Orchestrating a brighter world NEC

ProgrammableFlow　White Paper

2016 年 3 月 24 日

日本電気株式会社

INDEX

はじめに

ソフトウェアによってネットワークを動的に集中制御する技術の総称である SDN（Software-Defined Networking）は、現在のネットワークが抱える課題を解決し、企業の変化にも柔軟に対応できるネットワーク技術として、今注目されています。ProgrammableFlow は、SDN を実現する代表的なネットワーク技術である「OpenFlow プロトコル」※をベースにしてオープン性を確保し、NEC がこれまで培ってきた実装技術を組み合わせたネットワーク技術です。NEC は、2011 年 3 月、この ProgrammableFlow を搭載した UNIVERGE PF シリーズを、世界初の OpenFlow 対応製品として商品化しています。

NEC は、SDN の実現に加え、従来のネットワーク設計・構築・管理に内在する様々な負の制約・固定観念・課題などを解決する技術の実現を目指し、ProgrammableFlow を開発しています。NEC が ProgrammableFlow の開発で目指したものとは、高度なネットワークスキルを必要としない、誰でも簡単にネットワークの設計・構築・管理ができる技術の実現です。その実現には、次の 3 つの課題を解決する必要がありました。

① ネットワーク機器の物理配置の制約

ルータ・スイッチなどの物理的なネットワーク機器を、通信の効率化や品質担保・冗長化を考慮した配置・構成にしなければならないこと。

② ネットワークトポロジの制約

ネットワーク機器の配置構成はコア、ディストリビューション、エッジという階層構造でスイッチを並べる必要があり、バックボーン帯域を担うコア層には、将来の拡張に備えて高価な機器をはじめから導入しなければならないこと。

③ ネットワーク機器の分散管理の複雑さ

分散する物理的なネットワーク機器ごとに、設定をそれぞれ行い、様々な技術や機器の整合性を考慮して設定・運用を行わなければならないこと。

ProgrammableFlow では、これら 3 つの課題に対して、①の解決に「ネットワーク仮想化実用化技術」を、②の解決に「フロー制御実用化技術」を、③の解決に「集中制御実用化技術」を主に開発し、先に掲げた理想とする技術を実現しています。

本稿では、3 つの主要技術と、それを構成する 7 つの特徴的な機能・技術について、その動作概要とメリットを解説します。

※OpenFlow プロトコルは、2011 年に設立された OpenFlow 標準化団体の ONF（Open Networking Foundation）によって標準スペックの策定が進められており、現在 v1.5 まで仕様化されています。NEC は、この ONF に設立当初から参加し、積極的に活動しています。

ネットワーク仮想化実用化技術

1. 仮想ノード	ネットワークリソースを抽象化し、ネットワークの設定と動作確認を簡易化する技術
2. マルチテナント	1 つの物理ネットワーク上に独立したアドレス空間とポリシーを持つ複数の仮想ネットワークを構築する技術

フロー制御実用化技術

3. 分散仮想ルータ	ルータ機能を複数のスイッチで実現し、ネットワーク内のルータ設置とルーティング設計を不要にする技術
4. マルチレイヤファブリック	物理的なトポロジの制約から解放し、ネットワーク要件に応じて最適なトポロジを採用可能にする技術

集中制御実用化技術

5. 集中管理	コントローラによる集中管理で運用を簡素化し、他システムとの連携性を向上させる技術
6. 高拡張性	ハイブリッドのフロー制御方式とコントローラの高速化・階層化などにより、集中制御を大規模ネットワークへ適用可能にする技術
7. 高信頼性	コントローラとスイッチの状態整合や障害時の切り替えの高速化により高信頼な集中制御を実現する技術

