す情報。
関連回線	・ フロー情報と回線情報を紐付けるための情報。

第6節 ポートオブジェクト

ポートはノードが 2 つ以上有してリンクを接続する。またフローの端点となる。フロー、リンク、ノードのオブジェクトで構成される（図 2-43）。

ポートとフローの関係は、1 ポートには複数のフローが設定される場合があるが、フローが設定されていないポートも取り得る。また 1 フローは複数のポートで構成される。

ポートとリンクの関係は、1 ポートに対してリンクが存在する場合としない場合がある。また 1 リンクは複数（2 つ）のポートで構成される。

ポートとノードの関係は、1 ポートに対して一意のノードが定まる。また 1 ノードには複数のポートが存在する。

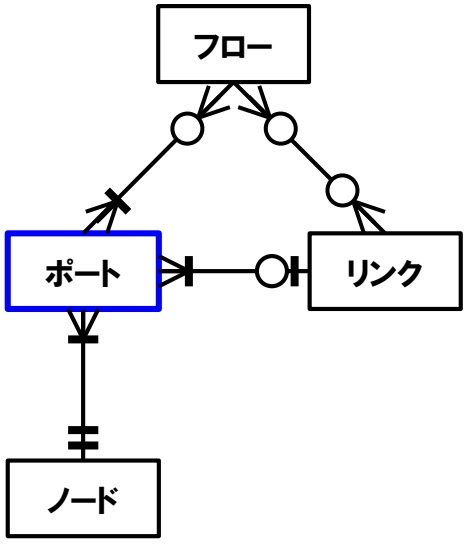


図 2-43　ポートオブジェクト

ポートオブジェクトがもつデータ属性の例を表 2-10 に示す。

表 2-10　ポートオブジェクトのデータ属性の例

データ属性	概要
ポート-ID	・ ポートにユニークに割り振られた識別子。
関連ノード	・ ポートが存在するノードを示す情報。
関連リンク	・ ポートが接続するリンクを示す情報。
関連フロー	・ ポート情報とフロー情報を紐付けるための情報。

第7節 リンクオブジェクト

リンクはノード - ノードのポート間を繋ぐもの（物理／論理）である。フロー、ポートのオブジェクトで構成される（図 2-44）。

リンクとフローの関係は、1 リンクに対して複数のフローが設定される場合があるが、フローが設定されていないリンクも取り得る。また 1 フローは複数のリンクで構成される。

リンクとポートの関係は、1 リンクは複数（2 つ）のポートで構成される。また 1 ポートに対してリンクが存在する場合としない場合がある。

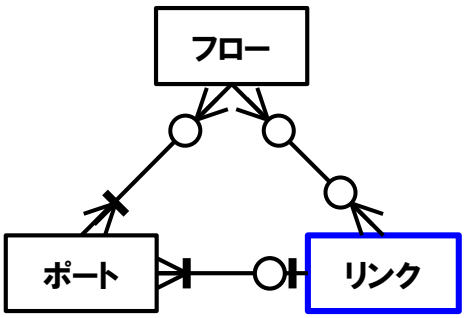


図 2-44　リンクオブジェクト

リンクオブジェクトがもつデータ属性の例を表 2-11 に示す。

表 2-11　リンクオブジェクトのデータ属性の例

データ属性	概要
リンク-ID	・ リンクにユニークに割り振られた識別子。
関連ポート	・ リンクが存在するポートを示す情報。
帯域	・ リンクの帯域を示す情報。
関連フロー	・ リンク情報とフロー情報を紐付けるための情報。

第8節 ノードオブジェクト

ノードはデータプレーン機能を搭載する SDN ノードであり、OpenFlow スイッチなどの SDN 対応スイッチが該当する。ポートのオブジェクトで構成される（図 2-45）。

1ノードは複数のポートをもつ。また1ポートに対して一意のノードが定まる。

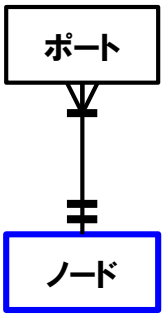


図 2-45　ノードオブジェクト

ノードオブジェクトがもつデータ属性の例を表 2-12 に示す。

表 2-12　ノードオブジェクトのデータ属性の例

データ属性	概要
ノード-ID	・ ノードにユニークに割り振られた識別子。
関連ポート	・ ノードに存在するポートを示す情報。
関連フロー	・ ノード情報とフロー情報を紐付けるための情報。

第3編 運用・監視フェーズ

通信事業者がネットワークサービスを提供するにあたって、一般的に設計、構築、運用、監視といった業務フェーズがある。本ガイドラインは一般的な業務フェーズに則すものとし、第 2 編では設計・構築について、第 3 編では運用・監視について、通信事業者のネットワークに SDN を用いるための基本的な考え方を示す。

- 第 2 編 設計・構築フェーズ
- 第 3 編 運用・監視フェーズ

SDN を用いたネットワークの運用・監視に関して、基本的には従来のネットワークの考え方と大きく変わるものではない。ネットワークの状態を常時把握し、異常発生時には、その検出と対処を行うことがポイントとなる。また下位レイヤを含めて、リソース管理や収容管理のデータが一元的に管理できれば、レイヤにまたがるリソース配分の最適化や、故障発生時の切替え、被疑箇所の推定などの運用の効率化が図れる。

第1章 運用・監視フェーズの基本的な考え方

第1節 運用・監視フェーズの位置付け

運用・監視フェーズとは、SDN を用いた通信事業者のネットワークにおいて各種ネットワークサービスの提供を開始し、提供したネットワークサービスの維持・管理を行うフェーズである。ネットワークサービスを構成するフローは「SDN NW」のリソースを利用して「仮想 NW」に設定されるため、「SDN NW」と「仮想 NW」のネットワーク階層を中心に考えるものとし、「SDN NW」ではデータプレーンとコントロールプレーンについての運用・監視が必要となる。

データプレーンに関しては、回線サービスの特性に応じてリンク及びノードの状態を把握し、異常発生時にはその検出と対処を行う。コントロールプレーンに関しては安定稼働のため SDN コントローラの冗長化を行い、SDN コントローラ間の監視や異常発生時の切替え方式が重要となる。

第2節 運用・監視フェーズのネットワークモデル

SDN を用いた通信事業者ネットワークの運用･監視の基本的な考え方を示すにあたり、第 2 編第 4 章で定義した基本的なネットワークモデル（ネットワーク基本モデル）を前提に解説するものとする。本節ではネットワーク基本モデルの要旨を再掲する。

1. 回線の設定

ネットワーク基本モデルは、ユーザにネットワークサービスを提供するにあたり、回線及び回線を構成するフローが設定されると考える。図 3-1 ではエッジノード EN1 のポート en10 と、エッジノード EN7 のポート en72 間に、両方向の基本回線 C1 を設定した例である。基本回線 C1 は方向の異なる 2 つのフロー（F1、F2）で構成されている。

エッジノード EN1 からは、コアノード CN1、CN2、CN4 を経由してエッジノード EN7 に到達する。コアノード間は、CN1 と CN4 の間に設定された中継パスを使用してパケットが転送される。

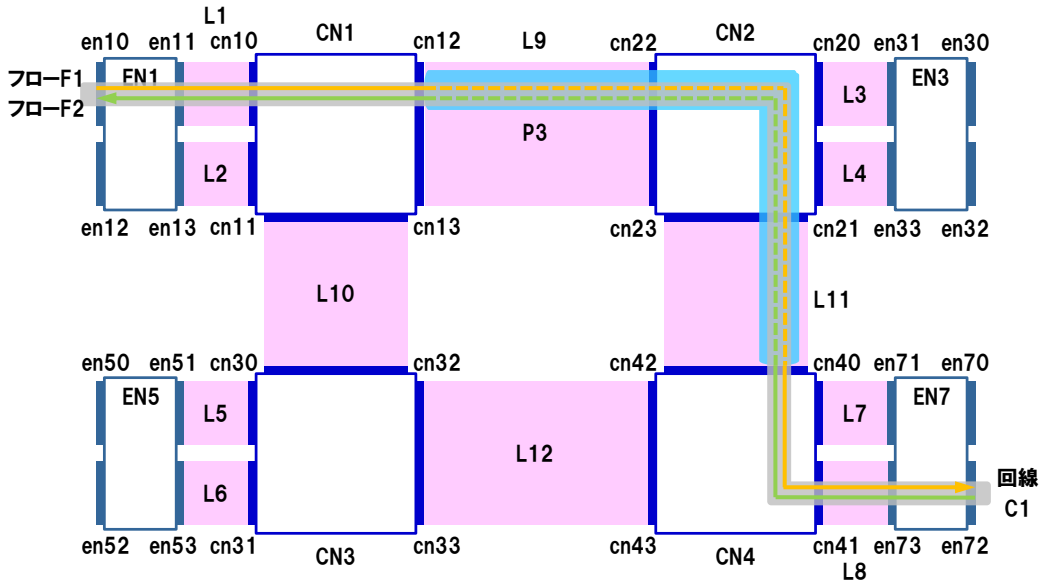

L1
en10
en11
cn10
CN1
cn12
L9
cn22
CN2
cn20
en31
en30
フローF1
フローF2
EN1
L3
EN3
P3
L2
L4
en12
en13
cn11
cn13
cn23
cn21
en33
en32
L10
L11
en50
en51
cn30
cn32
cn42
cn40
en71
en70
EN5
L5
L7
EN7
L12
回線
C1
L6
en52
en53
cn31
CN3
cn33
cn43
CN4
cn41
en73
en72
L8

図 3-1　回線の設定

2. 中継パスの設定

ネットワーク基本モデルは、コアノード間に中継パスが設定されると考える。図 3-2 ではコアノード（CN1、CN2、CN3、CN4）に対して、全てのコアノード間に直通となる中継パスが設定され、各中継パスは冗長化を行った例である。

例えばコアノード CN1 と CN4 の間には現用系の中継パス P3 と、P3 とは逆方向となる予備系の P9 の 2 本の中継パスが設定されている。コアノード間の 2 本の中継パスは重複しない予備の経路を持つことになり、中継パスの異常が発生した際には中継パス単位での切替えが可能となる。

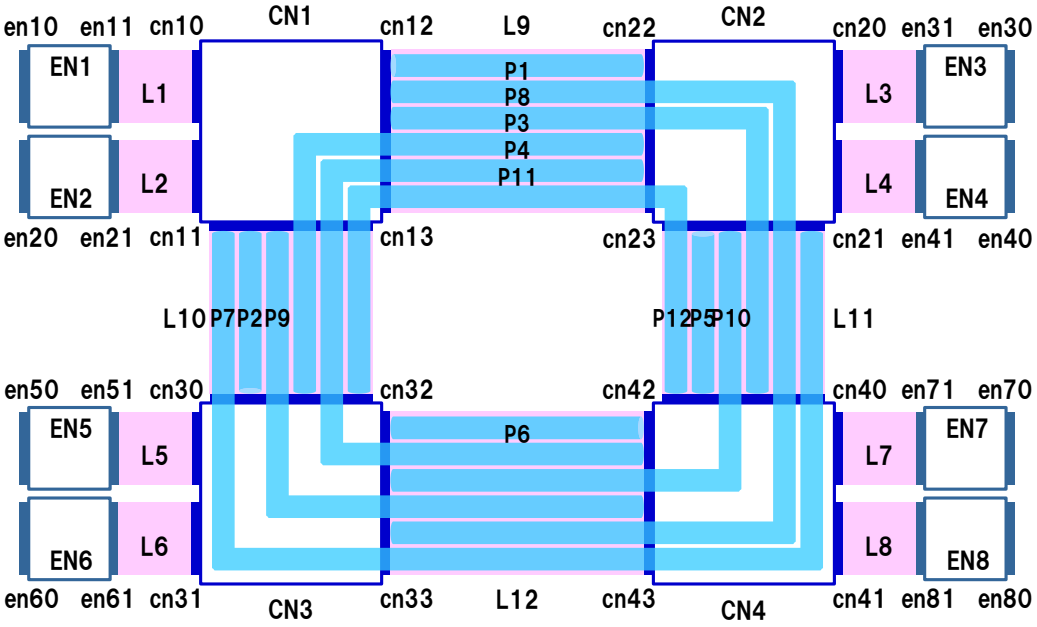


図 3-2　中継パスの設定（冗長構成あり）

また、多面構成では各面で中継パスの冗長化を行う（図 3-3）。中継パスに異常が発生した際には、面内での切替えと面間での切替えが可能となり、ネットワークの信頼性がより向上する。

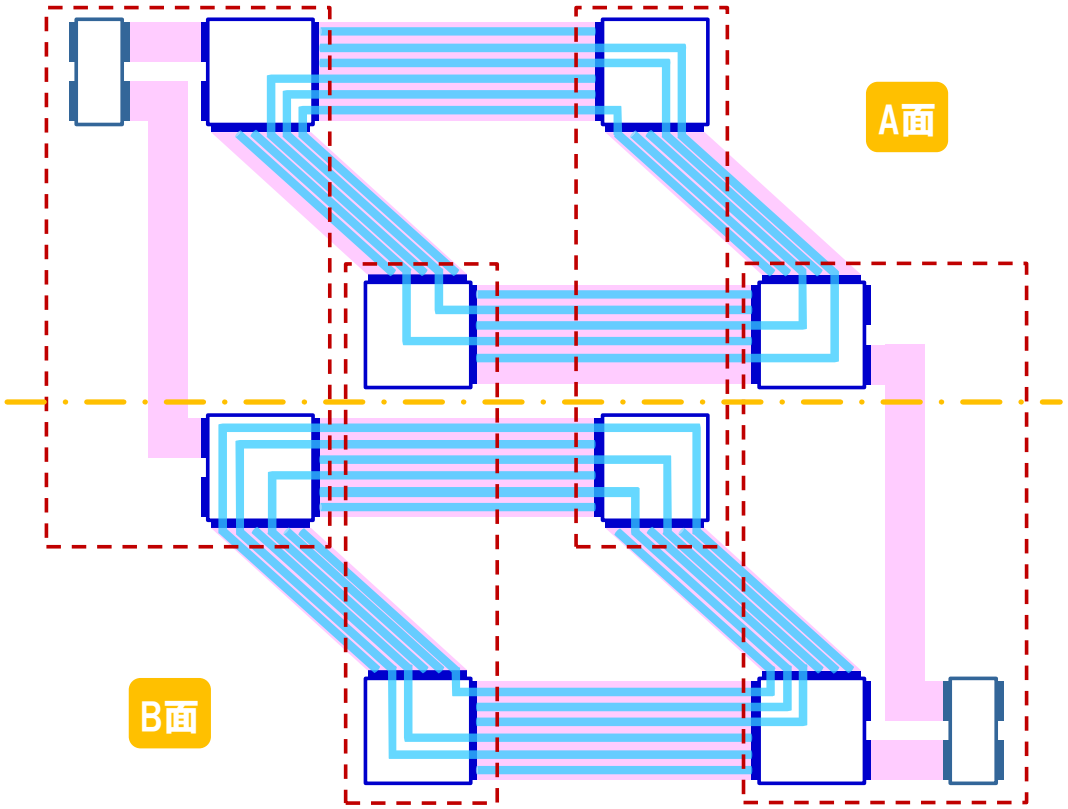


図 3-3　多面構成における中継パスの設定（冗長構成あり）

第3節 パケット経路に着目した回線パタン

OpenFlow で制御されるパケットの経路に着目し、回線サービスを 3 パタンに分類する。第 3 編 運用・監視フェーズでは本節に示す回線サービスを想定して解説するものとする。

- Point-to-Point 回線
- Drop 回線
- 分岐回線

1. Point-to-Point 回線

「Point-to-Point 回線」は 2 つの端点となるポート間で設定される基本回線である。パケットは OpenFlow の Actions における Output（指定されたポートからパケットを送出する）により、フローテーブルに指定された経路を流れる（図 3-4）。

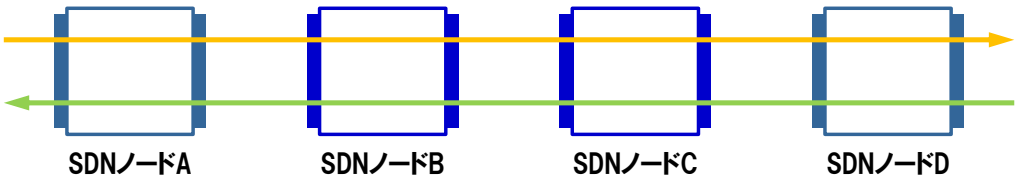


図 3-4　Point-to-Point 回線

2. Drop 回線

「Drop 回線」は経路の途中でパケットが廃棄される回線オプションである。パケットは OpenFlow の Actions における Drop により、経路の途中で廃棄される（図 3-5）。

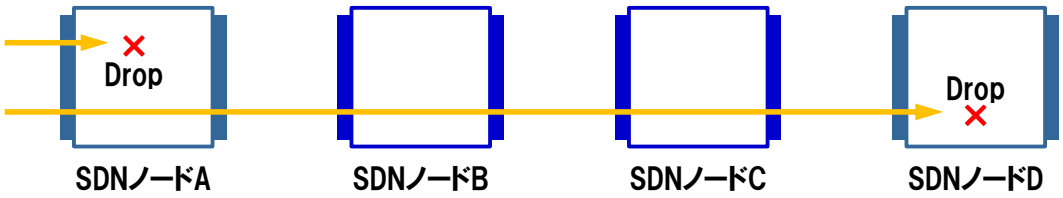


図 3-5　Drop 回線

3. 分岐回線

「分岐回線」は経路の途中でパケットをコピーし、複数の対地に対して通信を行う回線オプションである。パケットは OpenFlow の Group テーブル（グループ毎に Actions を指定した情報）等を使用することにより、複数の経路に分岐する（図 3-6）。

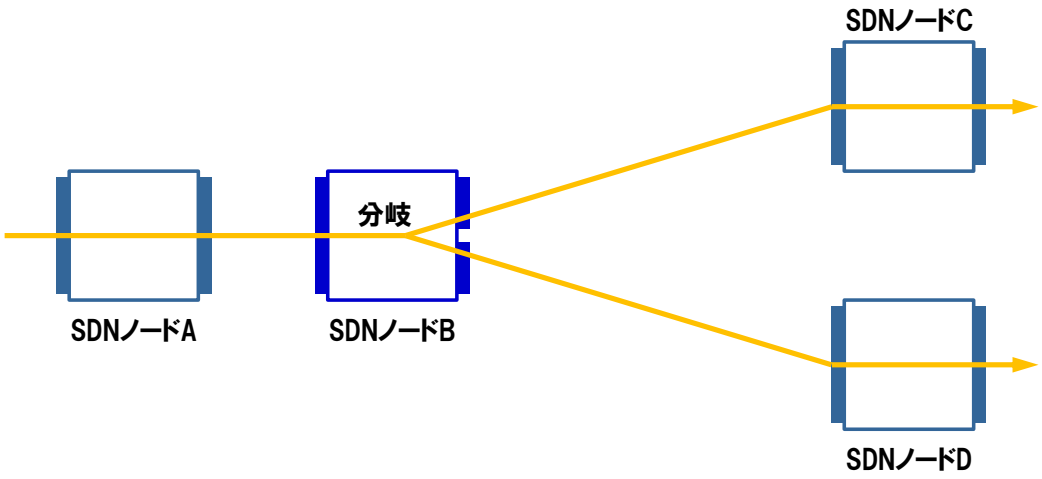


図 3-6　分岐回線

第4節 運用・監視フェーズのプロセス

通信事業者のネットワークサービス運用業務を、3 つのプロセスに分類する。第 3 編 運用・監視フェーズでは本節に示すプロセスを想定して解説するものとする。

1. 開通試験

ユーザへのサービスインの前に、設定したフローや回線に問題がないことを確認する。具体的には、回線の始点・終点間でパケットが疎通することや、パケットの経路に異常がないことを試験する。

2. 定期監視

ユーザへのサービスインの後に、設定したフローや回線に問題がないことを定期的に確認する。定期監視で問題が確認された場合には異常措置プロセスへ移行する。

3. 異常措置

定期監視で故障等の異常が検出された場合には、ネットワークの切替えにより被疑箇所を迂回させてネットワークサービスを回復するとともに、問題の発生した設備を正常状態に復旧させる。

第2章 運用・監視フェーズで使用する OAM ツール

第1節 OAM ツールの基本的な考え方

OAM とは「Operations Administration and Maintenance」の略で、ネットワークの保守・管理の機能を示し、OAM ツールを活用することで運用・監視の効率化が図れる。

例えば既存技術の Ethernet では「Ethernet OAM」として標準化がなされており（ITU-T「Y.1731」、IEEE「IEEE802.1ag」）、主な機能として Continuity Check（接続性確認）、Loop Back（IP における ping 相当）、Link Trace（IP における traceroute 相当）などが規定されている。Ethernet OAM 対応スイッチには OAM 機能が実装され、スイッチ間での運用・監視が行われる（図 3-7）。

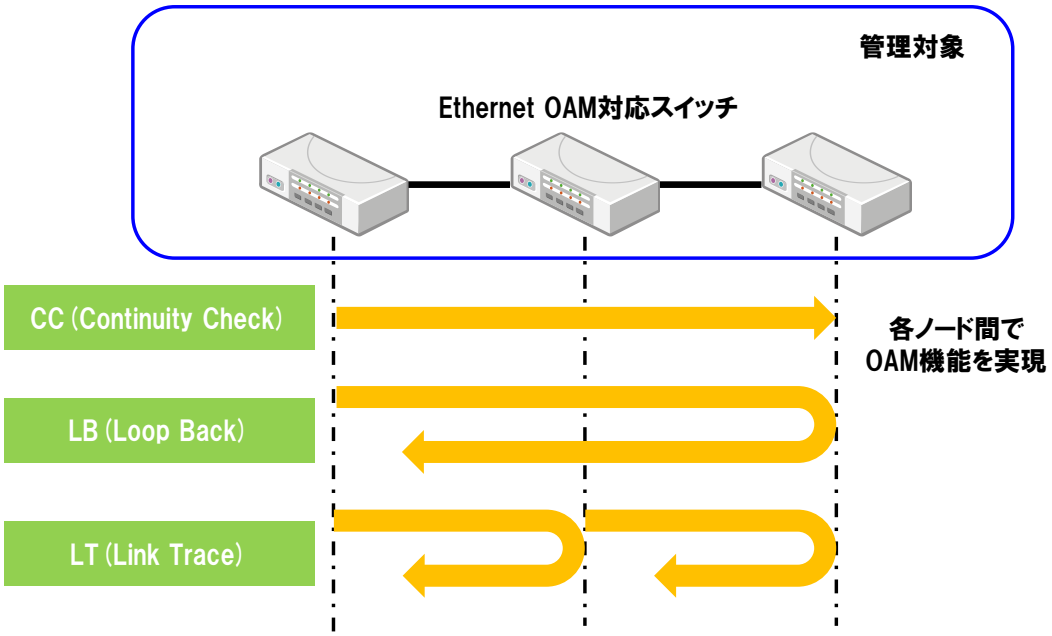


図 3-7 Ethernet OAM のイメージ

OpenFlow における OAM 機能の実現例のひとつとして、ネットワークアプリケーションとして OAM ツールを開発・導入する方法が考えられる。OpenFlow ではコントローラがコントロールプレーンの機能を担う集中制御型のアーキテクチャを採ることから、コントローラ（OFC）から試験対象スイッチに対して試