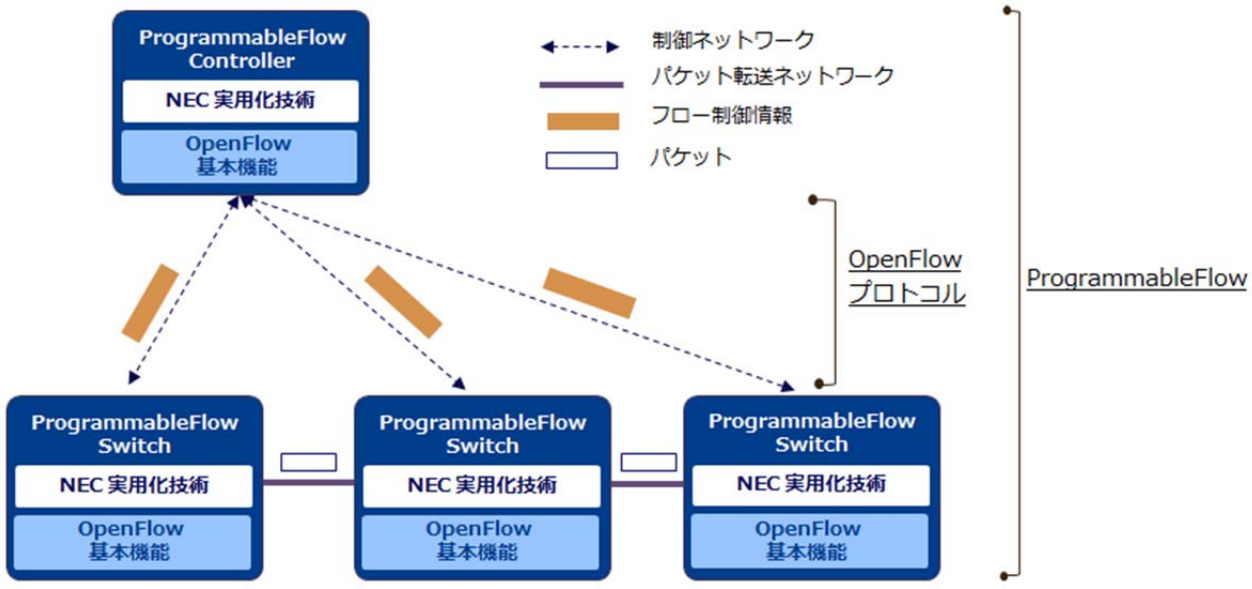
OpenFlow と ProgrammableFlow

OpenFlow は、SDN を実現する代表的な手段の 1 つで、スイッチを制御するプロトコルです。従来のネットワークは「自律分散制御」として個々のネットワーク機器が通信経路制御機能とパケット転送機能を併せ持っていました。OpenFlow は、この通信経路制御機能とパケット転送機能を分離し、あらたに制御機能として OpenFlow プロトコルを使い、コントローラがスイッチに「パケットの流れ（フロー）」の制御情報を展開するしくみで、「集中制御」を実現します。

OpenFlow では、制御対象のフローについて、OSI 参照モデルの L1～L4 まで 4 つのレイヤ※のアドレス／識別子を任意に組み合わせて細かく定義できるため、ネットワークの柔軟性が大幅に向上しています。フロー単位での制御によってネットワーク帯域を有効利用でき（マルチパス）、また、フローの片寄せも容易なため障害時などのメンテナンス性にもすぐれています。さらに、経路の途中にセキュリティデバイスを配備して、特定のフローだけを経由させること（ウェイポイント）も可能です。

ProgrammableFlow は、OpenFlow プロトコルや OpenFlow の基本機能をベースに、NEC の実装技術を結集したネットワーク技術です。この ProgrammableFlow を搭載したコントローラとスイッチが、様々なネットワークに対して、最適な SDN 環境を提供します。NEC 製品をはじめ OpenFlow をベースに開発されたネットワーク製品は、OpenFlow プロトコルに準拠することで異なるベンダー間における相互接続性を高めています。

※レイヤとはネットワークの階層をいいます。L（レイヤ）1 は物理層、L2 はデータリンク層、L3 はネットワーク層、L4 はトランスポート層に対応します。OpenFlow では L1 の物理ポート番号、L2 の MAC アドレス、L3 の IP アドレス、L4 の TCP/UDP のポート番号などのアドレス／識別子の組み合わせでフローを定義できます。