験パケットを送信（Packet-Out）／受信（Packet-In）することで OAM 機能を実現する（図 3-8）。

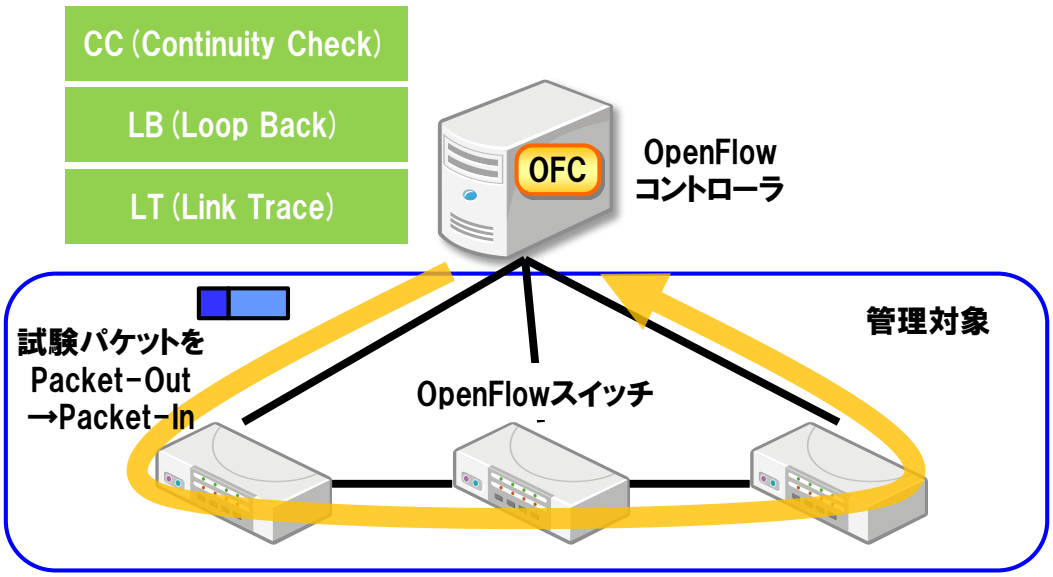


図 3-8　ネットワークアプリケーションによる OAM 機能の実現例

次節では本方式を用いた以下の OAM ツールについて実現例を示す。

- Continuity Check（CC）ツール
- Loop Back（LB）ツール
- Link Trace（LT）ツール

第2節 OAM ツールの実現例

1. Continuity Check ツール（CC ツール）

Continuity Check ツール（CC ツール）は、特定ノード間の疎通を確認するためのツールである。CC ツールの実現例を図 3-9 に示す。

コントローラより CC 試験パケットを入側ノードに Packet-Out し、フローテーブルに従いパケットを転送する。出側ノードでは試験パケットをコントローラへ Packet-In する。試験パケットが一定期間内に Packet-In されたら、指定したノード間は正常とみなす。

CC ツールによる疎通の確認は、回線レベル（エッジノード間）で試験を行う場合と、中継パスレベル（コアノード間）で試験を行う場合が考えられる。

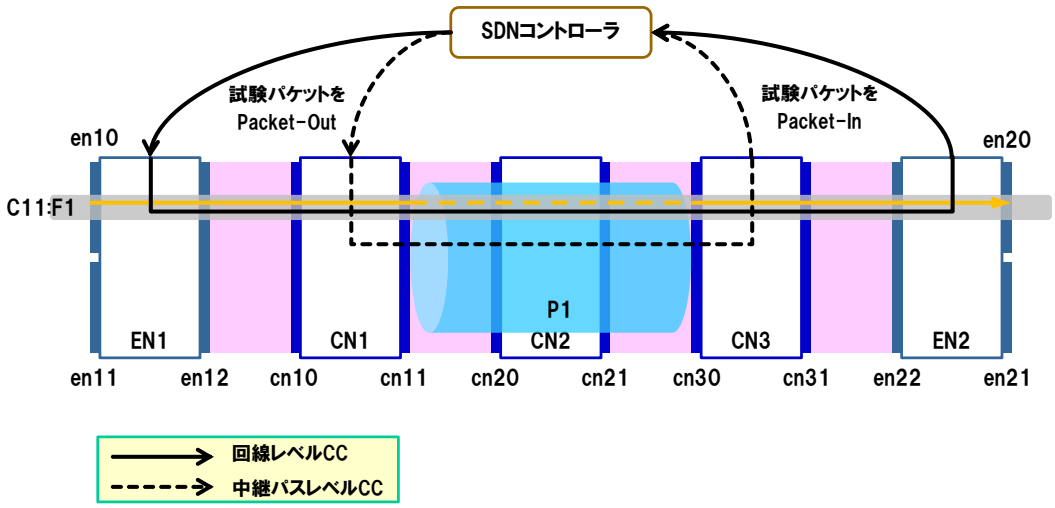


図 3-9　CC ツールの実現例

2. Loop Back ツール（LB ツール）

Loop Back ツール（LB ツール）は、故障等の被疑箇所を推定するためのツールである。LB ツールの実現例を図 3-10 に示す。

LB ツールでは CC ツールの機能を活用して、Loop Back と同等の機能を実現する。試験区間となる入側ノードを固定してコントローラより CC 試験パケット

（LB 試験パケットと同質）を Packet-Out し、出側のノードを順次変化させて複数回の CC ツールを実行することで、被疑箇所を絞り込む。異常が発生したノードの前後で CC ツールの成否の結果が変化するため、被疑箇所を推定できる。

このように、試験区間となる出側ノードで試験パケットが折り返す（IP における ping のように）試験ではないが、被疑箇所を推定するという Loop Back と同等の機能を実現できる。

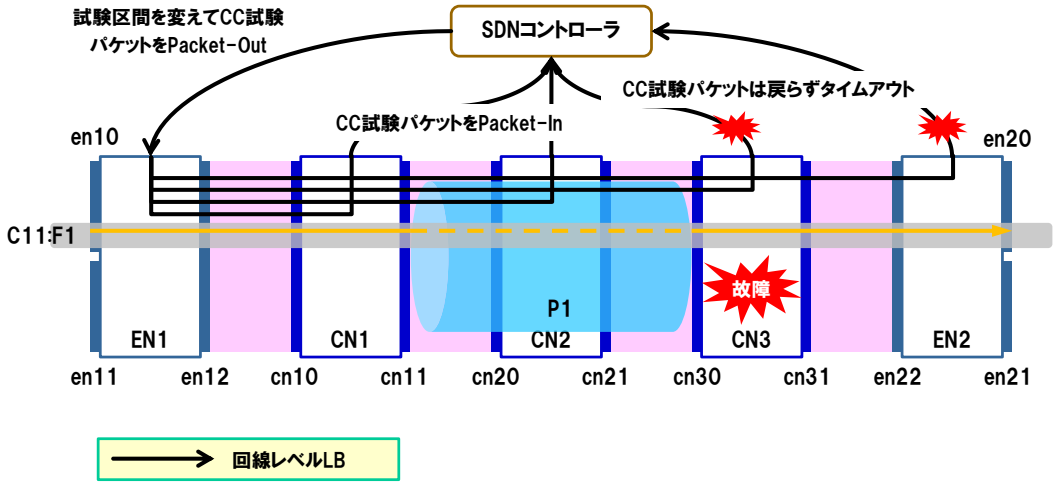


図 3-10　LB ツールの実現例

3. Link Trace ツール（LT ツール）

Link Trace ツール（LT ツール）は、特定のノード間の経路が正常であることを確認するためのツールである。LT ツールの実現例を図 3-11 に示す。

コントローラより LT 試験パケットを入側ノードに Packet-Out し、フローテーブルに従いパケットを転送する。経路途中のノードでは試験パケットの中継と合わせて試験パケットをコピー（分岐）し、必要な情報（dpid 等）を付加してコントローラへ Packet-In する。出側ノードでは試験パケットのコピーは行わずに、コントローラへ Packet-In する。コントローラは各ノードから Packet-In された試験パケットの IP ヘッダの TTL (Time To Live) を確認するなどして総合的に判断し、指定したノード間の経路を確認する。

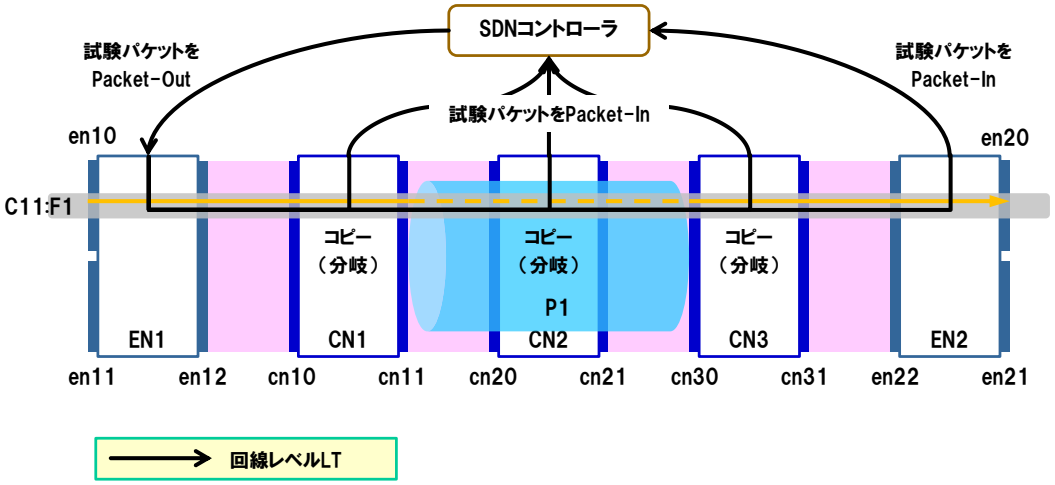


図 3-11　LT ツールの実現例

第3節 現行方式の課題と対策

前節に示した OAM ツールは、本来であればノード間で行うべき試験を、コントローラを介して行う実現例である。この方式はコントローラが試験パケットを送信（Packet-Out）／受信（Packet-In）する必要があるため、試験頻度が高い場合や、管理するスイッチ数が増加した場合などに、コントローラの高負荷に繋がる懸念がある。

対策のひとつとして、分散型コントローラを採用する方法が考えられる（第 2 編第 2 章第 1 節 3.3 参照）。OpenFlow スイッチに OpenFlow コントローラの機能を分散配備して連携を行う方式であり、OAM 機能を各スイッチに分散配備して各ノード間で試験を行う（図 3-12）。

ただし、本方式はスイッチ間やスイッチとコントローラ間の連携方法を規定する必要があり、具体的な実現例は今後の課題とする。

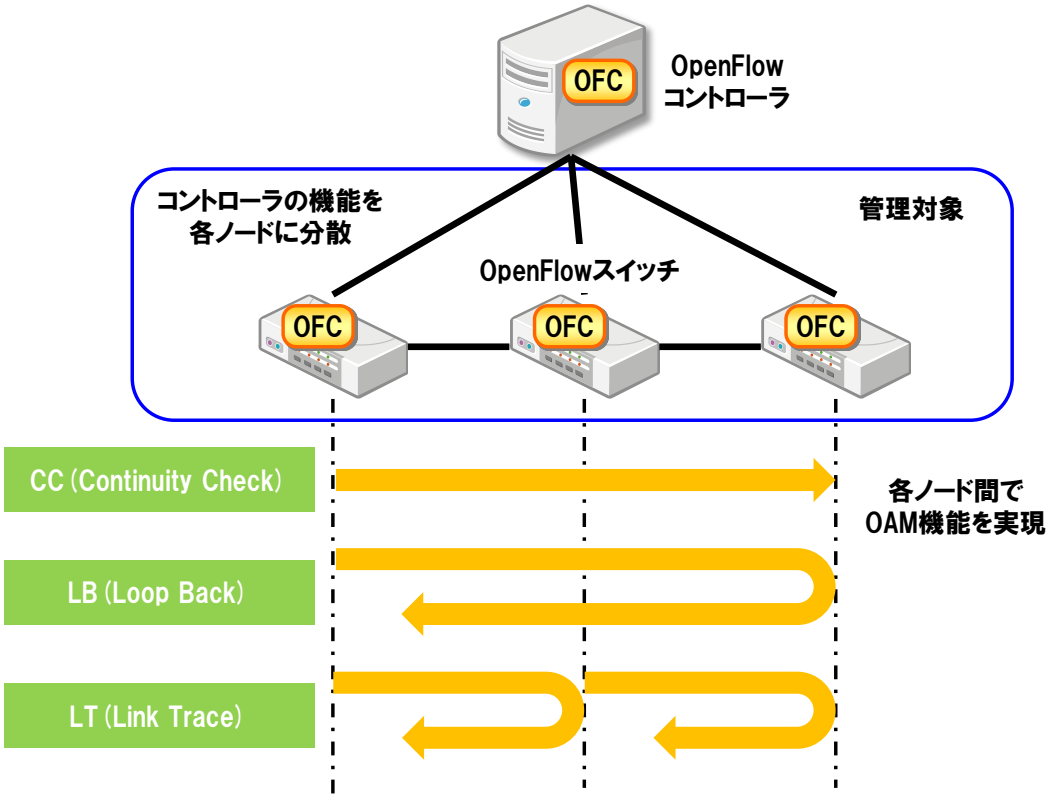


図 3-12　分散型コントローラによる OAM 機能の実現例

第3章 Point-to-Point 回線の運用・監視

『第 3 章 Point-to-Point 回線の運用・監視』では、第 1 節において本章で説明の前提とする Point-to-Point 回線のモデルについて示し、第 2 節において Point-to-Point 回線の開通時の試験方法及び開通後の正常性の定期監視方法について示す。第 3 節では、定期監視により異常を検出した場合の迂回方法や被疑箇所の推定方法について示す。

- 第 1 節 Point-to-Point 回線モデル
- 第 2 節 Point-to-Point 回線の開通試験・定期監視
- 第 3 節 Point-to-Point 回線の異常措置

第1節 Point-to-Point 回線モデル

第 3 編第 1 章第 3 節に示すように、Point-to-Point 回線は、2 つの端点となるポート間で設定される基本回線である。

Point-to-Point 回線のモデルとして、図 3-13 のように、エッジノード EN1 のポート en10 と、エッジノード EN2 のポート en20 の間の回線 C1（ユーザ U1）を考える。

回線 C1 は、回線オプションで冗長化を行うものとし、A 面に設定する回線 C11 と B 面に設定する回線 C12 を予め設定しておき、故障時等には切替えられるようにしておく。故障時の切替えはエッジノード EN1 及び EN2 で行う。

A 面及び B 面のコアノード間には中継パスが冗長構成ありで設定されている。A 面のコアノード CN1 とコアノード CN4 間には、中継パス P1 と P2 が予め設定されており、故障時等には切替えられるようにしておく。回線 C11 は中継パス P1 及び P2 に収容する。故障時等の切替えはコアノード CN1 及び CN4 で行う。

同様に B 面のコアノード CN5 とコアノード CN8 間には、中継パス P3 と P4 が予め設定されており、故障時等には切替えられるようにしておく。回線 C12 は中継パス P3 及び P4 に収容する。故障時等の切替えはコアノード CN5 及び CN8 で行う。

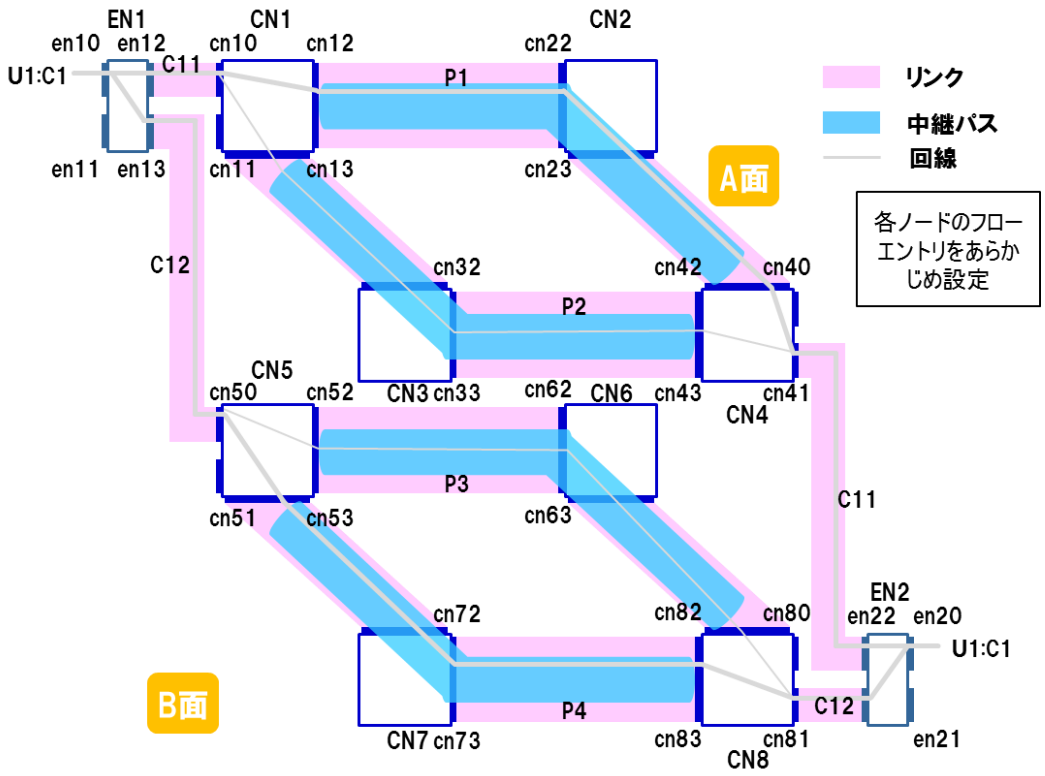


図 3-13　Point-to-Point 回線モデル

第2節 Point-to-Point 回線の開通試験・定期監視

1. 開通試験・定期監視の基本的な考え方

Point-to-Point 回線の開通試験では、Point-to-Point 回線や利用する中継パスについて、フローエントリの正常性やリンクの正常性を確認し、意図した通りにパケットを送信できるか確認する。確認ポイントとして以下の 3 つがある。

①宛先まで送信されること

回線及び中継パスの始点・終点間で、パケットが疎通することを確認する。この試験には CC ツールを用いる。

②正しい経路で送信されること

回線及び中継パスの始点・終点間で、パケットが経由する SDN ノードが意図した通りかを確認する。この試験には LT ツールを用いる。

③宛先以外に送信されないこと

回線及び中継パスが、パケットの分岐などにより意図した宛先以外に送信されていないことを確認する。この試験には CC ツールを使用する。

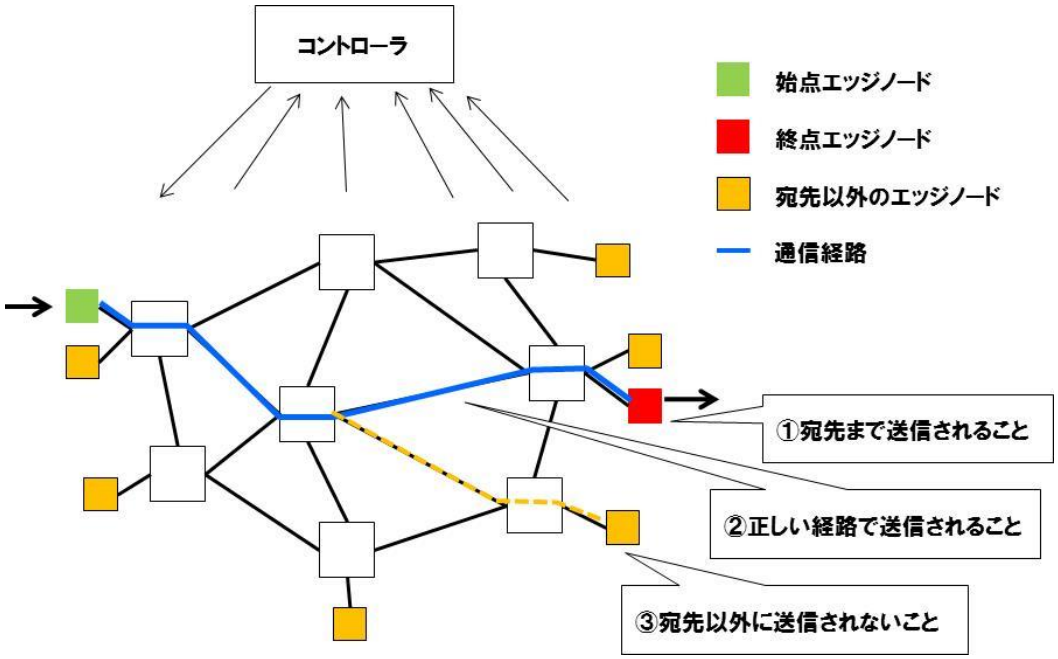


図 3-14　Point-to-Point 回線の開通試験の確認ポイント

Point-to-Point 回線の定期監視では、運用中の回線及び中継パスを定期的に監視して正常性が維持されていることを確認する。定期監視では、「①宛先まで送信されること」の試験を行う。「②正しい経路で送信されること」「③宛先以外に送信されないこと」については、SDN コントローラの処理負荷増加の懸念があるため、異常検出時に適宜実施するのがよい。

これらを図 3-15 にまとめる。

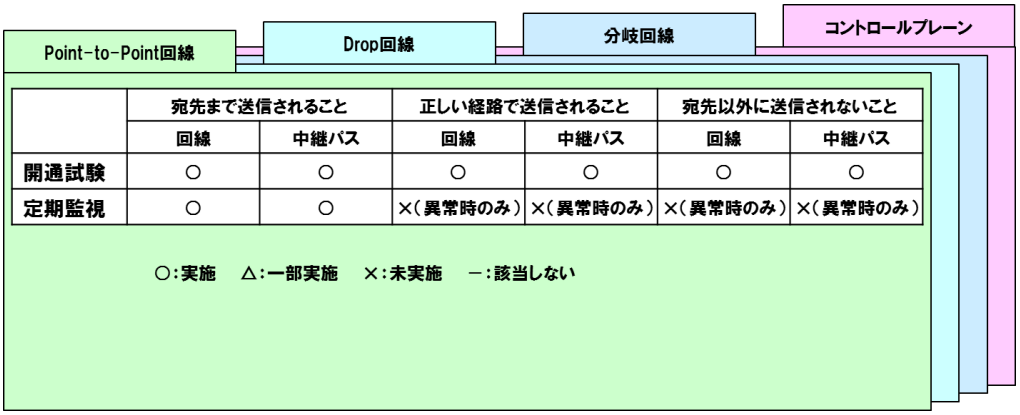


図 3-15 Point-to-Point 回線の開通試験・定期監視

2. 宛先まで送信されることの試験

2.1. 試験手順

「宛先まで送信されること」の試験は Continuity Check (CC) ツールにより確認する。Point-to-Point 回線の回線レベルの試験は、図 3-16 に示すように実施できる。

①入側エッジノード N1 において、回線 C1 に対する CC 試験パケットについて、回線 C1 と同一の処理（網内タグ付与、転送処理）を行うための、試験用フローエントリを設定する。

②出側エッジノード N5 において、回線 C1 に対する CC 試験パケットについて、必要な情報（dpid 等）を付加してコントローラに Packet-In させるための、試験用フローエントリを設定する。

③コントローラから入側エッジノード N1 に、回線 C1 に対する CC 試験パケットを Packet-Out する。

④入側エッジノード N1 では、①で設定した試験用フローエントリに従い、CC 試験パケットに網内タグを付与し、CC 試験パケットをコアノード N2 に転送する。

⑤コアノード N2 から N4 では、網内タグに基づき、回線 C1 が用いるフローエントリに従って CC 試験パケットを転送する。

⑥出側エッジノード N5 では、②で設定した試験用フローエントリに従い、CC 試験パケットに必要な情報（dpid 等）を付加してコントローラに Packet-In する。

⑦コントローラでは、③で Packet-Out した CC 試験パケットが、所定の時間内に⑥で Packet-In することにより正常性を判断する。

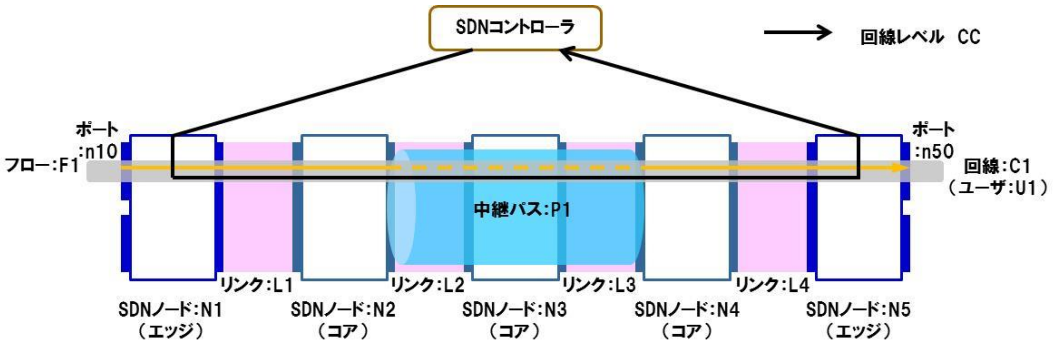


図 3-16　宛先まで送信されることの試験（Point-to-Point 回線）

Point-to-Point 回線の中継パスレベルの試験は、図 3-17 のように実施できる。

①入側コアノード N2 において、中継パス P1 に対する CC 試験パケットについて、中継パス P1 と同一の処理（転送処理）を行うための、試験用フローエントリを設定する。

②出側コアノード N4 において、中継パス P1 に対する CC 試験パケットについて、必要な情報（dpid 等）を付加してコントローラに Packet-In させるための、試験用フローエントリを設定する。

③コントローラから入側コアノード N2 に、中継パス P1 に対する CC 試験パケットを Packet-Out する。CC 試験パケットには中継パス P1 の網内タグを付与しておく。

④入側コアノード N2 では、①で設定した試験用フローエントリに従い、CC 試験パケットをコアノード N3 に転送する。

⑤コアノード N3 では、網内タグに基づき、中継パス P1 が用いるフローエントリに従って CC 試験パケットを転送する。

⑥出側コアノード N4 では、②で設定した試験用フローエントリに従い、CC 試験パケットに必要な情報(dpid 等)を付加してコントローラに Packet-In する。

⑦コントローラでは、③で Packet-Out した CC 試験パケットが、所定の時間内に⑥で Packet-In することにより正常性を判断する。

回線レベルと中継パスレベルの試験では、Packet-Out/Packet-In を行う対象がエッジノードかコアノードか、また、中継パスレベルの場合は網内タグを付与するエッジノードを通過しないため、コントローラにおいて網内タグを付与して、CC 試験パケットを Packet-Out するという違いがある。

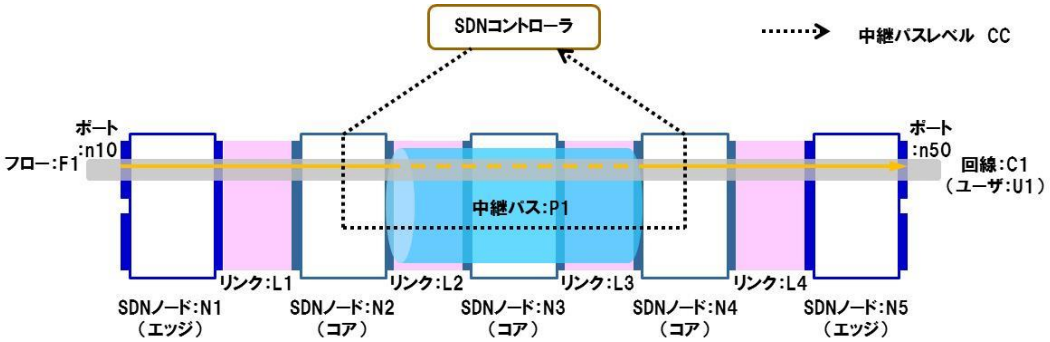


図 3-17　宛先まで送信されることの試験（中継パス）

2.2. 留意事項

Point-to-Point 回線の回線レベルの試験では、図 3-18 に示すように CC 試験パケットをコントローラから入側エッジノード N1 に Packet-Out し、出側エッジノード N5 で Packet-In を行う。入側エッジノード N1 では、ユーザが使用する Point-to-Point 回線の入力ポート n10 と、CC 試験パケットが使用する入力ポートが異なるため、Point-to-Point 回線とは別のフローエントリ（試験用のフローエントリ）を用いることになる。同じく出側エッジノード N5 では、ユーザが使用する Point-to-Point 回線の出力ポート n50 と、CC 試験パケットが使用する出力ポートが異なるため、Point-to-Point 回線とは別のフローエントリ（試験用のフローエントリ）を用いることになる。

また、入側エッジノード N1 の入力ポート n10 や入側エッジノード N1 とユーザ間のアクセスリンク AL1、同じく出側エッジノード N5 の出力ポート n50 や出側エッジノード N5 とユーザ間のアクセスリンク AL2 は確認が行えない。

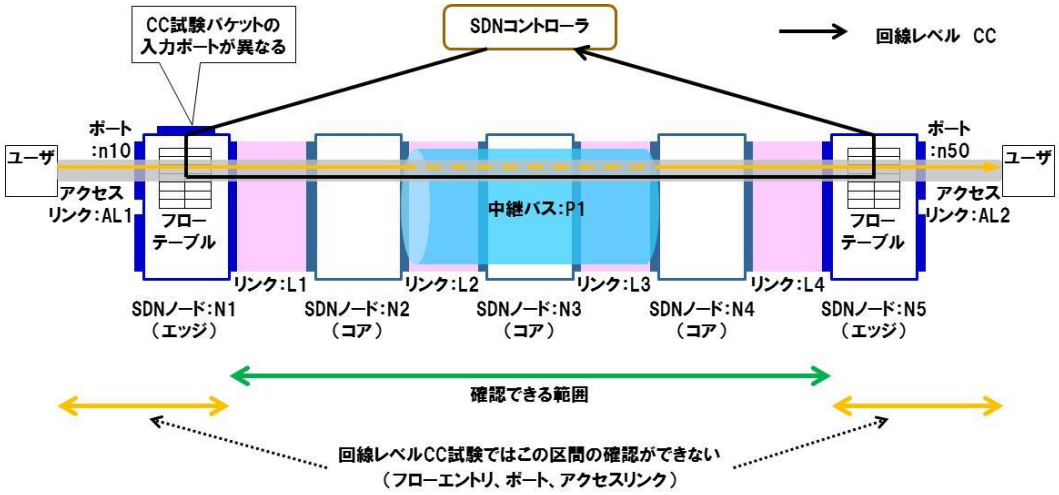


図 3-18　回線レベル CC により確認される区間

これらの区間の試験を行うには、以下の 2 つの方法が考えられる。

● 方法 1

エッジノードの外側（ユーザ宅等）に試験用のノードを置き、試験用ノード間で End-to-End の試験を行う。概要を図 3-19 に示す。この方法では、アクセスリンク、エッジノードのポート、フローエントリの確認ができる。

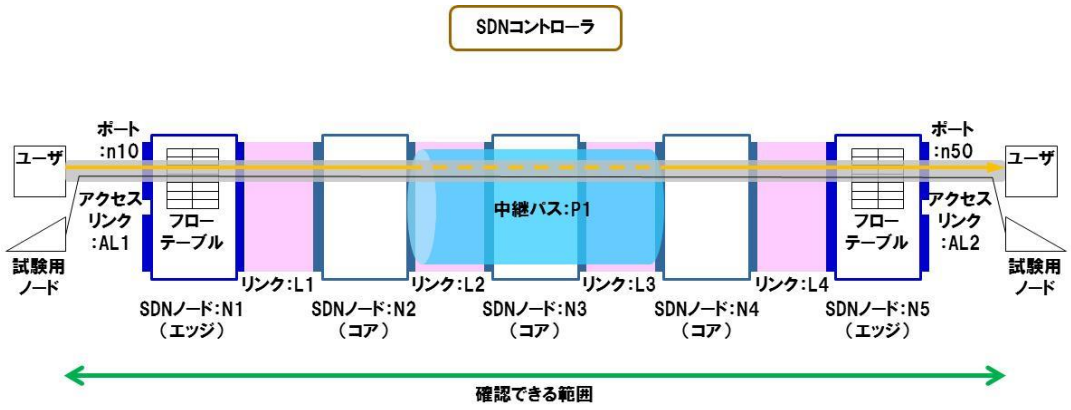


図 3-19　アクセス区間を含む End-to-End の確認（方法 1）

● 方法 2

ユーザ端末に折り返し設定を行い、アクセス区間のみの試験を行う（図 3-20）。手順を以下に示す。

①ユーザ端末に試験パケットの折り返し設定を行う。

②コントローラからエッジノード N1 に試験パケットを Packet-Out する。

③エッジノード N1 では、試験パケットをユーザ端末に転送する。

④ユーザ端末では試験パケットを折り返し、エッジノード N1 に転送する。

⑤エッジノード N1 ではユーザ端末から送信された試験パケットをコントローラに Packet-In する。

⑥コントローラでは、Packet-Out した試験パケットが Packet-In することで、アクセス区間の正常性を確認する。

この方法では、アクセスリンク、エッジノードのポートの確認ができるが、フローエントリの確認はできない。また、この方法はユーザ端末に試験パケットを折り返す機能が必要となる。

なお、方法 2 をエッジノード N5 とユーザ間で行うことにより、エッジノード N5 の出力ポート n50 やアクセスリンク AL2 の確認が可能である。

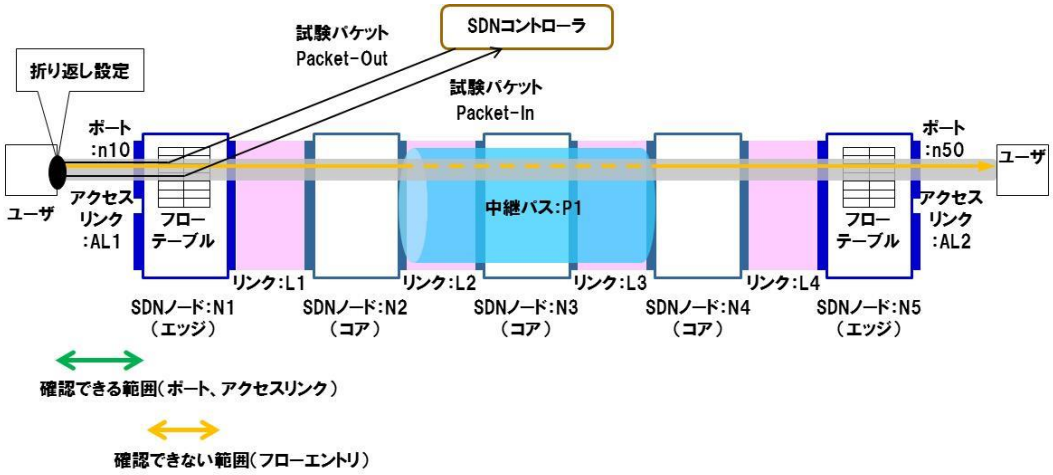


図 3-20　アクセス区間のみの確認（方法 2）

回線レベルの試験方法と確認できる区間を表 3-1 に示す。

表 3-1　回線レベルの試験方法と確認できる区間

	アクセスリンク	エッジノード N1			リンク	コアノード N2-N4			リンク	エッジノード N5			アクセスリンク
		ポート	フローエントリ	ポート		ポート	フローエントリ	ポート		ポート	フローエントリ	ポート	
CC ツール	―	―	―	○	○	○	○	○	○	○	―	―	―
方法 1	○	○	○	○	○	○	○	○	○	○	○	○	○
方法 2	○	○	―	―	―	―	―	―	―	―	―	○	○

○：確認可能、―：確認できない

方法 1 はユーザ側に試験ノードを設置する必要があり、また、方法 2 はユーザ端末に折り返し設定を行うことが必要になるため、開通時や異常時の試験のみとし、定期監視は推奨しない。

中継パスレベルの試験では回線レベルの試験と同様に、CC 試験パケットをコントローラから入側コアノード N2 に Packet-Out し、出側コアノード N5 で

Packet-In を行うため、入側コアノード N2 と出側コアノード N4 のフローエントリの確認はできない。しかし、試験対象となる中継パスを用いる回線レベルでの試験を行い、結果に問題がなければ、入側コアノード N2 及び出側コアノード N4 のフローエントリも、同様に問題がないと判断できる。

中継パスレベルの試験方法と確認できる区間を表 3-2 に示す。

表 3-2　中継パスレベルの試験方法と確認できる区間

	コアノード N2		リンク	コアノード N3			リンク	コアノード N4	
	フローエントリ	ポート		ポート	フローエントリ	ポート		ポート	フローエントリ
中継パスレベル CC	―	○	○	○	○	○	○	○	―
回線レベル CC	○	○	○	○	○	○	○	○	○

○：確認可能、―：確認できない

3. 正しい経路で送信されることの試験

3.1. 試験手順

「正しい経路で送信されること」の試験は Link Trace（LT）ツールにより確認する。Point-to-Point 回線の回線レベルの試験は、図 3-21 に示すように実施できる。

①入側エッジノード N1 において、回線 C1 に対する LT 試験パケットについて、回線 C1 と同一の処理（網内タグ付与、転送処理）を行うための、試験用フローエントリを設定する。

②出側エッジノード N5 において、回線 C1 に対する LT 試験パケットについて、必要な情報（dpid 等）を付加してコントローラに Packet-In させるための、試験用フローエントリを設定する。

③回線 C1 の経路上のその他のノードでは、回線 C1 に対する LT 試験パケットについて、LT 試験パケットの中継と合わせて、コピー（分岐）して必要な情報（dpid 等）を付加し、コントローラに Packet-In させるための、試験用フローエントリを設定する。

④コントローラから入側エッジノード N1 に、回線 C1 に対する LT 試験パケットを Packet-Out する。

⑤入側エッジノード N1 では、①で設定した試験用フローエントリに従い、LT 試験パケットに網内タグを付与し、LT 試験パケットをコアノード N2 へ転送する。

⑥コアノード N2 から N4 では、③で設定した試験用フローテーブルに従って LT 試験パケットを転送するとともに、LT 試験パケットのコピーを作成し、必要な情報（dpid 等）を付加してコントローラに Packet-In する。

⑦出側エッジノード N5 では、②で設定した試験用フローエントリに従い、LT 試験パケットに必要な情報（dpid 等）を付加してコントローラに Packet-In する。

⑧コントローラでは、Packet-In した LT 試験パケットを TTL（Time To Live）の順番に並べ、TTL の順番に抜けがないことを確認することにより、正しい経路で送信されていることを確認できる。TTL に抜けがある場合、抜けの前後のノードのフローエントリを調べることにより、意図しないノードに転送されていないかを確認する。

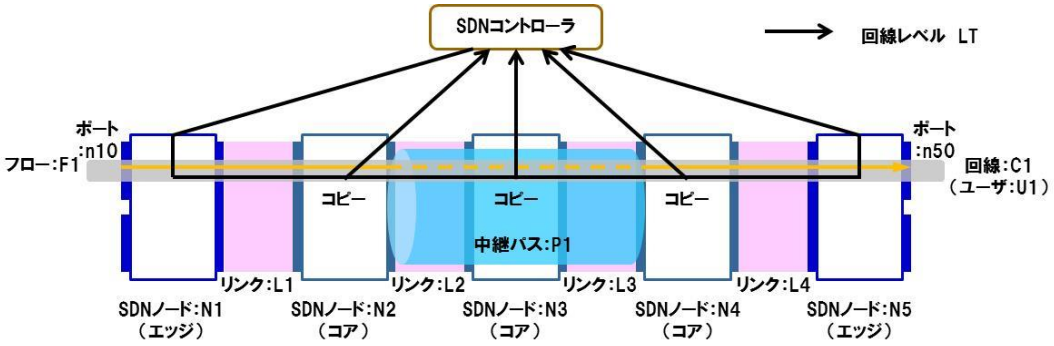


図 3-21　正しい経路で送信されることの試験（Point-to-Point 回線）

Point-to-Point 回線の中継パスレベルの試験も、図 3-22 のように回線レベルの試験と同様に実施できる。コントローラから Packet-Out/Packet-In する LT 試験パケットはコアノードに対して行われること、また、コントローラから Packet-Out する LT 試験パケットには網内タグを付与しておくことが、回線レベルと中継パスレベル試験の違いとなる。

①入側コアノード N2 において、中継パス P1 に対する LT 試験パケットについて、中継パス P1 と同一の処理（転送処理）を行うための、試験用フローエントリを設定する。

②出側コアノード N4 において、中継パス P1 に対する LT 試験パケットについて、必要な情報（dpid 等）を付加してコントローラに Packet-In させるための、試験用フローエントリを設定する。

③中継パス P1 の経路上のその他のノードでは、中継パス P1 に対する LT 試験パケットについて、LT 試験パケットの中継と合わせて、コピー（分岐）して必要な情報（dpid 等）を付加し、コントローラに Packet-In させるための、試験用フローエントリを設定する。

④コントローラから入側コアノード N2 に、中継パス P1 に対する LT 試験パケットを Packet-Out する。LT 試験パケットには中継パス P1 の網内タグを付与しておく。

⑤入側コアノード N2 では、①で設定した試験用フローエントリに従い、LT 試験パケットをコアノード N3 に転送する。

⑥コアノード N3 では、③で設定した試験用フローテーブルに従って LT 試験パケットを転送するとともに、LT 試験パケットのコピーを作成し、必要な情報（dpid 等）を付加してコントローラに Packet-In する。

⑦出側コアノード N4 では、LT 試験パケットに必要な情報（dpid 等）を付加してコントローラに Packet-In する。

⑧コントローラでは、Packet-In した LT 試験パケットを TTL (Time To Live) の順番に並べ、TTL の順番に抜けがないことを確認することにより、正しい経路で送信されていることを確認できる。TTL に抜けがある場合、抜けの前後のノードのフローエントリを調べることにより、意図しないノードに転送されていないかを確認する。

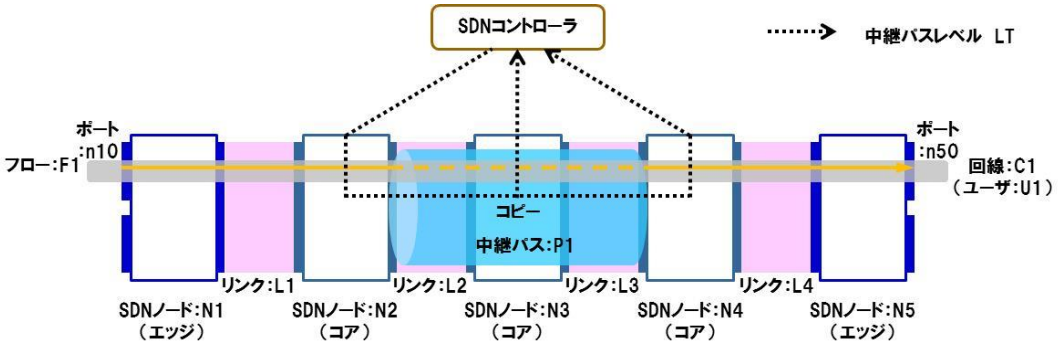


図 3-22　正しい経路で送信されることの試験（中継パス）

3.2. 留意事項

「正しい経路で送信されること」の回線レベルの試験も、「宛先まで送信されること」の試験と同様に、試験パケットをコントローラから入側エッジノード N1 に Packet-Out することから、エッジノード N1 で用いるフローエントリはユーザが使用する Point-to-Point 回線のフローエントリとは異なるため注意が必要である。そのため、エッジノード N1 からコアノード N2 間に別のノードを経由していないかを確認するべきである。これには、隣接するコアノード N2 から Packet-In した LT 試験パケットの TTL 値が想定より少なくなっていることで、想定していないノードを経由していることが推測できる。この場合、エッジノード N1 のフローエントリを調べる必要がある。

「正しい経路で送信されること」の中継パスレベルの試験も、「宛先まで送信されること」の試験と同様に、試験パケットをコントローラから入側コアノード N2 に Packet-Out することから、コアノード N2 で用いるフローエントリは試験対象となる中継パスのフローエントリとは異なる。隣接するコアノード N3 から Packet-In した LT 試験パケットの TTL 値が想定より少なくなっていることで、想定していないノードを経由していることが推測できる。この場合、コアノード N2 のフローエントリを調べる必要がある。また、別の方法として、回線レベルの試験を行うことにより、中継パスの経路を確認することもできる。

「正しい経路で送信されること」の試験では、経路上の通過した全てのノードから LT 試験パケットが Packet-In されるため、コントローラの負荷が大きくなる懸念がある。そのため、「正しい経路で送信されること」の試験は、開通時及び異常検出時に行うものとし、定期監視は推奨しない。

4. 宛先以外に送信されないことの試験

4.1. 試験手順

回線レベルの「宛先以外に送信されないこと」の試験は Continuity Check (CC) ツールにより確認する。図 3-23 に示すように、「宛先まで送信されること」の試験と同じ方法であるが、宛先以外も含む全てのエッジノードに対して、CC 試験パケットをコントローラに Packet-In するように設定しておく点が異なる。全てのエッジノードに設定を行うことで、「宛先まで送信されること」の試験と合わせて同時に行うことも可能である。

①入側エッジノード N1 において、回線 C1 に対する CC 試験パケットについて、回線 C1 と同一の処理（網内タグ付与、転送処理）を行うための、試験用フローエントリを設定する。

②入側エッジノードを除くその他の全てのエッジノードに対し、回線 C1 に対する CC 試験パケットについて、コントローラに Packet-In させるための試験用フローエントリを設定する。

③コントローラから入側エッジノード N1 に、回線 C1 に対する CC 試験パケットを Packet-Out する。

④入側エッジノード N1 では、①で設定した試験用フローエントリに従い、CC 試験パケットに網内タグを付与し、CC 試験パケットをコアノード N2 へ転送する。

⑤コアノードでは、網内タグに基づき、回線 C1 が用いるフローエントリに従って CC 試験パケットを転送する。

⑥エッジノードでは、回線 C1 に対する CC 試験パケットを受信した場合、②で設定した試験用フローエントリに従い、必要な情報（dpid 等）を付加してコントローラに Packet-In する。

⑦コントローラでは、宛先以外のエッジノードから Packet-In がないことにより、宛先以外に送信されていないことを確認する。

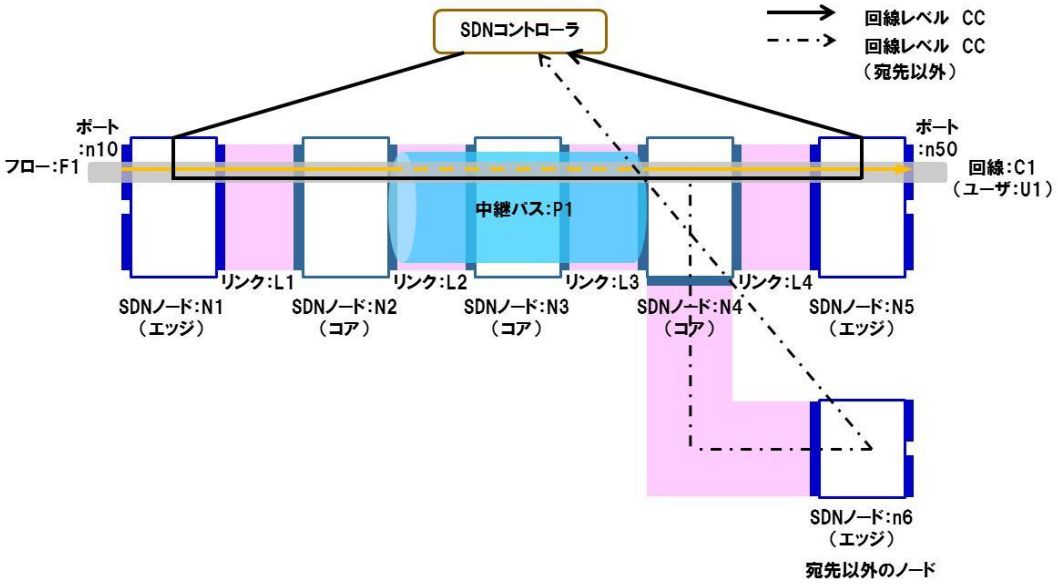


図 3-23　宛先以外に送信されないことの試験（Point-to-Point 回線）

中継パスレベルの「宛先以外に送信されないこと」の試験は、Continuity Check (CC) ツールにより確認する。図 3-24 に示すように、中継パスレベルの「宛先まで送信されること」の試験と同じ方法であるが、試験対象となる中継パスの経路以外も含む全てのコアノードに対して、CC 試験パケットをコントローラに Packet-In するように設定しておく点が異なる。

①試験対象となる中継パスの経路を除く全てのコアノードに対し、中継パス P1 に対する CC 試験パケットについて、コントローラに Packet-In させるための試験用フローエントリを設定する。

②中継パスの出側コアノード N4 にも同様に、中継パス P1 に対する CC 試験パケットについて、コントローラに Packet-In させるための試験用フローエントリを設定する。

③コントローラから入側コアノード N2 に、中継パス P1 に対する CC 試験パケットを Packet-out する。CC 試験パケットには網内タグを付与しておく。

④コアノードでは、網内タグに基づき、中継パス P1 が用いるフローエントリに従って CC 試験パケットを転送する。

⑤出側コアノード N4 では、中継パス P1 に対する CC 試験パケットを受信した場合、②で設定した試験用フローエントリに従い、必要な情報（dpid 等）を付加してコントローラに Packet-In する。

⑥経路以外のコアノードが中継パス P1 に対する CC 試験パケットを受信した場合、①で設定した試験用フローエントリに従い、必要な情報（dpid 等）を付加してコントローラに Packet-In する。

⑦コントローラでは、中継パス P1 に対する CC 試験パケットが、正しい経路以外のコアノードから Packet-In していないか確認し、中継パスが正しい宛先以外に送信されてないことを確認する。

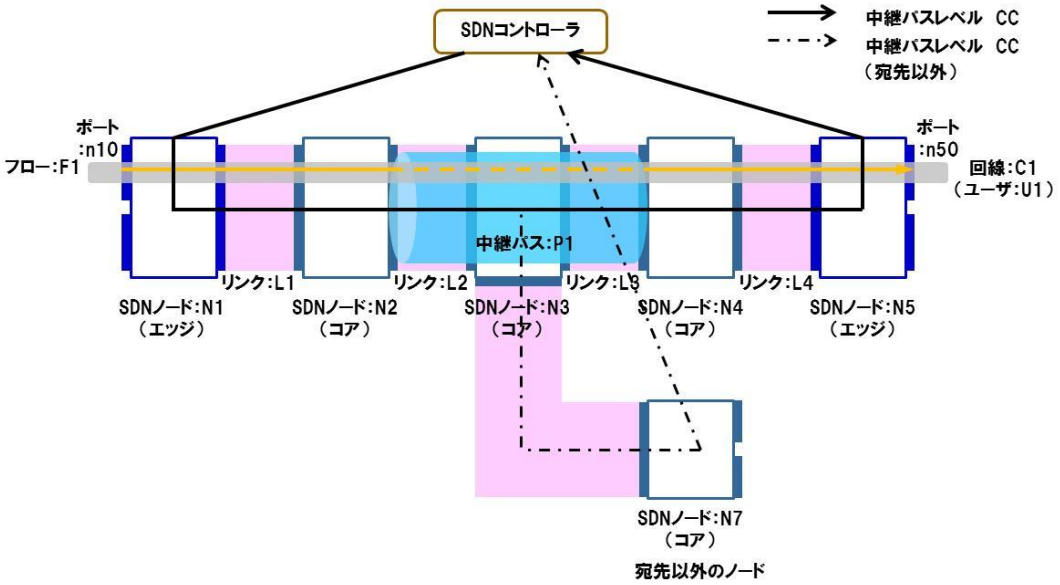


図 3-24　宛先以外に送信されないことの試験（中継パス）

4.2. 留意事項

「宛先以外に送信されないこと」の試験は、予期しないノードからの Packet-In の検出を行うこととなるため、開通時にのみ行うこととし、定期監視は推奨しない。また、「宛先以外に送信されないこと」の試験と「宛先まで送信されること」の試験は、どちらも CC ツールを使用し、コントローラに Packet-In する CC 試験パケットの結果に基づき確認を行うことから、各々の試験を同時に行うことができる。

第3節 Point-to-Point 回線の異常措置

定期監視プロセスで異常を検出した場合は異常措置プロセスへと移行し、冗長化されたネットワークリソースに切替えることにより、ネットワークサービスの中断を極力抑えることができる。

サービス中断時間の短縮のためには、検出した故障に応じて適切な切替えを行うことが重要である。中継パスレベルの定期監視で故障を検出した場合には、同一面内での中継パス単位での切替えを行い、回線レベルの定期監視で故障を検出した場合には、個々の回線単位で面の切替え（A 面から B 面への切替え等）を行うことが望ましい。

予備系への切替え後は、LB ツール等を利用して故障の被疑箇所を推定し、リセットやハードウェア交換等の回復措置を行う必要がある。また、回復措置後は、正常性を確認して現用系に切戻しをすることが望ましい。切戻しはオペレータ主導で行う。

なお、工事等のために運用中の回線や中継パスを、冗長化したリソースに切替える支障移転の場合も、オペレータ主導で、中継パスや面の切替えを行う。

1. 中継パスレベルの切替え

中継パスの定期監視で異常を検出した場合には、図 3-25 で示すように同一面内で中継パスの切替えを行う。

中継パスの異常の際には該当する中継パスに収容される全ての回線が影響を受けることになるが、中継パス単位で切替えを行うことで、影響を受けた回線を 1 本ずつ切替る必要がなく一度に救済することができる。

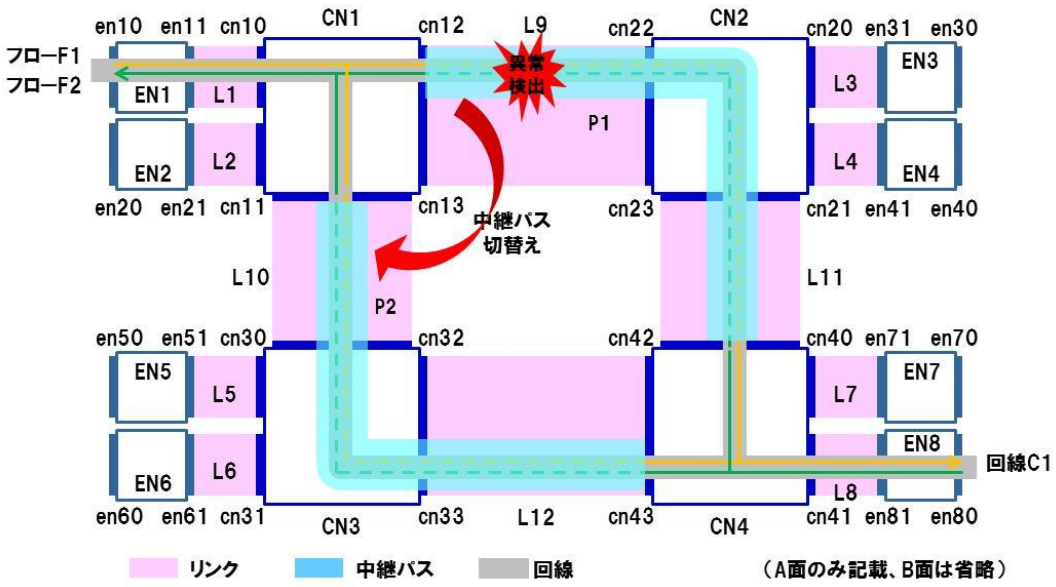


図 3-25　中継パスレベルの切替え（Point-to-Point 回線）

2. 面レベルの切替え

回線の定期監視で異常を検出した場合には、図 3-26 で示すように個々の回線単位で面の切替え（A 面から B 面への切替え等）を行う。

回線レベルの定期監視の故障検出間隔に対し、中継パスレベルの定期監視の故障検出間隔を短く設定することで、中継パスの異常を優先的に検出できるようになり、不必要な切替えを避けることができる。

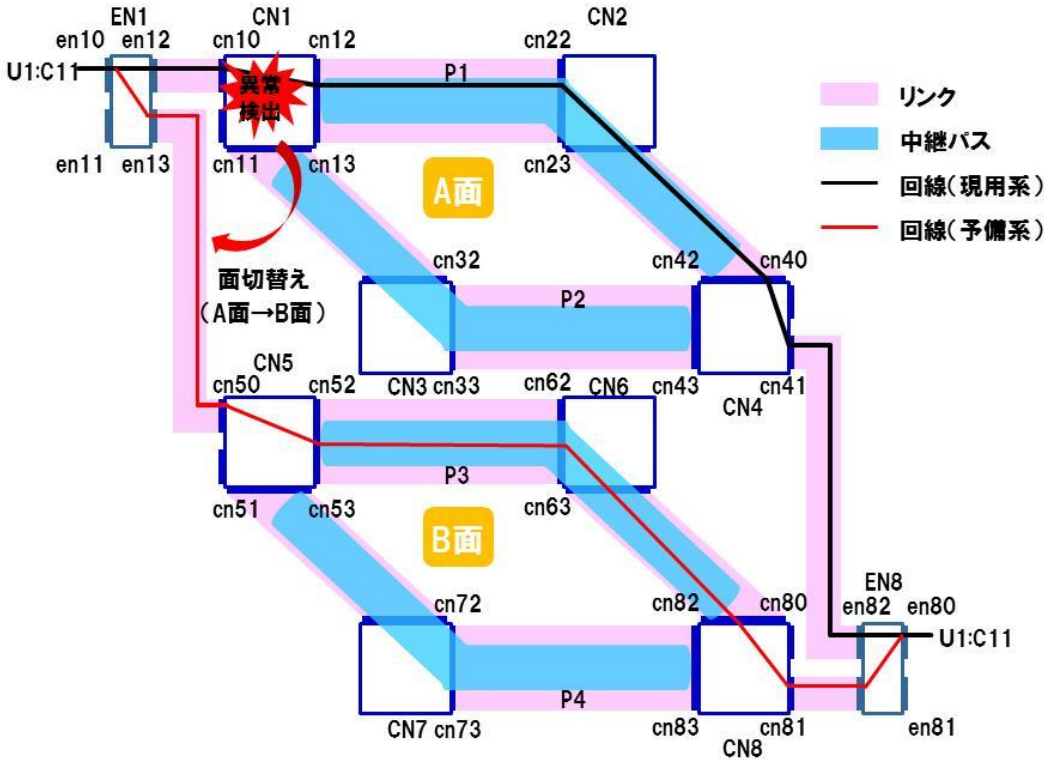


図 3-26　面レベルの切替え（Point-to-Point 回線）

3. 被疑箇所の推定

定期監視で異常が検出された場合には冗長系に切替えてネットワークサービスの回復を図るが、切替えた後は故障の被疑箇所の推定を行い、リセットやハードウェア交換等の回復措置を行う必要がある。被疑箇所の推定には LB ツールを用いる。

図 3-27、図 3-28 に示すように、SDN コントローラから、試験対象区間となる SDN ノードに対して LB 試験パケットを Packet-Out する。試験対象区間は入側エッジノードである N1 を起点とし、終点となる SDN ノードを順次変えて複数の LB 試験パケットを送出する。

故障箇所の手前にある SDN ノード N2、N3 からは、SDN コントローラへ LB 試験パケットが Packet-In されるが、故障箇所より遠い SDN ノード N4、N5 には LB 試験パケットは届かず、SDN コントローラへ Packet-In しないためタイムアウトとなる。

次に、SDN ノード N5 を起点とし、逆方向に試験対象区間を順次変えて LB 試験パケットを Packet-Out する。

故障箇所の手前にある SDN ノード N4 からは、SDN コントローラへ LB 試験パケットが Packet-In されるが、故障箇所より遠い SDN ノード N3、N2、N1 には LB 試験パケットは届かず、SDN コントローラへ Packet-In しないためタイムアウトとなる。

2 つの LB 試験により、故障被疑箇所が SDN ノード 3 と SDN ノード 4 のリンク（ノード出力ポートを含む）と想定されるので、故障箇所を特定する。

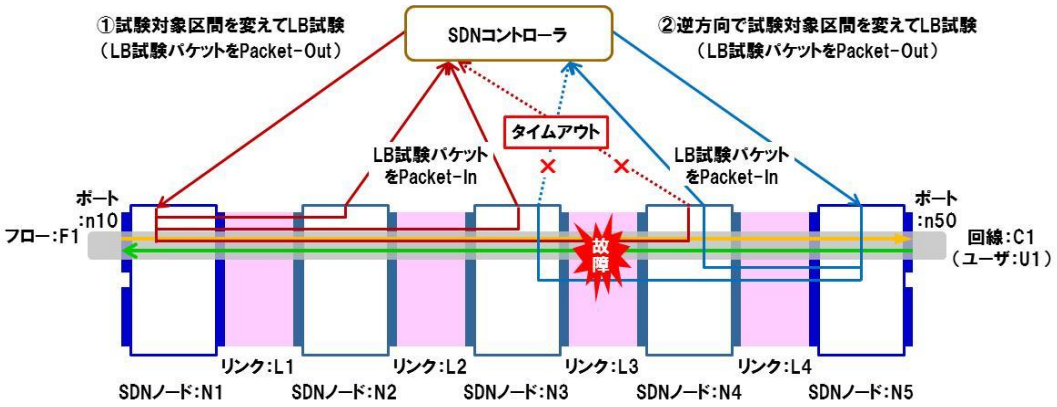


図 3-27　被疑箇所の推定（経路上のノードを図示）

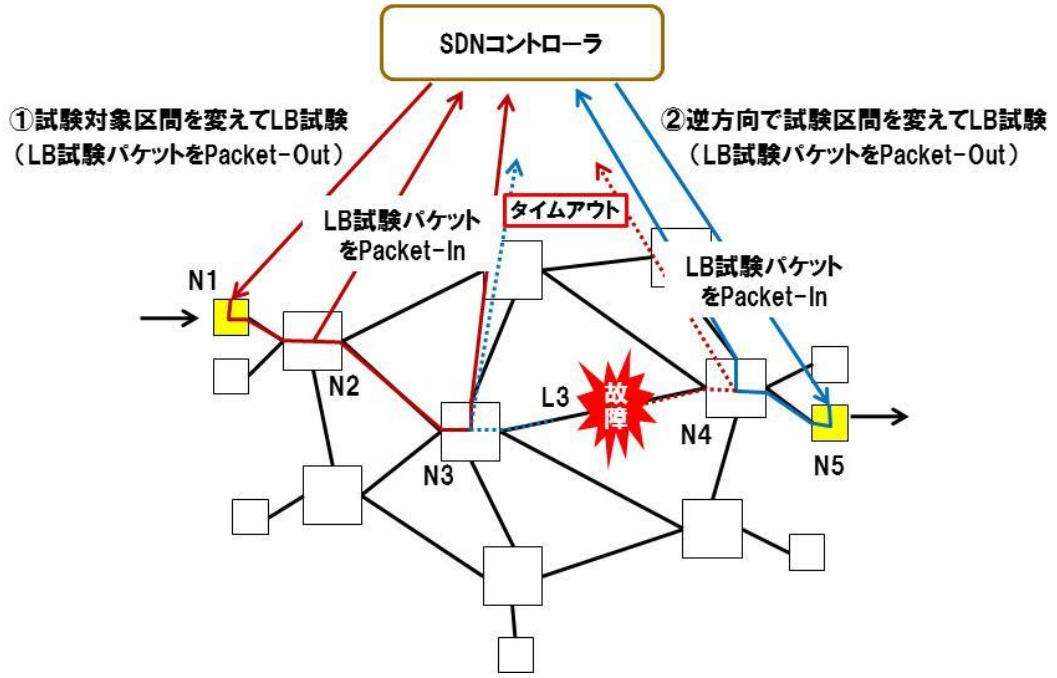


図 3-28　故障個所の特定（経路外のノードも図示）

4. 支障移転時の切替え

支障移転では、運用中の回線サービスの工事等を実施するため、冗長化したリソースに予め切替えを行い、工事等を行うリソースを空けておく。図 3-29 に示すように、工事等を行う箇所により切替え方法が異なる。

- 中継パスレベルの切替えを行う場合
  - コアノード間のリンク（L2、L3）の工事等
  - 中継パスが経由するコアノード（CN2）の工事等
- 面レベルの切替えを行う場合
  - エッジノードとコアノード間のリンク（L1、L4）の工事等
  - 入側コアノード（CN1）及び出側コアノード（CN4）の工事等

なお、エッジノード EN1 及びエッジノード EN8 の工事等を行う場合は、冗長リソースがないためネットワークサービスが中断することになる。サービス中断の影響を少なくするには、代替するエッジノードを借用し、ユーザを収容替えしておく等の対応が必要になる。

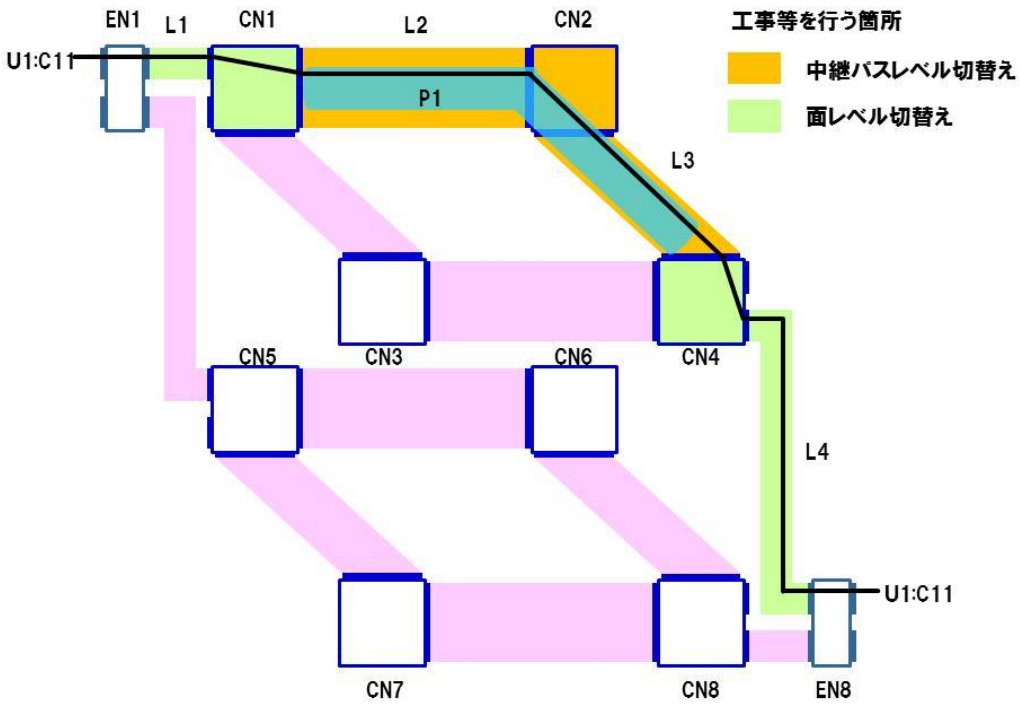


図 3-29　支障移転時の切替え方法（Point-to-Point 回線）

第4章 Drop 回線の運用・監視

『第 4 章 Drop 回線の運用・監視』では、第 1 節において本章で説明の前提とする Drop 回線のモデルについて示し、第 2 節において Drop 回線の開通時の試験方法及び開通後の正常性の定期監視方法について示す。

- 第 1 節 Drop 回線モデル
- 第 2 節 Drop 回線の開通試験・定期監視

第1節 Drop 回線モデル

第 3 編第 1 章第 3 節に示すように、Drop 回線は、経路の途中でパケットが廃棄される回線オプションである。

Drop 回線のモデルとして、図 3-30 のように、エッジノードでパケットを廃棄するモデルを基本として考え、入側エッジノードで Drop するパタンと出側エッジノードで Drop するパタンがある。中継パスでの Drop は考慮しない。

入側エッジノードで Drop するパタンでは、入力パケットを input_port や宛先／送信元アドレス等でマッチングして Drop する。

出側エッジノードで Drop するパタンでは、入力パケットを input_port や宛先／送信元アドレス等のほか、回線識別タグでマッチングして Drop することも可能である。

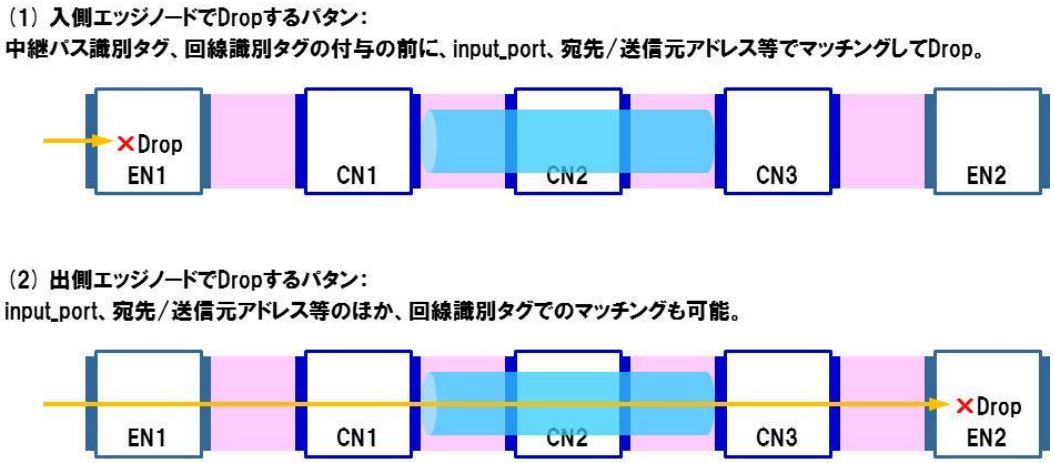


図 3-30　Drop 回線モデル

第2節 Drop 回線の開通試験・定期監視

1. 開通試験・定期監視の基本的な考え方

Drop 回線の開通試験では、指定したノードで Drop されることを確認する。Drop 回線の定期監視は行わず、異常発生時に適宜試験を行う。また、中継パスでは Drop を行わないため、中継パスの試験は対象外とする（図 3-31）。

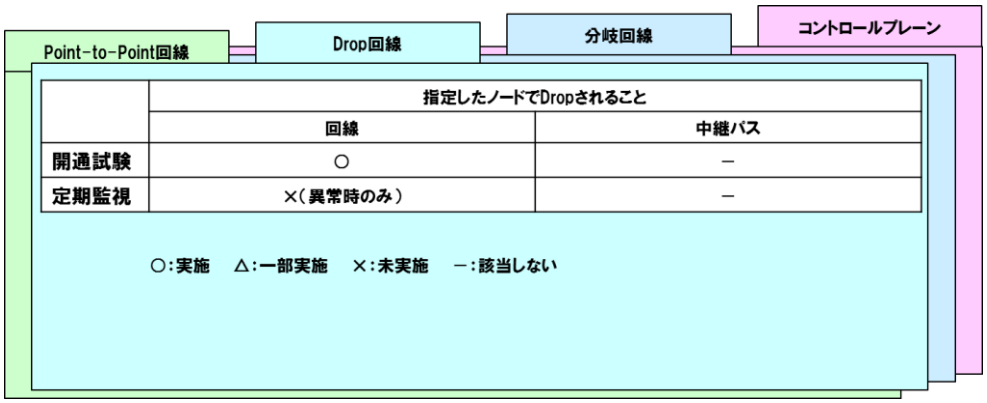


図 3-31　Drop 回線の開通試験・定期監視

2. 指定したノードで Drop されることの試験

2.1. 試験手順

「指定したノードで Drop されること」の試験は Match 条件をカウントする統計情報カウンタを用いて行う。

図 3-32 に出側エッジノードで Drop するパタンの開通試験を示す。

①コントローラから出側エッジノード EN2 のフローエントリの Match 条件カウンタを読み取る。

②コントローラから入側エッジノード EN1 に CC 試験パケットを Packet-Out する。

③出側エッジノード EN2 では、フローエントリに従い、CC 試験パケットを Drop し、フローエントリの Match 条件カウンタをカウントアップする。

④コントローラから出側エッジノード EN2 の Match 条件カウンタを読み取り、①で読み取った値と比較しカウントアップされていることを確認する。

なお、本試験は、Match 条件に該当したものをカウントしたものであり、実際に Drop アクションが実行されているかは確認できていない。

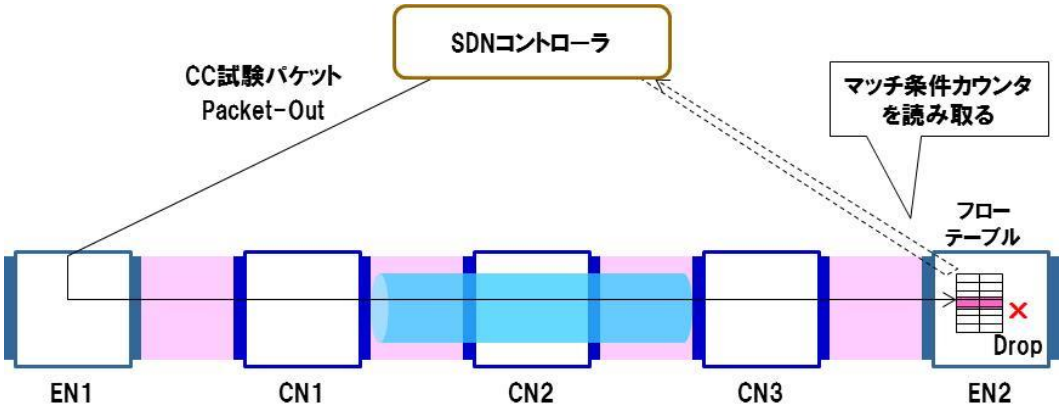


図 3-32　Drop 回線の開通試験（出側エッジノードで Drop するパタン）

2.2. 留意事項

入側エッジノードで Drop するパタンの開通試験は注意が必要である（図 3-33）。

出側エッジノードで Drop するパタンと同様の試験を行う場合、CC 試験パケットをコントローラから入側エッジノード EN1 に Packet-Out するが、EN1 では、ユーザが使用する Drop 回線の入力ポート en11 と、CC 試験パケットが使用する入力ポート en10 が異なる。そのためフローエントリが異なるため、Drop 回線の試験を行うことができない。

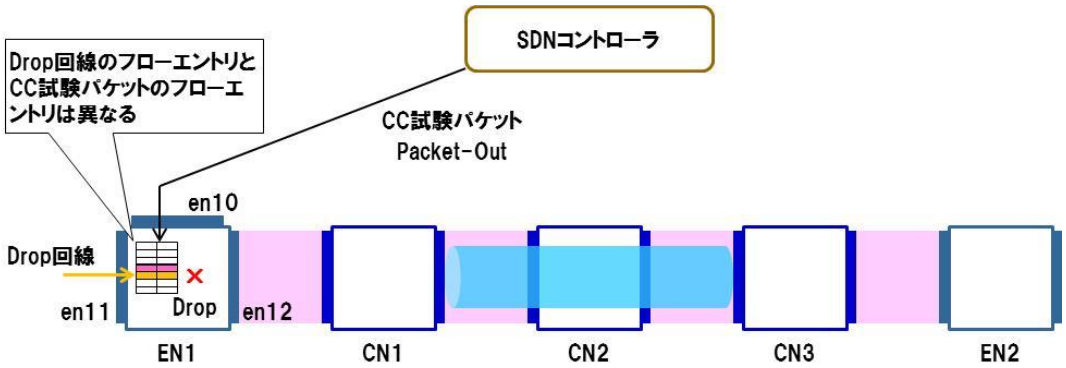


図 3-33　入側エッジノードで Drop するパタンの留意事項

入側エッジノードで Drop されるパタンの開通試験を行う場合には、エッジノードの外側（ユーザ宅等）に試験用のノードを置き、試験用ノードから試験用パケットを挿入して、Drop 回線と同一のフローエントリを用いるようにする。

①コントローラから入側エッジノード EN1 のフローエントリの Match 条件カウンタを読み取る。

②ユーザ宅側の試験用ノードから試験用パケットを挿入する。

③入側エッジノード EN1 では、フローエントリに従い試験用パケットを Drop し、フローエントリの Match 条件カウンタをカウントアップする。

④コントローラから入側エッジノード EN1 の Match 条件カウンタを読み取り、①で読み取った値と比較しカウントアップされていることを確認する。

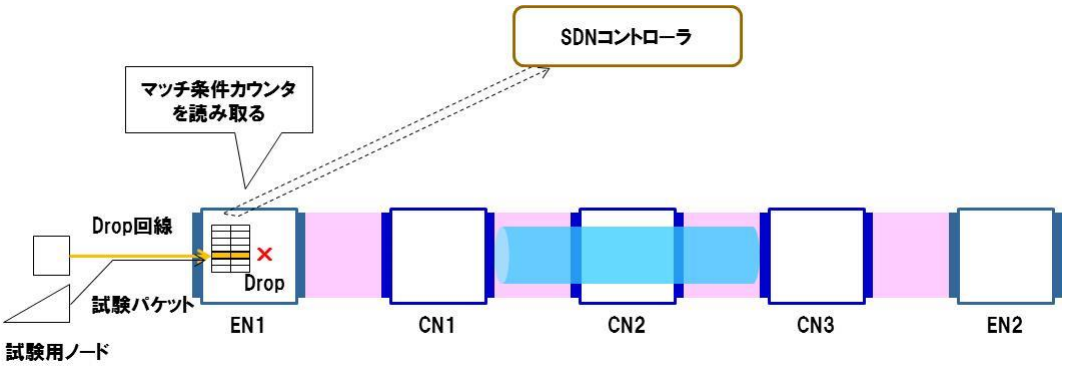


図 3-34　Drop 回線の開通試験（入側エッジノードで Drop するパタン）

なお、Match 条件カウンタは OpenFlow で規定されているものであるが、現状は装置の実装依存の部分が多いので注意が必要である。

第5章 分岐回線の運用・監視

『第 5 章 分岐回線の運用・監視』では、第 1 節において本章で説明の前提とする分岐回線のモデルについて示し、第 2 節において Drop 回線の開通時の試験方法及び開通後の正常性の定期監視方法について示す。第 3 節では、定期監視により異常を検出した場合の迂回方法や被疑箇所の推定方法について示す。

- 第 1 節 分岐回線モデル
- 第 2 節 分岐回線の開通試験・定期監視
- 第 3 節 分岐回線の異常措置

第1節 分岐回線モデル

第 3 編第 1 章第 3 節に示すように、分岐回線は、経路の途中でパケットをコピーし、複数の対地に対して通信を行う回線オプションである。

分岐回線のモデルとして、エッジノードで分岐する場合と、コアノードで分岐する場合とが考えられるが、本章では、エッジノードで回線の分岐処理（パケットのコピー）を行うモデルを基本とする。

これは以下の理由からである。第 2 編第 3 章第 3 節に示すようにエッジノードとコアノードは機能分担を明確にしている。

エッジノードでは個々の回線単位の処理と網内タグの管理を担い、コアノードでは網内タグを利用して中継パス間のパケット転送を効率的に行うことが求められる。つまり、コアノードでは回線単位の処理を行わないことから、分岐回線においても、エッジノードで回線の宛先に応じたパケットのコピー処理を行い、分岐した回線に応じた網内タグの管理を行うモデルが、SDN ノードの機能分担に適合する。

エッジノードで分散処理を行うモデルにおいて、コアノードの配下に複数のエッジノードがある場合、分岐処理を行うエッジノードを代表するノードに集約するパタン（図 3-35）と、複数のノードに分散するパタン（図 3-36）が考えられる。

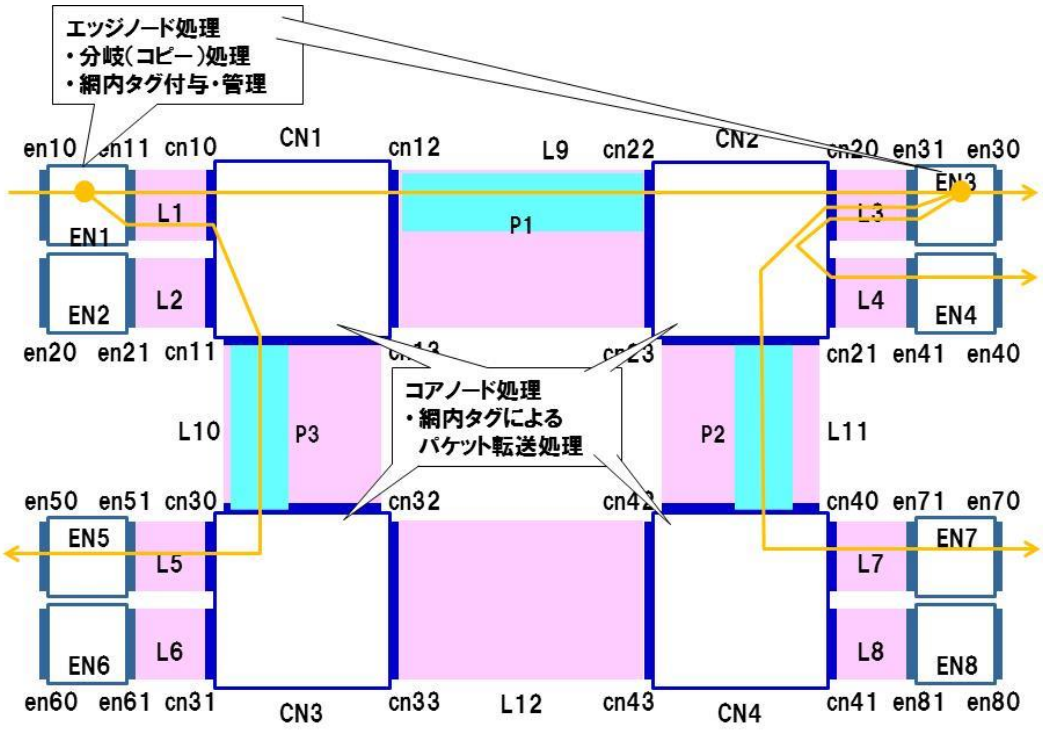


図 3-35　分岐回線モデル（エッジノードを集約するパタン）

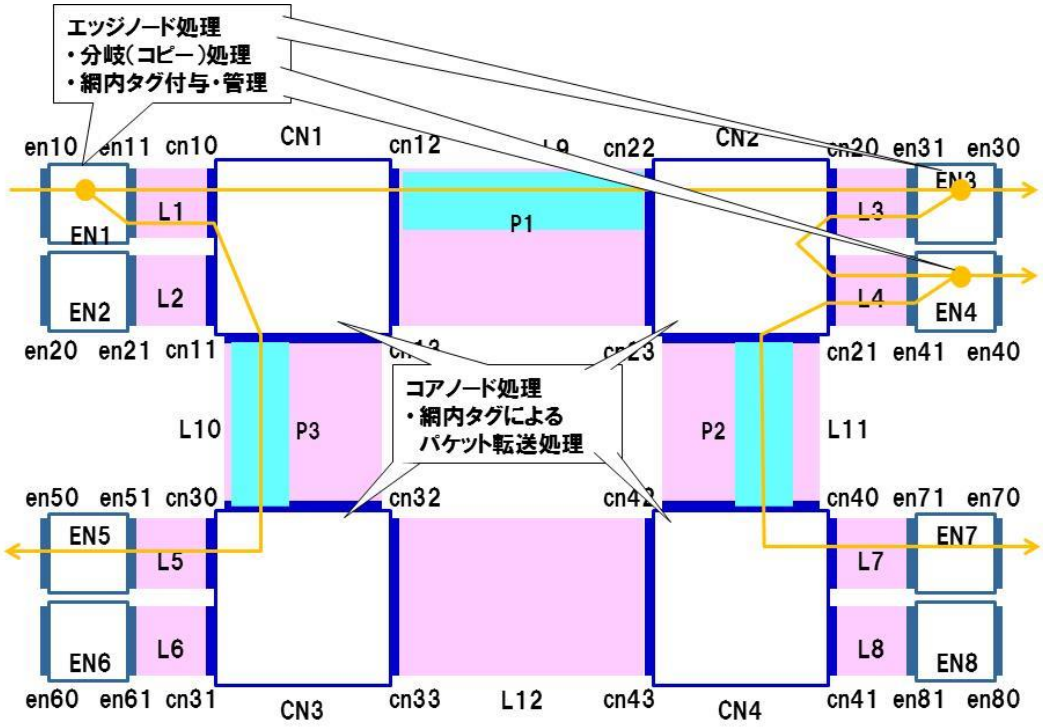


図 3-36　分岐回線モデル（エッジノードを分散するパタン）

図 3-37 は分岐回線モデルの多面構成の例である。図 3-37 では、A 面の現用系の分岐回線に対して、予備系となる分岐回線が B 面に予め設定され、A 面で異常が発生した際には、B 面へ切替えられるようにする。また、各面内の中継パスについても図 3-38 に示すように、それぞれ冗長構成ありで設定をしておき、中継パスで異常が発生した際には、同一面内の予備系の中継パスに切替えられるようにしておく。

なお、分岐回線で使用する中継パスは Point-to-Point 回線で使用する中継パスと共用する。

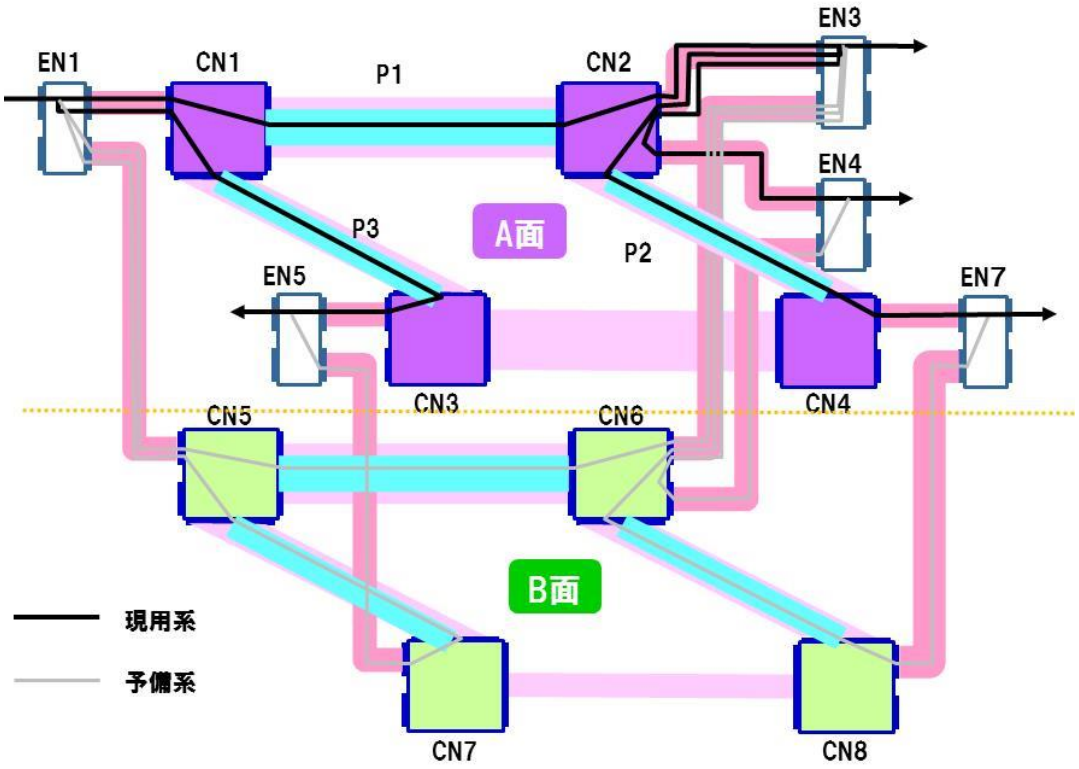


図 3-37　分岐回線モデル（多面構成）

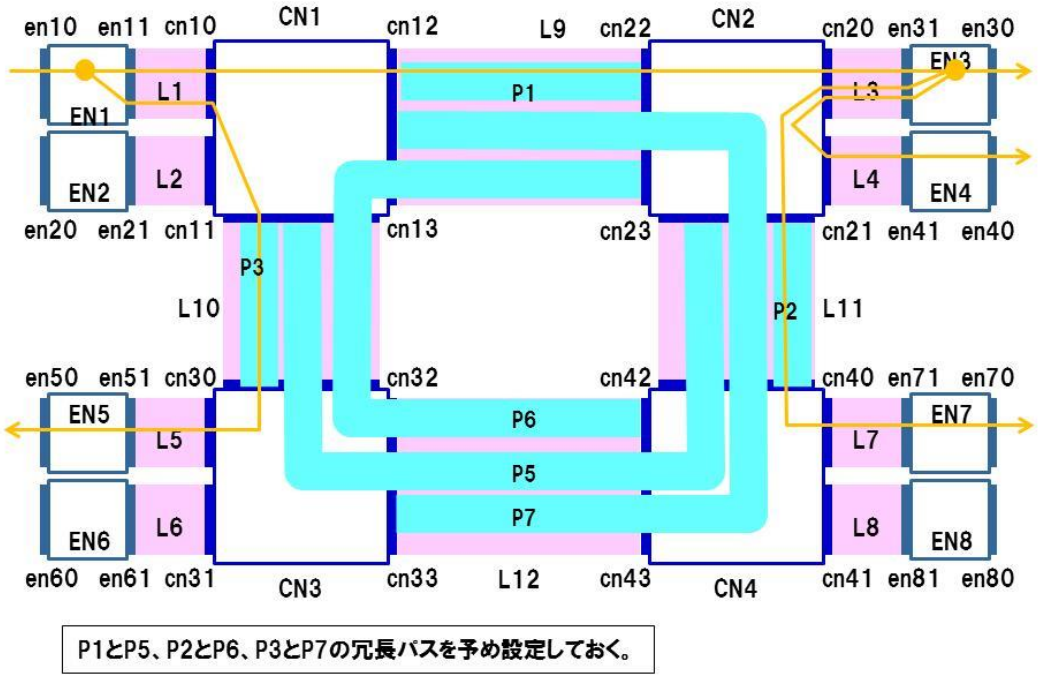


図 3-38　分岐回線モデル（面内の中継パス）

第2節 分岐回線の開通試験・定期監視

1. 開通試験・定期監視の基本的な考え方

分岐回線の開通には、新規に分岐回線を開通しフロー全体を設定する場合と、既存の分岐回線に新たな分岐先を追加設定する場合とがある。どちらの場合においても、分岐回線としての開通試験と、分岐回線が使用する中継パスとしての開通試験を行うが、分岐回線で使用する中継パスは、Point-to-Point 回線で使用する中継パスと共用するため、Point-to-Point 回線の開通時に該当する中継パスの正常性を確認している場合には、試験を省略することができる。中継パスの試験方法は、第 3 編第 3 章第 2 節の Point-to-Point 回線の中継パスの試験方法を参照のこと。

新規の分岐回線の開通試験（フロー全体を設定）では、分岐回線や利用する中継パスについて、フローエントリの正常性やリンクの正常性を確認し、意図したとおりにパケットを送信できるか確認する。確認ポイントとして以下の 3 つがある。

①全ての宛先まで送信されること

回線及び中継パスの全ての始点・終点間で、パケットが疎通することを確認する。この試験には CC ツールを用いる。

②正しい経路で送信されること

回線及び中継パスの全ての始点・終点間で、経由する SDN ノードが意図した通りかを確認する。この確認には LT ツールを用いる。

③宛先以外に送信されないこと

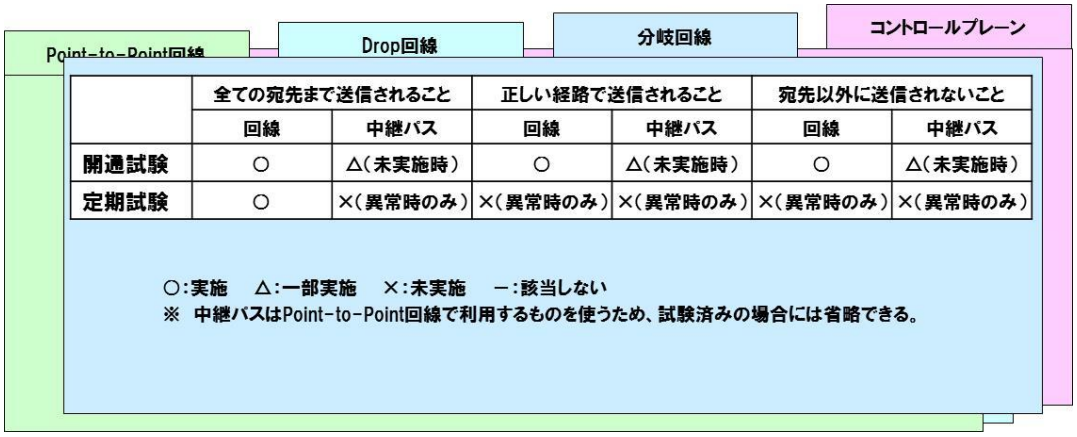
回線及び中継パスが、意図しないパケットの分岐などにより宛先以外に送信されないことを確認する。確認には CC ツールを使用する。

既存の分岐回線に新たな分岐先を追加設定する場合には、追加するフローに対して、フロー全体の開通試験と同様の確認が必要となる。

分岐回線の定期監視では、運用中の回線及び中継パスを定期的に監視して正常性が維持されていることを確認する。定期監視では、「①宛先まで送信されること」の試験を行う。「②正しい経路で送信されること」「③宛先以外に送信されな

いこと」については、SDN コントローラの処理負荷増加の懸念があるため、異常検出時に適宜実施するのがよい。

これらを図 3-39 にまとめる。



	全ての宛先まで送信されること		正しい経路で送信されること		宛先以外に送信されないこと	
	回線	中継パス	回線	中継パス	回線	中継パス
開通試験	○	△(未実施時)	○	△(未実施時)	○	△(未実施時)
定期試験	○	×(異常時のみ)	×(異常時のみ)	×(異常時のみ)	×(異常時のみ)	×(異常時のみ)

図 3-39　分岐回線の開通試験・定期監視

2. 全ての宛先まで送信されることの試験

2.1. 試験手順

「全ての宛先まで送信されること」の試験は Continuity Check (CC) ツールにより確認する。分岐回線の回線レベルの試験は図 3-40 に示すように実施できる。

①入側エッジノード EN1 において、分岐回線 C1 に対する CC 試験パケットについて、分岐回線 C1 と同一の処理（分岐処理、網内タグ付与、転送処理）を行うための、試験用フローエントリを設定する。

②全ての出側エッジノード EN3、EN4、EN5、EN7 において、分岐回線 C1 に対する CC 試験パケットについて、必要な情報（dpid 等）を付加してコントローラに Packet-In させるための、試験用フローエントリを設定する。

③コントローラから入側エッジノード EN1 に、分岐回線 C1 に対する CC 試験パケットを Packet-Out する。

④入側エッジノード EN1 では、①で設定した試験用フローエントリに従い、CC 試験パケットの分岐処理、網内タグの付与、転送処理を行う。

⑤コアノードでは、網内タグに基づき、分岐回線 C1 が用いるフローエントリに従って、CC 試験パケットを転送する。

⑥出側エッジノードでは、②で設定した試験用フローエントリに従い、分岐処理、網内タグの付与、転送処理を行うとともに、CC 試験パケットに必要な情報（dpid 等）を付加してコントローラへ Packet-In する。

⑦コントローラでは、③で Packet-Out した CC 試験パケットが、全ての宛先の出側エッジノードから Packet-In することにより、全ての宛先まで送信されたことを確認する。

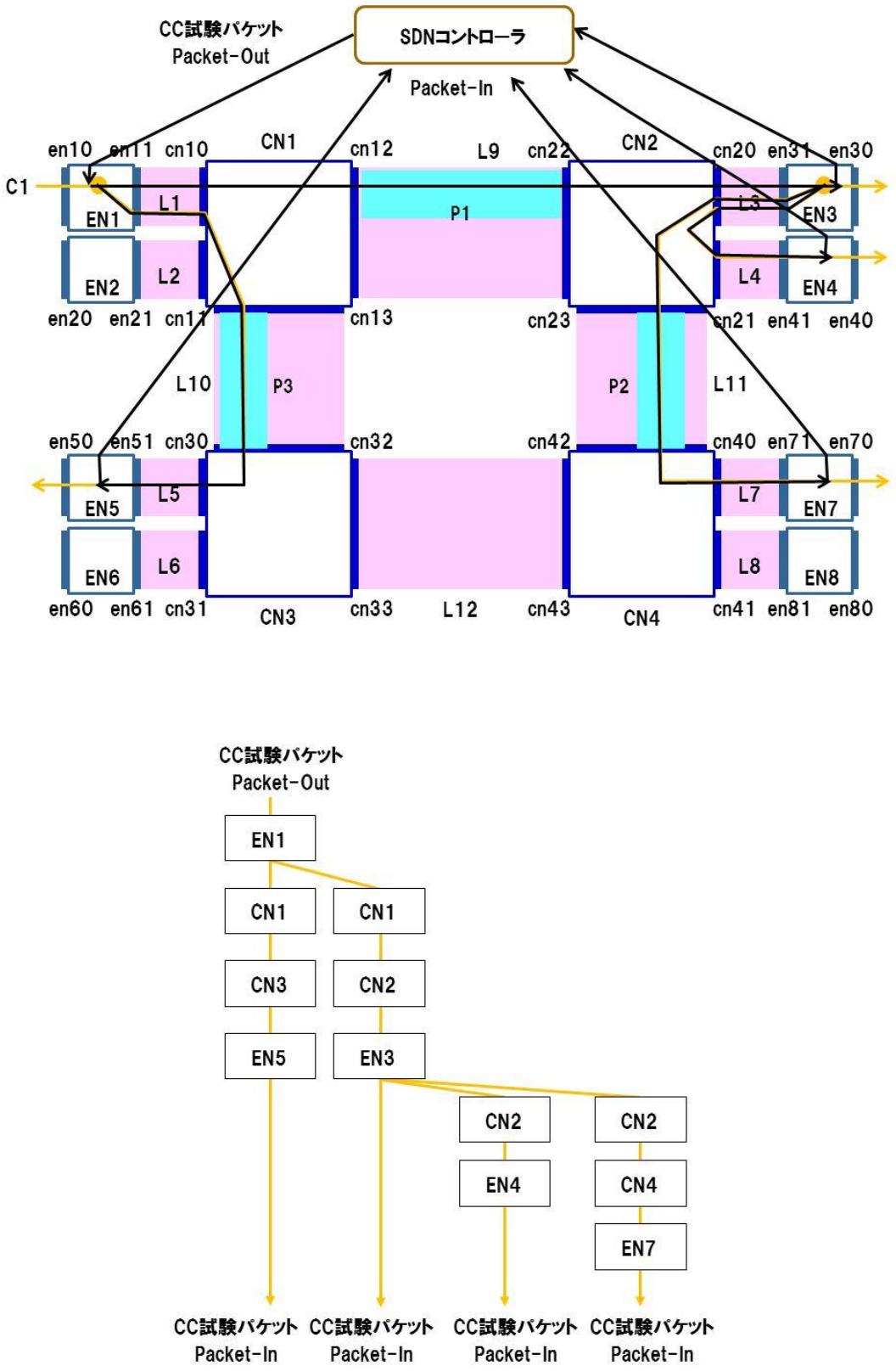


図 3-40　全ての宛先まで送信されることの試験（分岐回線）

既存の分岐回線に新たな分岐先を追加設定する場合の開通試験も、同様に CC ツールを用いて、新たに追加した宛先の出側エッジノードから CC 試験パケット パケットがコントローラに Packet-In することにより、全ての宛先まで送信されたことを確認する。

2.2. 留意事項

本試験では、CC 試験パケットをコントローラから入側エッジノードに Packet-Out する。入側エッジノードでは、ユーザが使用する分岐回線の入力ポートと、CC 試験パケットが使用する入力ポートが異なるため、分岐回線とは別のフローエントリ（試験用のフローエントリ）を用いることになる。このため、入側エッジノードのフローテーブルの確認は行えない。

入側エッジノードのフローテーブルの確認を行うには、図 3-41 のように入側エッジノードの外側（ユーザ宅等）に試験用のノードを置き、試験用ノードから CC 試験パケットを挿入する等の方法が必要になる。なお、本試験はユーザ側に試験用ノードを置く必要があるため、定期監視は推奨しない。

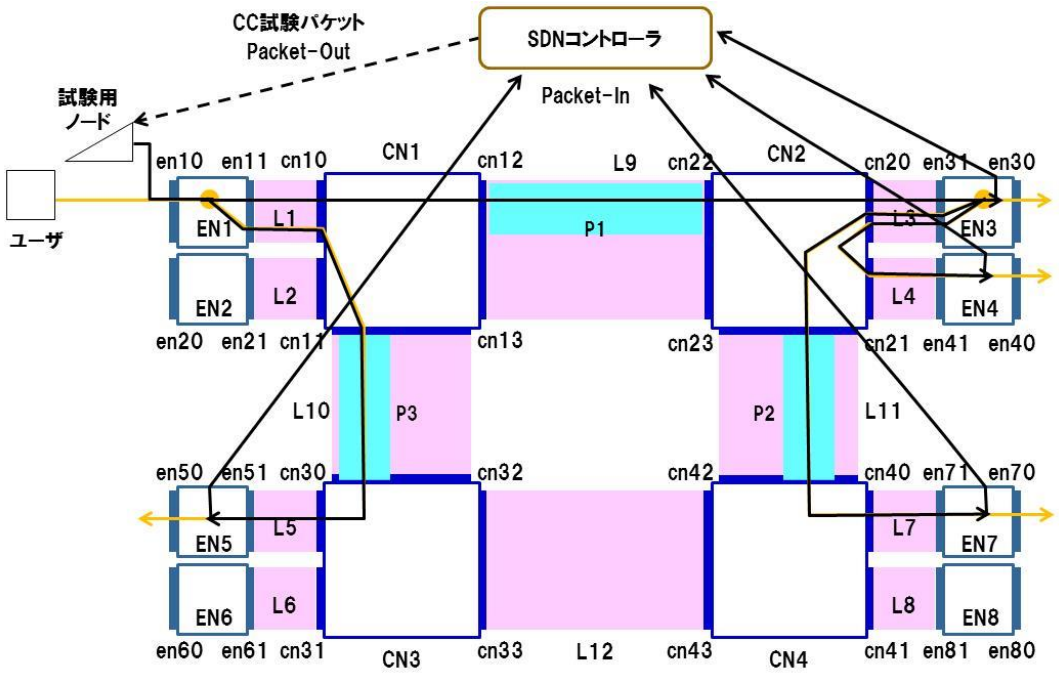


図 3-41　入側エッジノードのフローテーブルの確認

3. 正しい経路で送信されることの試験

3.1. 試験手順

「正しい経路で送信されること」の試験は Link Trace (LT) ツールにより確認する。分岐回線は、宛先が分岐した後、複数の経路にパケットが同時に転送されるため、経路の把握が難しくなる。そのため、分岐回線を複数の Point-to-Point 回線に分解し、個々の Point-to-Point 回線の経路として試験する。

図 3-42 の例では、入側エッジノード EN1 の宛先として、出側エッジノード EN5、EN3、EN4、EN7 が存在する。この分岐回線を以下の 4 つの Point-to-Point 回線に分解して考える。

- 入側エッジノード EN1～出側エッジノード EN5
- 入側エッジノード EN1～出側エッジノード EN3
- 入側エッジノード EN3～出側エッジノード EN4
- 入側エッジノード EN3～出側エッジノード EN7

分解したそれぞれの回線に対してコントローラより LT 試験パケットを Packet-Out（LT1、LT2、LT3、LT4）して経路を確認する。

①分解したそれぞれの回線に対して、送信元となるエッジノードへコントローラから LT 試験パケットを Packet-Out する。

②分解したそれぞれの回線の送信元となるエッジノードには、分岐回線の分岐後のフローと同じ処理を行うようフローエントリを設定しておき、LT 試験パケットに網内タグを付与して転送処理を行う。

③コアノードでは、LT 試験パケットをコピーし、必要な情報（dpid 等）を付加してコントローラに Packet-In させるとともに、通常の分岐回線の処理に従い網内タグにより LT 試験パケットを転送する。

④分解したそれぞれの回線の宛先のエッジノードでは、LT 試験パケットに必要な情報（dpid 等）を付加してコントローラに Packet-In させ、ユーザや他の分岐経路には届かないようにする。

⑤コントローラでは、分解したそれぞれの回線別に、Packet-In した LT 試験パケットに付加されたノード情報や TTL (Time To Live) を確認し、TTL の順番に抜けがないことを確認する。分解したそれぞれの回線で経路が正しいことを確認できたら、分岐回線全体として正しい経路で送信されていると判断する。

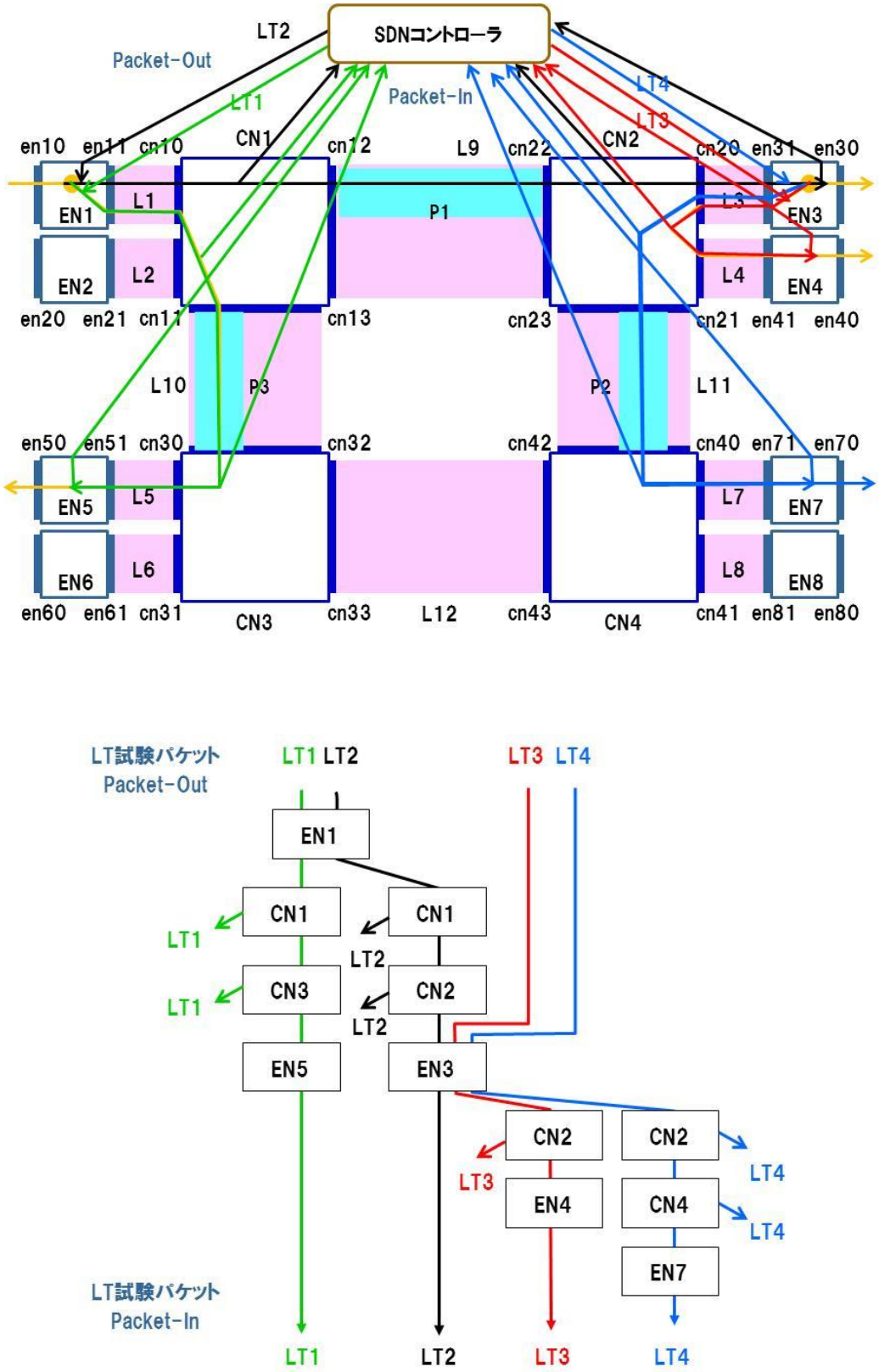


図 3-42　正しい経路で送信されることの試験（分岐回線）

既存の分岐回線に新たな分岐先を追加設定する場合の開通試験は、追加した経路を個別の Point-to-Point 回線として分解し、LT 試験パケットを用いた同様の試験により確認を行う。

3.2. 留意事項

本試験では、LT 試験パケットをコントローラからエッジノードに Packet-Out する。エッジノードでは、ユーザが使用する分岐回線の入力ポートと、LT 試験パケットが使用する入力ポートが異なるため、分岐回線とは別のフローエントリを用いることになる。このため、エッジノードで分岐回線が実際に分岐処理を行うフローエントリの確認は行えない。

分岐回線が使用するフローエントリを確認するには、図 3-43 のようにエッジノードの手前のノード(EN3 の場合には CN2)に LT 試験パケットを Packet-Out し、分岐後に Packet-In する LT 試験パケットを TTL 順に並べ、分岐経路外のノードから Packet-In していないことを確認する。

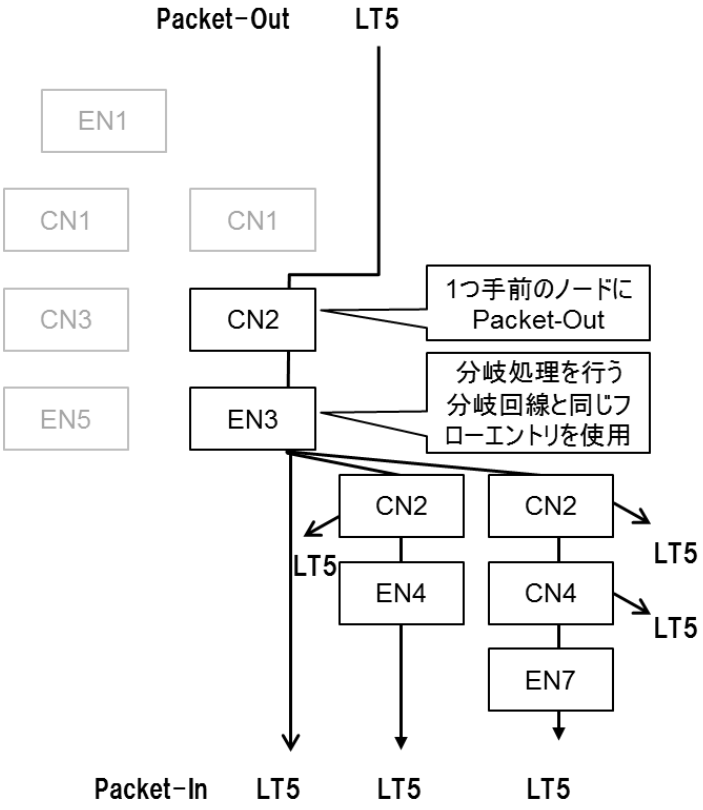


図 3-43　エッジノードのフローテーブルの確認

4. 宛先以外に送信されないことの試験

4.1. 試験手順

「宛先以外に送信されないこと」の試験は Continuity Check (CC) ツールにより確認する（LT ツールでも代用可能)。分岐回線の回線レベルの試験は図 3-44 のように実施できる。

「全ての宛先まで送信されること」の試験と同様の方法となるが、宛先以外のエッジノードも含め、全てのエッジノードに対して、送信される CC 試験パケットをコントローラに Packet-In するよう試験用フローエントリを設定する点が異なる。コントローラでは宛先以外のエッジノードから CC 試験パケットの Packet-In があった場合に、宛先以外に送信されたをとを確認できる。図 3-44 では、宛先以外の EN8 からの Packet-In があることにより宛先以外に送信されたことを判断する。

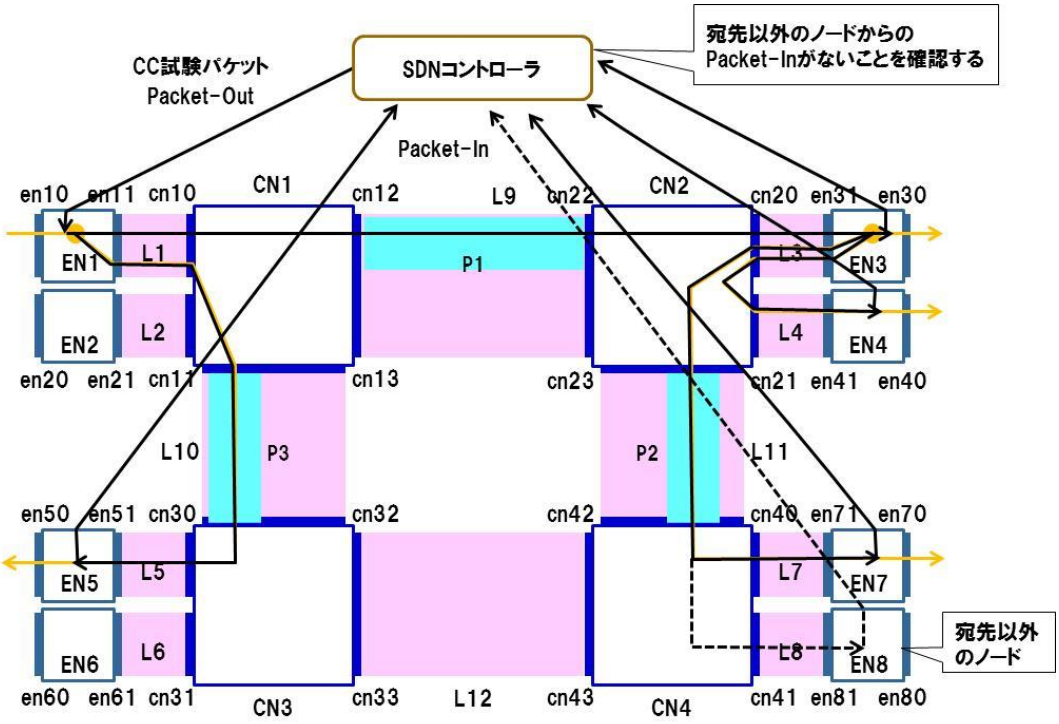


図 3-44　宛先以外に送信されないことの試験

既存の分岐回線に新たな分岐先を追加設定する場合の開通試験も、同様に CC ツールを用い、宛先以外の出側エッジノードから Packet-In しないことを確認する。

4.2. 留意事項

「宛先以外に送信されないこと」の試験は、予期しないノードからの Packet-In の検出を行うこととなるため、開通時にのみ行うこととし、定期監視は推奨しない。

第3節 分岐回線の異常措置

定期監視プロセスで異常を検出した場合は異常措置プロセスへと移行し、冗長化されたネットワークリソースに切替えることにより、ネットワークサービスの中断を極力抑えることができる。

サービス中断時間の短縮のためには、検出した故障に応じて適切な切替えを行うことが重要である。中継パスレベルの定期監視で故障を検出した場合には、同一面内での中継パス単位での切替えを行い、回線レベルの定期監視で故障を検出した場合には、個々の回線単位で面の切替え（A 面から B 面への切替え等）を行うことが望ましい。また、分岐回線では、経路の途中で分岐処理を行うエッジノードが故障した際の切替えについても考慮する必要がある。

予備系への切替え後は、LB ツール等を利用して故障の被疑箇所を推定し、リセットやハードウェア交換等の回復措置を行う必要がある。また、回復措置後は、正常性を確認して現用系に切戻しをすることが望ましい。切戻しはオペレータ主導で行う。

なお、工事等のために運用中の回線や中継パスを、冗長化したリソースに切替える支障移転の場合も、オペレータ主導で、中継パスや面の切替えを行う。

分岐回線では複数の宛先向けに経路が複雑化し、異常の発生箇所により影響を受ける宛先も変化する。予め異常措置を考慮したネットワーク設計を行うとともに、設備と回線の収容関係が明確となるような情報の管理を行うことも重要である。

1. 中継パスレベルの切替え

中継パスの定期監視で異常を検出した場合には、図 3-45 で示すように同一面内で中継パスの切替えを行う。

これにより、中継パスの異常で影響を受けた分岐回線を 1 本ずつ切替える必要がなく、中継パスに収容される Point-to-Point 回線や分岐回線の区別なく一括して切替えることができる。

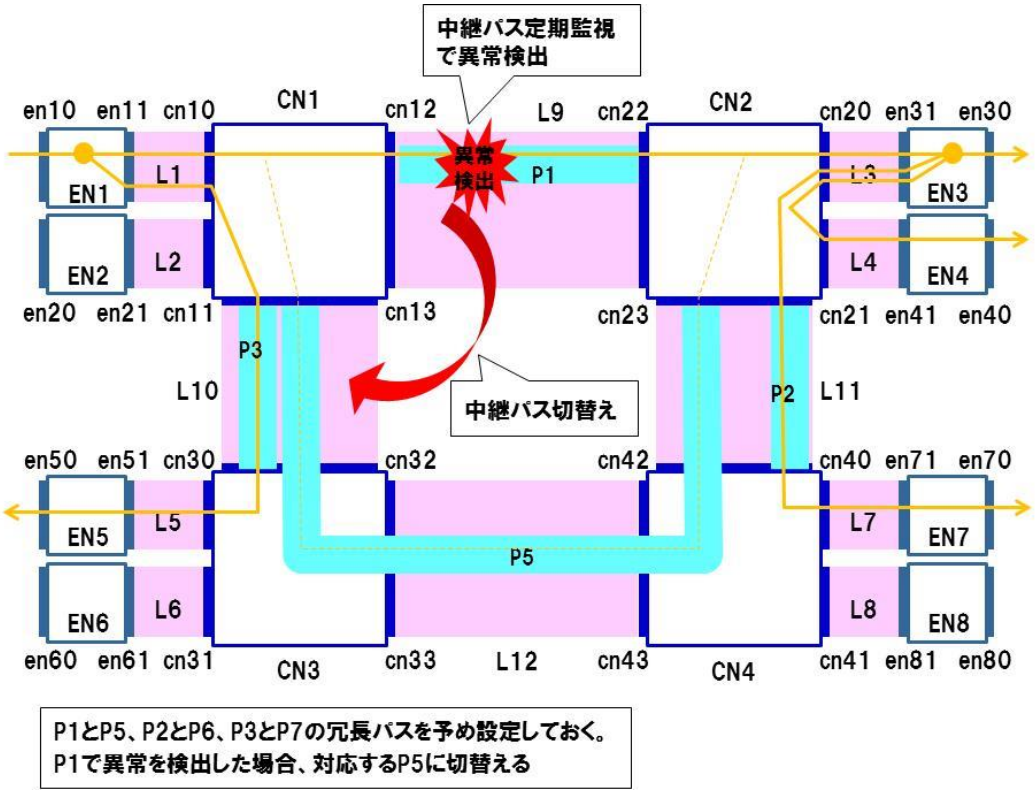


図 3-45　中継パスレベルの切替え（分岐回線）

図 3-45 は、コアノード CN1 とコアノード CN2 間のリンク L9 が故障し、中継パス P1 の定期監視で故障を検出した場合の例である。この場合、エッジノード EN5 宛の通信には影響はないが、その他の分岐先であるエッジノード EN3、EN4、EN7 ではサービス中断となる。

コアノード CN1 とコアノード CN2 間の中継パス P1 を、予備系の中継パス P5 に切替えることで、中継パス P1 に収容していた分岐回線は全て中継パス P5 に切替えられ、エッジノード EN3、EN4、EN7 のネットワークサービスが救済される。

2. 面の切替え

回線の定期監視で異常を検出した場合には、図 3-46 で示すように個々の回線単位で面の切替え（A 面から B 面への切替え等）を行う。

回線レベルの定期監視の故障検出間隔に対し、中継パスレベルの定期監視の故障検出間隔を短く設定することで、中継パスの異常を優先的に検出できるようになり、不必要な切替えを避けることができる。

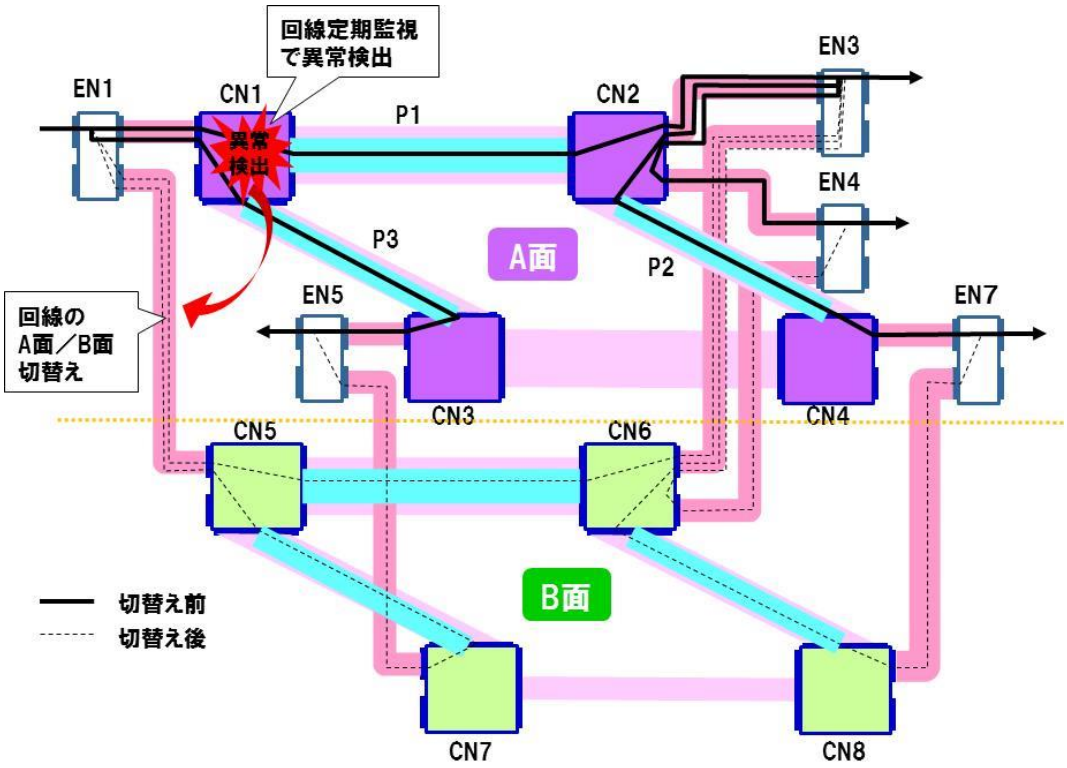


図 3-46　面レベルの切替え（分岐回線）

3. 分岐処理を行うエッジノードの切替え

分岐処理を行っているエッジノードが故障した場合には、回線の定期監視で故障を検出できるが、回線の A 面／B 面の切替えでは分岐回線を救済することができない。

図 3-47 は分岐回線の分岐処理を行うエッジノード EN3 が故障した例である。この場合、EN3 配下の回線は故障の影響を受けサービスが中断する。さらに、故障の影響を直接的には受けない、EN3 の分岐先の EN4、EN7 でもサービス中断となり、故障の影響範囲が拡大している（経路の異なる EN5 は影響を受けない）。

この状況で A 面から B 面への切替えを行ったとしても、分岐処理を行う EN3 を回避しない限りは、EN3、EN4、EN7 のサービス中断を救済することができない。

これより、回線の定期監視で故障を検出した場合には、分岐処理を行っているエッジノードで故障が発生していないかを確認し、適切な対応が求められる。

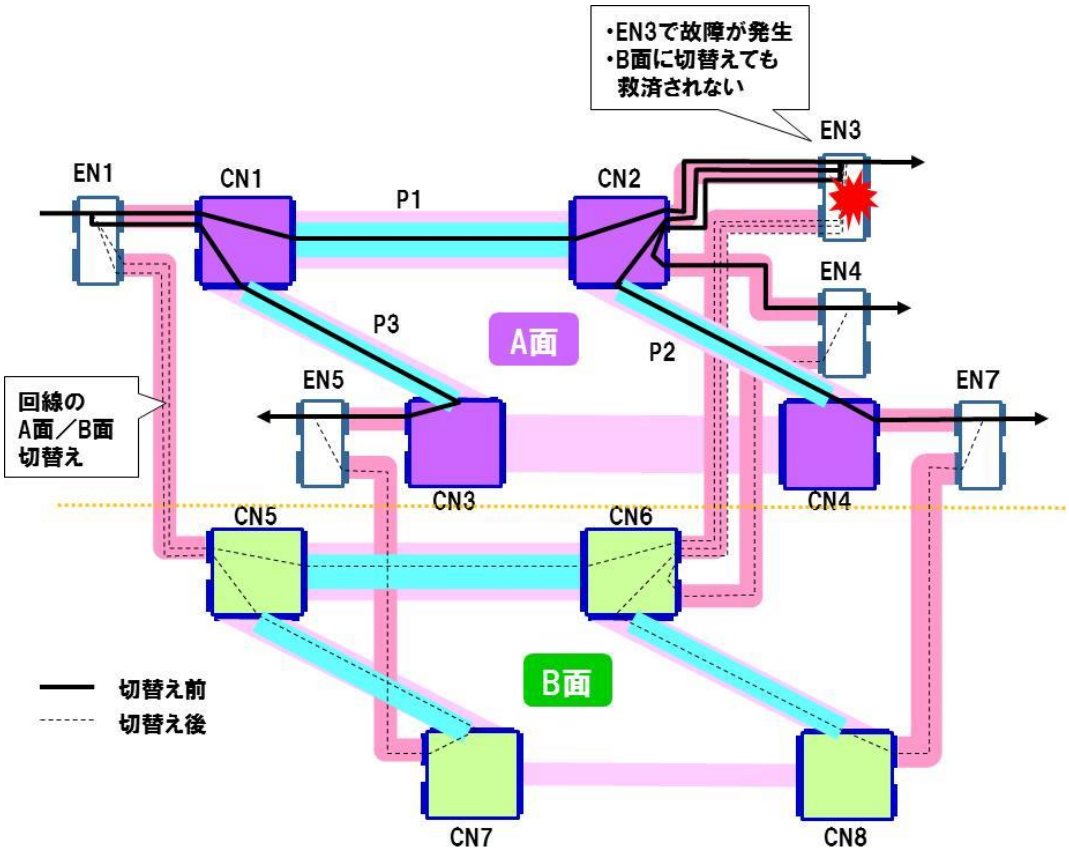


図 3-47　エッジノード故障時の例

3.1. ケース 1 ：エッジノードで 2 つ以上の宛先に分岐

本ケースでは、故障の発生したエッジノードを経由せずに、他のエッジノードで分岐処理を行うように変更する。

図 3-48 では、エッジノード EN3 において、EN4 と EN7 向けの分岐処理を行っている。EN3 の故障の際には、コアノード CN2 において、エッジノード EN3 ではなく EN4 へ転送するようフローテーブルを変更し、さらに、エッジノード EN4 において、分岐回線の分岐処理を行うようフローテーブルを変更する。これ

により EN3 の分岐処理が EN4 に代行され、EN4 と EN7 のサービスが救済される（EN3 については早急に回復措置を行う必要がある）。

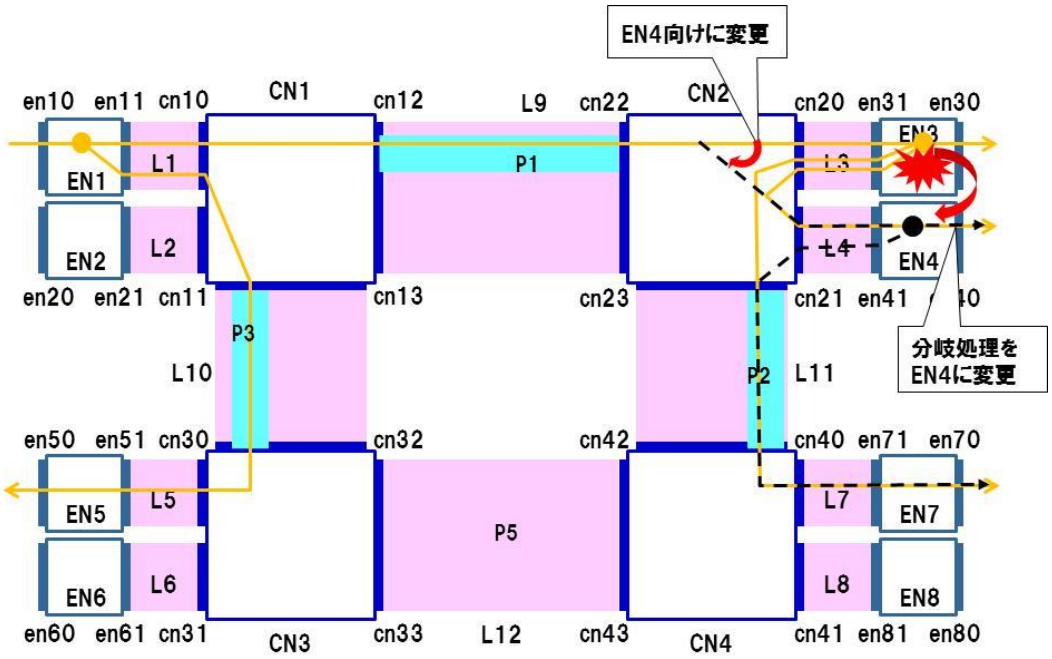


図 3-48　複数宛先に分岐処理を行うエッジノードの故障

3.2. ケース 2：エッジノードで 1 つの宛先に分岐

本ケースでは、故障の発生した分岐処理を行っているエッジノードを、分岐回線の経路から除くように変更する。

図 3-49 では、コアノード CN2 の配下にエッジノード EN3 と EN4 とがあり、EN3 において EN4 向けの分岐処理、さらに、EN4 において EN7 向けの分岐処理を行っている（CN2 配下の各エッジノードで 1 つの宛先に分岐）。

EN3 の故障の際には、コアノード CN2 において、エッジノード EN3 ではなく EN4 へ転送するようフローテーブルを変更する。これにより EN4 と EN7 のサービスが救済される（EN3 については早急に回復措置を行う必要がある）。

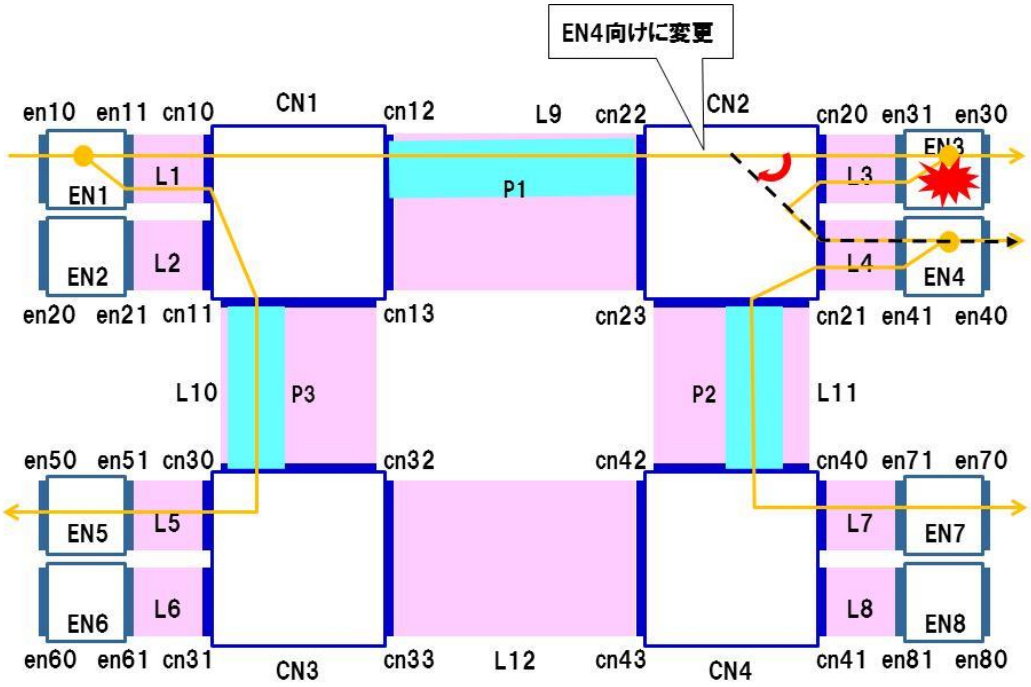


図 3-49　1 つの宛先に分岐処理を行うエッジノードの故障(1)

図 3-50 では、コアノード CN2 の配下にエッジノード EN3 しかなく、EN3 において EN7 向けの分岐処理を行っている。

EN3 の故障の際には、コアノード CN2 の配下に EN3 の分岐処理を代行できるエッジノードが存在しない。これより、EN3 を分岐回線の経路から除くために、CN1 において中継パスを P1 から P9 へ切替えて、CN1 と CN4 間の経路を設定する。そのためには、エッジノード EN1 において中継パス P9 を使用するようフローエントリを変更し、合わせて、コアノード CN4 において、中継パス P9 からの分岐回線を EN7 へ転送するようフローエントリの変更を行う。

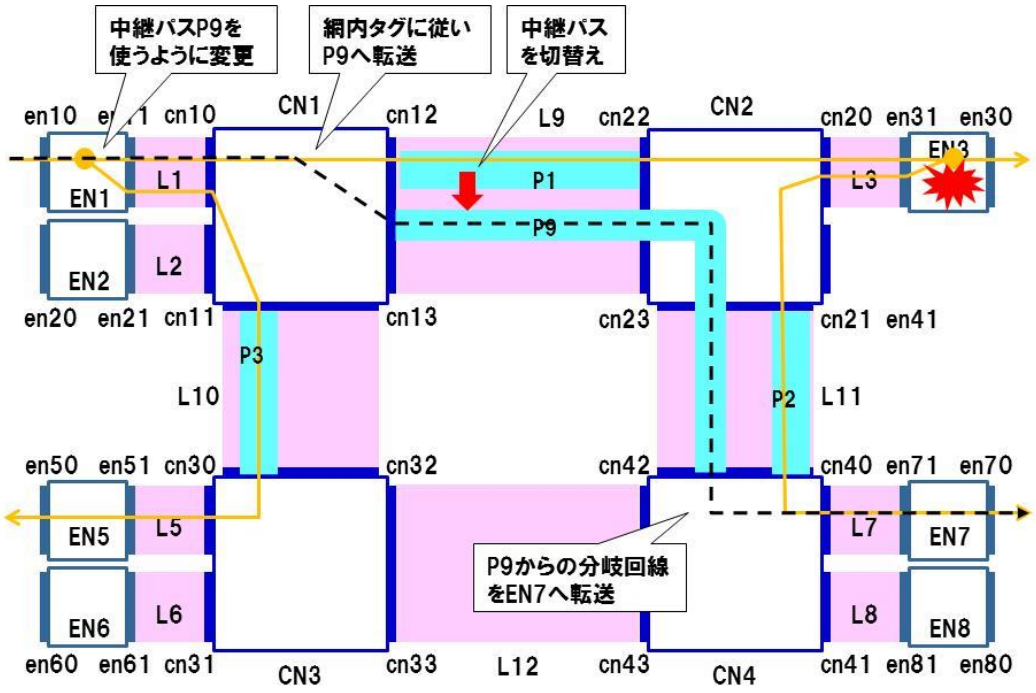


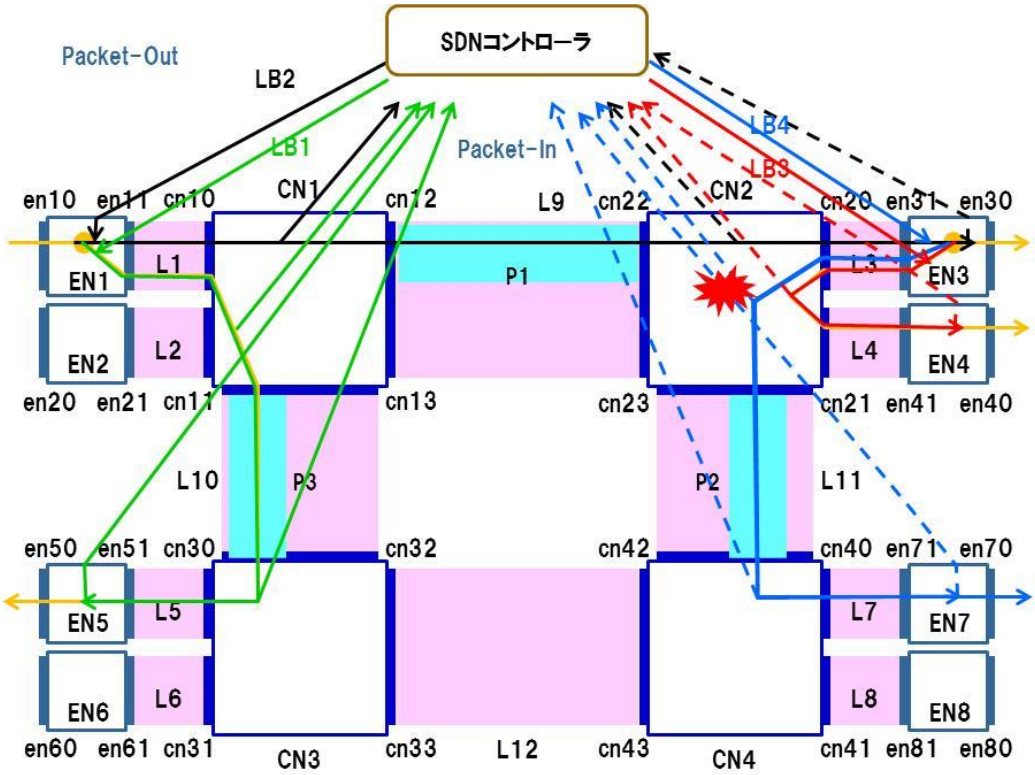
図 3-50　１つの宛先に分岐処理を行うエッジノードの故障(2)

4. 被疑箇所の推定

定期監視で異常が検出された場合には冗長系に切替えてネットワークサービスの回復を図るが、切替えた後は故障の被疑箇所の推定を行い、リセットやハードウェア交換等の回復措置を行う必要がある。被疑箇所の推定には LB ツールを用いる。

中継パスレベルで故障を検出している場合には、Point-to-Point 回線と同様に被疑箇所の推定を行うことができる。

回線レベルで故障を検出して面を切替えている場合には、分岐回線を複数の Point-to-Point 回線に分解し、個々の Point-to-Point 回線として LB ツールによる試験を行う。なお、分岐回線の分解の仕方によっては、被疑箇所を推定できない場合もある。その場合は分解箇所を変えてみるなどして、複数回の試験を組み合わせる等の工夫が必要となる。



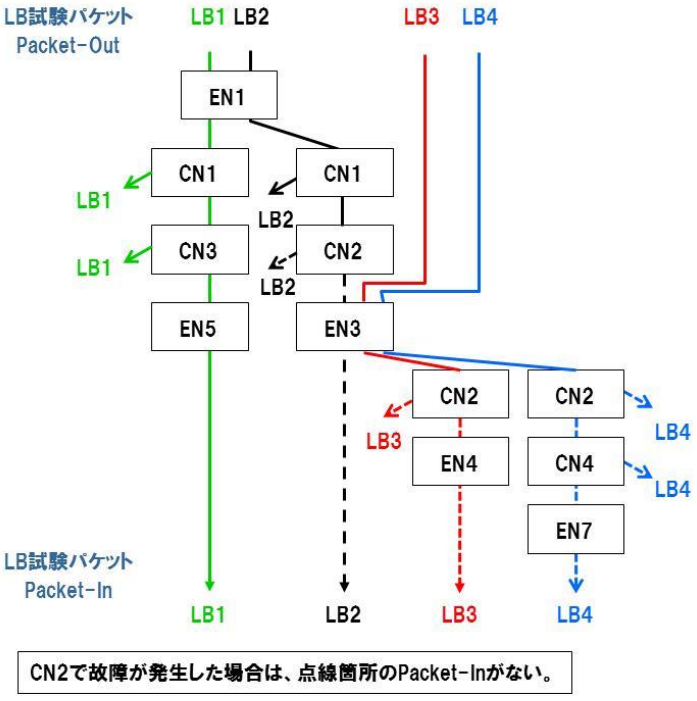


図 3-51　故障箇所の切分け

5. 支障移転時の切替え

支障移転では、運用中の回線サービスの工事等を実施するため、冗長化したリソースに予め切替えを行い、工事等を行うリソースを空けておく。図 3-52 に示すように、工事等を行う箇所により切替え方法が異なる。

- 中継パスレベルの切替えを行う場合
  - コアノード間のリンクの工事等
- 面レベルの切替えを行う場合
  - エッジノードとコアノード間のリンクの工事等
  - 入側コアノード（CN1）及び出側コアノード（CN2、CN3、CN4）の工事等
- 代替エッジノード借用を行う場合
  - 入側エッジノード（EN1）、出側エッジノード（EN3、EN4、EN5、EN7）の工事等
  - 分岐処理を行うエッジノードの工事等

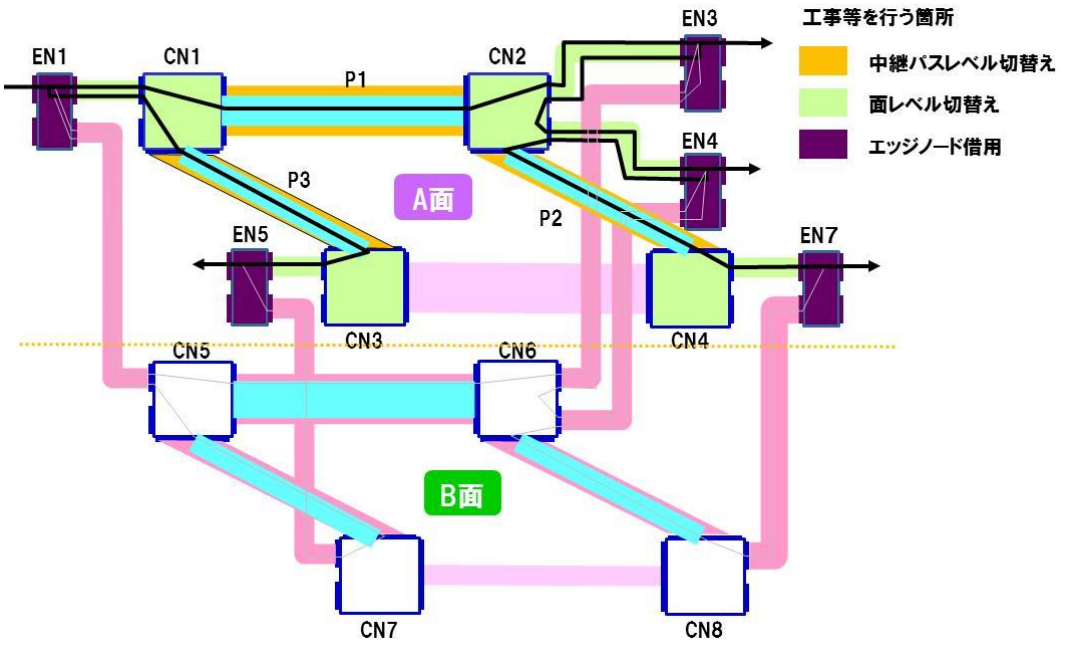


図 3-52　支障移転時の切替え方法（分岐回線）

第6章 コントロールプレーンの運用・監視

『第 6 章 コントロールプレーンの運用・監視』では、第 1 節において SDN コントローラの冗長化や運用・監視について示し、第 2 節において監視制御網の冗長化や運用・監視について示す。0 では、SDN コントローラ等から出力されるログファイルの監視について示す（図 3-53）。

- 第 1 節 SDN コントローラの運用・監視
- 第 2 節 監視制御網の運用・監視

0

● ログファイルの監視

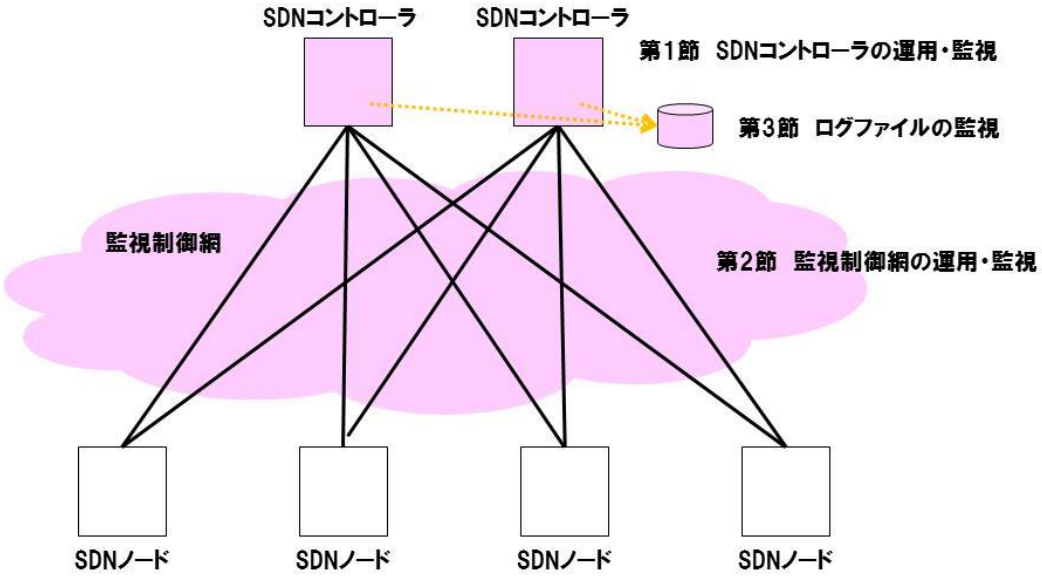


図 3-53　コントロールプレーンの運用・監視

第1節 SDN コントローラの運用・監視

1. SDN コントローラの冗長化

SDN コントローラは、パケット転送を担う SDN ノードであるスイッチ群が、どのようにパケットを処理するかを管理・制御する装置・ソフトウェアである。SDN コントローラに異常が発生した場合には、ネットワークの運用・監視に与える影響が大きく、信頼性の確保のため SDN コントローラやアプリケーション・DB の冗長化を行い、異常発生時に予備系へ切替えられるようにしておく（図 3-54）。

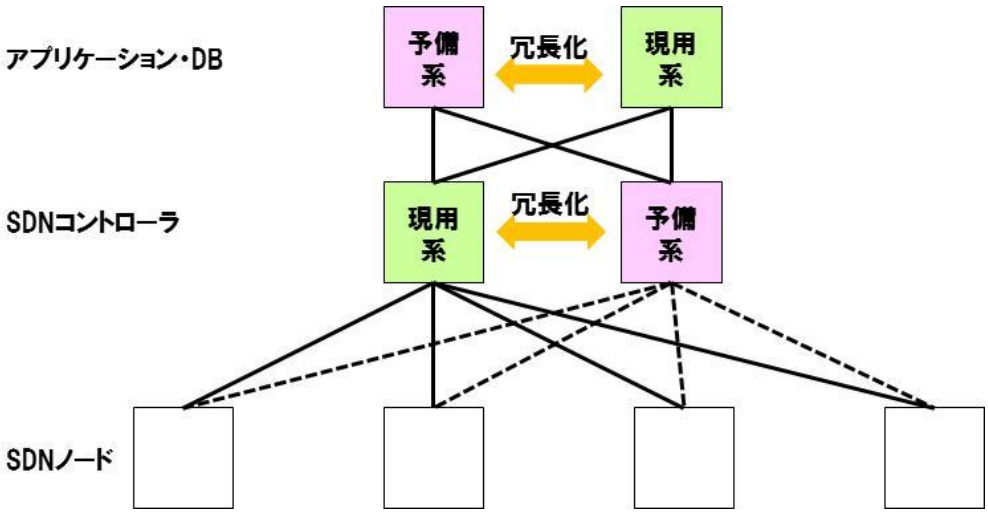


図 3-54　SDN コントローラの冗長化

2. SDN コントローラの定期監視

SDN コントローラの定期監視は、一般的な冗長化されたサーバ間の定期監視と同様の方法で実施できる。

SDN コントローラ間で定期的に通信を行い、この通信の途絶により故障を認識する。SDN コントローラ自身の故障の場合のほか、SDN コントローラ間のネットワーク故障の場合にも、SDN コントローラ間の定期的な通信は途絶するので注意が必要である。ネットワーク故障の場合、定期的な通信の途絶により、双方の SDN コントローラは他方の SDN コントローラの故障と認識し、SDN コントローラの切替えを繰り返し不安定になる恐れもある。SDN ノード等との通信等、第 3 者的な視点も踏まえて切替えることが必要となる。

OpenFlow では、OpenFlow コントローラと OpenFlow スイッチ間で、Role 要求メッセージ／Role 応答メッセージの通信を介して、OpenFlow コントローラの切替えを行っている。

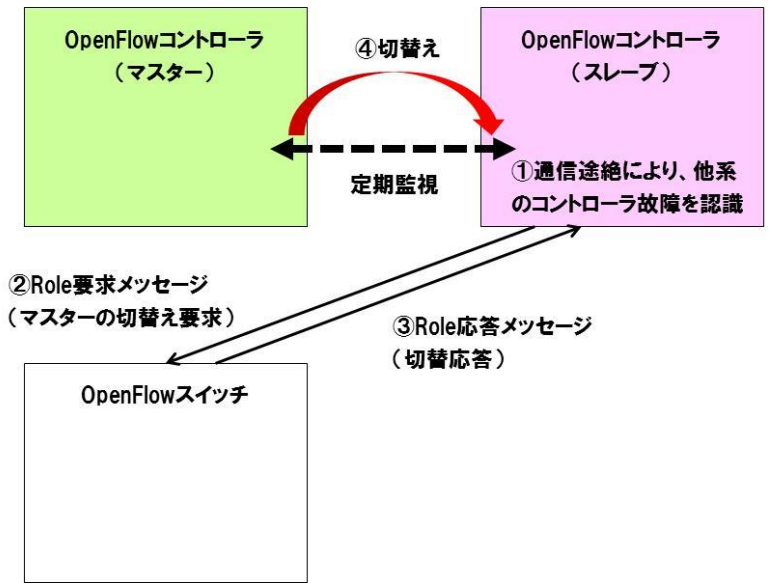


図 3-55　OpenFlow コントローラの定期監視と切替え

第2節 監視制御網の運用・監視

監視制御網は、SDN コントローラと SDN ノード間のネットワークである。監視制御網に故障が発生した場合には、SDN コントローラから SDN ノード間の通信が行えなくなり、通信できなくなった SDN ノードを経由する新たな回線の開通ができなくなるほか、SDN コントローラを用いた回線の定期監視等ができなくなり、通信できなくなった SDN ノードの運用・監視上支障が生じる。

このため、図 3-56 のように監視制御網も冗長化しておくことが望ましい。自前の設備を利用するほか、他社の通信事業者のネットワークを利用して分散する方法も考えられ、後者の方がより信頼性が高い構成といえる。

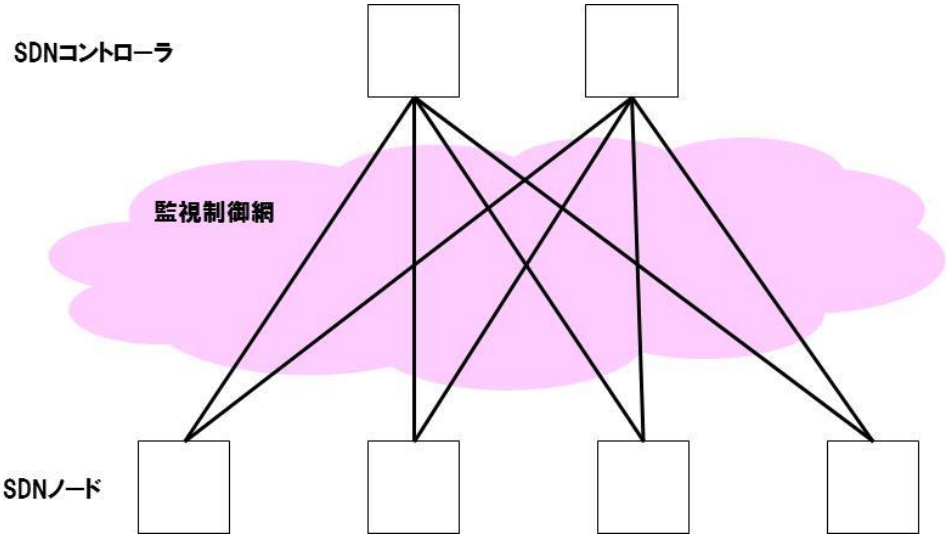


図 3-56　監視制御網の冗長化

第3節 ログファイルの監視

一般的なのサーバと同様に SDN コントローラについても、ログファイルの監視を行うことは有効である。スイッチとの接続状況の変化やエラー情報の収集、CPU やメモリ、回線等の利用率の収集、syslog の収集等を行い、問題が発見されたら解決を図るとともに、コントローラの予防保全、リソース計画等に反映させることも可能である。

第7章 統計情報の活用

第1節 統計情報の概要

OpenFlow のフローエントリの構成要素の一つに「カウンタ」があり、OpenFlow スイッチにおいて条件に一致したパケットの統計情報（転送データ量やパケット数、エラー数等）を保持している。主なカウンタを以下に示す。

- フローテーブルごと（表 3-3）
- フローエントリごと（表 3-4）
- ポートごと（表 3-5）
- キューごと（表 3-6）

表 3-3　フローテーブルごとのカウンタの例

カウンタ	ビット数
Reference Count (active entries)	32
Packet Lookups	64
Packet Matches	64

表 3-4　フローエントリごとのカウンタの例

カウンタ	ビット数
Received Packets	64
Received Bytes	64
Duration (seconds)	32
Duration (nanoseconds)	32

表 3-5　ポートごとのカウンタの例

カウンタ	ビット数
Received Packets	64
Transmitted Packets	64
Received Bytes	64
Transmitted Bytes	64
Receive Drops	64
Transmit Drops	64
Receive Errors	64
Receive Frame Alignment Errors	64
Receive Overrun Errors	64
Receive CRC Errors	64
Collisions	64

表 3-6　キューごとのカウンタの例

カウンタ	ビット数
Transmit Packets	64
Transmit Bytes	64
Transmit Overrun Errors	64

OpenFlow コントローラは「Read State メッセージ」によりカウンタの情報を取得することができ、カウンタの統計情報を利用することでトラヒック状況の可視化や、パケット流量に応じた制御などに活用できる。

- トラヒック状況の可視化
  - フロー別、VLAN 別、アプリケーション別等のパケット量の把握

- トラヒックの正常／異常状態の確認
- 設備の収容限界の把握（設備計画、予防保全への反映）

● パケット流量に応じた制御

- 帯域制御
- 負荷分散

統計情報を利用する場合の留意点を以下に示す。

取得する情報量が増すと装置の負荷も増加するため、CPU 負荷やデータベースの保存容量等を考慮して取得項目を設定する。また統計情報にはビット数の制限があり、カウントアップの上限を意識して取得情報の粒度を決める必要がある。

第2節 統計情報の活用事例

通信事業者の提供するネットワークサービスでは、ユーザに一定の通信速度を保証するギャランティ型サービスや、通信速度に保証のないベストエフォート型サービスなどが考えられるが、SDN を用いたネットワークにおいてもパケット流量に応じた帯域制御を行うことにより、品質の異なる回線サービスの提供が可能である。

OpenFlow 1.3 より導入された「メーターテーブル」を使用した帯域制御の例を示す。メーターテーブルでは、フローエントリごとのパケット流量に応じた処理方法が指定でき、トラヒックのポリシング制御が可能となる。メーターテーブル上のメーターエントリーは「Meter Identifer」、「Meter Bands」、「Counters」で構成されれ、「Meter Bands」においてパケット流量がしきい値を超えた場合の処理方法として、「drop (パケットを廃棄する)」、「dscp remark (IP パケットの DSCP 値を変更して優先度を下げる)」といった指定ができる。

例えばメーターエントリーの「Meter Bands」において「band type=drop, rate=10Mbps」と指定した場合、該当するフローエントリのパケット流量が 10Mbps 未満であればそのまま送出し、10Mbps 以上であればパケットを廃棄する（図 3-57）。

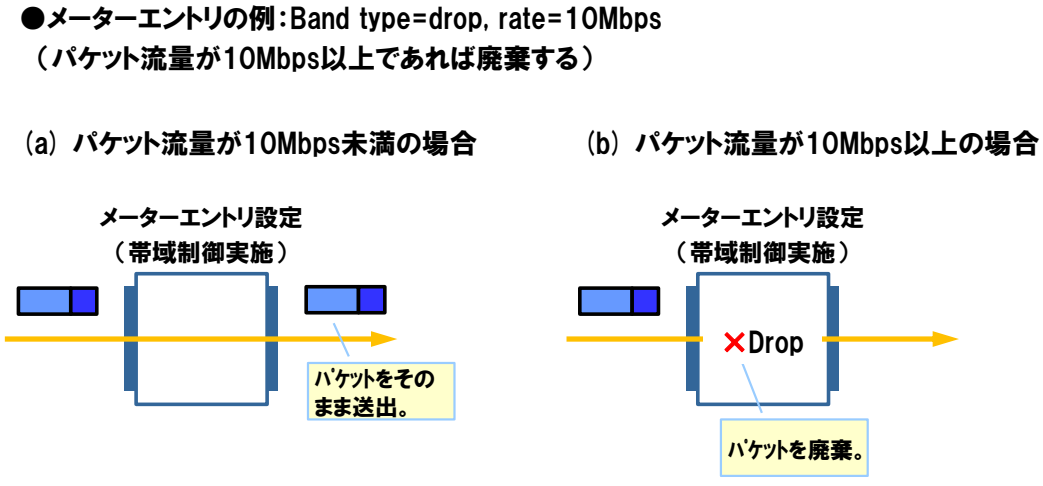


図 3-57　メーターを使用した帯域制御の例

第4編 付属資料

第1章 用語の定義

本ガイドラインで定義した主な用語について表 4-1 に整理にする。

表 4-1　用語の定義

用語	定義
SDN を用いたネットワークモデル	
仮想 NW	・ SDN NW 上に構成される L2 以上の論理ネットワーク。
SDN NW	・ SDN ノードと SDN ノード間のリンクで構成され、SDN コントローラから制御されるネットワーク。
Optical/Transport NW	・ SDN ノード間にリンクを提供するネットワーク。
フローと回線の定義	
フロー	・ リンク及び SDN ノードを通過するパケットの通り道。 ・ End-to-End のポート間に片方向で設定。
回線	・ ユーザに対してネットワークサービスを提供する単位。 ・ 1 つ以上のフローで構成。
基本回線	・ ユーザに提供する基本的な回線。
回線オプション	・ 基本回線に対して機能を追加するもの。
ユーザフローの分離と中継パス	

網内タグ	・ 複数のユーザを多重するネットワーク内で、ユーザのフローをユニークに識別するための情報。
中継パス	・ 複数の回線を集約して管理する方法。 ・ 網内タグを利用して複数の回線を効率的に転送することで、設計や運用の効率化を図る。
OAM ツールの実現例	
Continuity Check ツール	・ SDN コントローラから試験パケットを送出して、特定ノード間の疎通を確認するためのツール（CC ツールと略す)。
Loop Back ツール	・ SDN コントローラから試験パケットを送出して、故障等の被疑箇所を推定するためのツール（LB ツールと略す)。
Link Trace ツール	・ SDN コントローラから試験パケットを送出して、特定のノード間の経路が正常であることを確認するためのツール（LT ツールと略す)。

第2章 参照資料の一覧

本ガイドラインで参照している主な資料について整理する。

- O3 プロジェクト

  http://www.o3project.org/ja/index.html

- NTT 持株会社ニュースリリース

  「世界最高性能の SDN ソフトウェアスイッチをオープンソースソフトウェアとして公開」
  http://www.ntt.co.jp/news2014/1406/140606a.html

- Ryu Certification

  http://osrg.github.io/ryu/certification.html