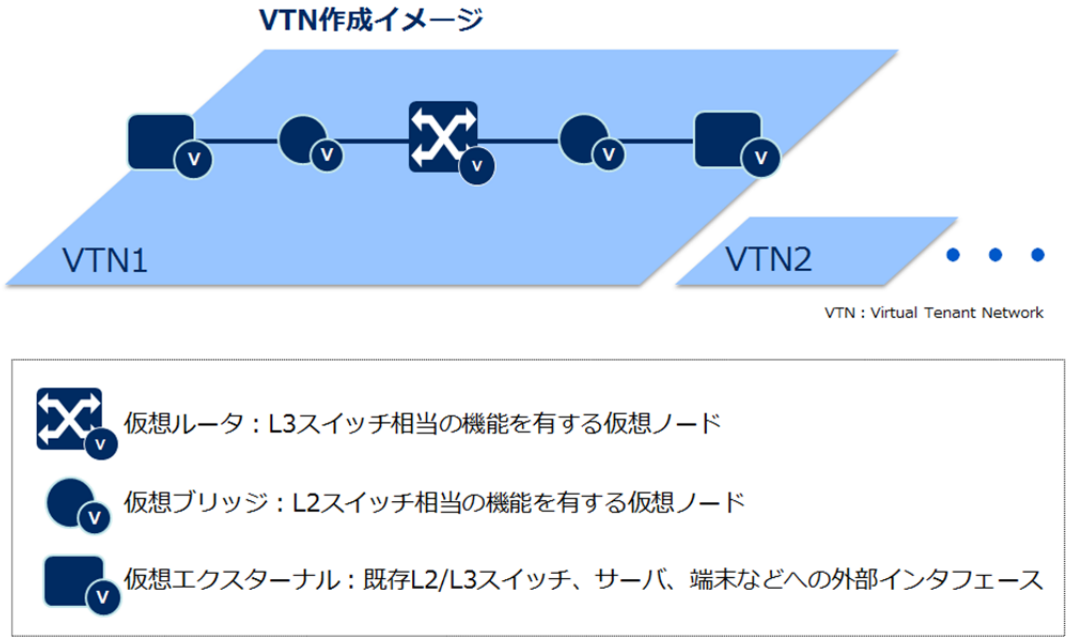


ProgrammableFlow の 7 つの機能・技術

ネットワーク仮想化実用化技術

近年、高度な市場要求に伴って、システムの高度化が進み、それに応じて多種・多様なネットワーク技術が進化してきました。それに伴い、ネットワーク機能や各種機能・設定は複雑化し、大規模なネットワーク構築や信頼性・冗長性設計においては、高度なスキルを要するようになりました。NEC は、ネットワークをシンプルかつ柔軟にすべくネットワークリソースを抽象化し、物理的な制御や設定を隠蔽化・自動化する技術としてネットワーク仮想化実用化技術を開発しました。

ProgrammableFlow のネットワーク仮想化実用化技術は、「仮想ノード」という機能でブリッジやルータのネットワークリソースを抽象化し、さらに「マルチテナント」機能により 1 つの物理ネットワークを複数の用途（テナント）で利用することができます。ProgrammableFlow は従来のネットワーク技術を統合し、柔軟かつ効率的なネットワークの運用を実現しています。

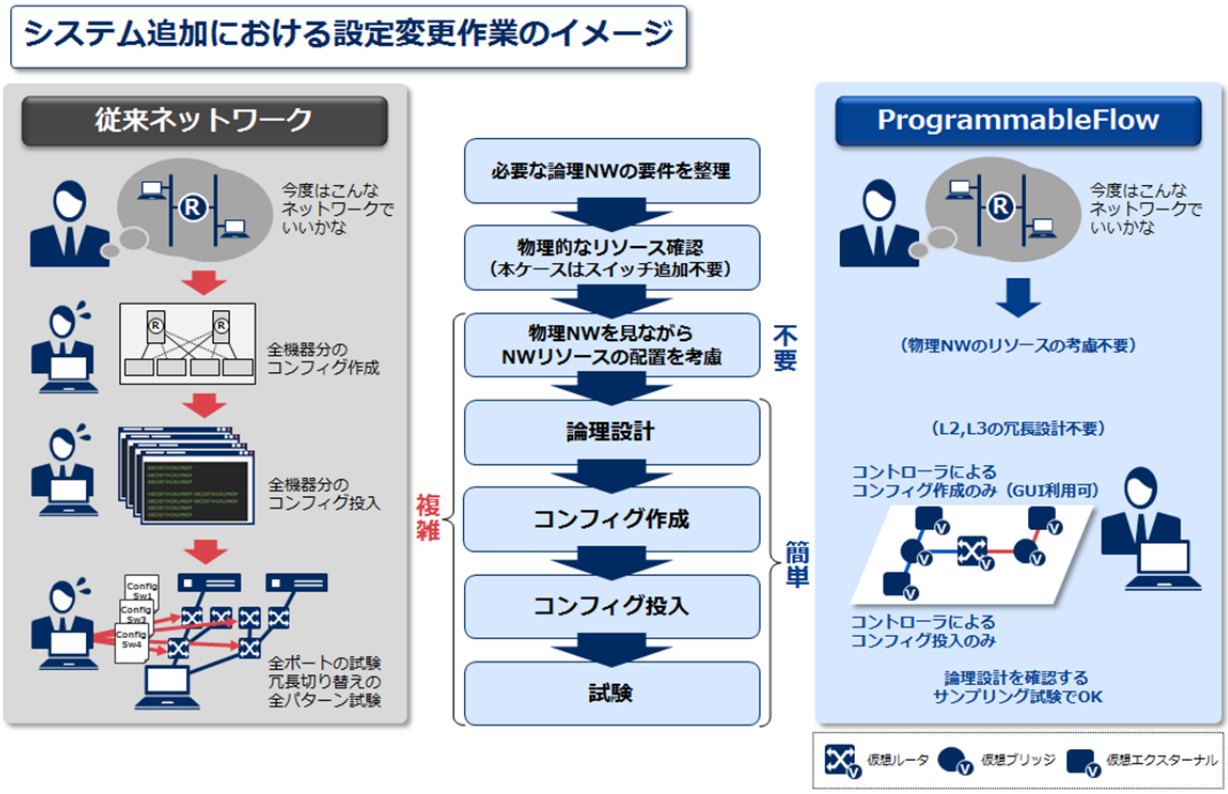


1. 仮想ノード

ProgrammableFlow は、各レイヤにおけるネットワークの機能を抽象化することで、従来必要だった冗長設計や個々の機器設定を不要とし、設定や確認作業を簡易化しています。システム運用中にネットワークの追加や変更を行う場合、これまではレイヤ 3、レイヤ 2 の論理設計を行い、その設計に基づいて個々の物理機器のルーティング、VLAN の設計・設定を行うという 2 段階の作業が必要でした。とりわけ冗長化については、各レイヤにおいて複雑な設計が必要となり、また、設定変更終了後も個々の機器の設定内容から動作まで、矛盾なくその完全性・統一性を確認する必要があり、その作業は高度な技術を持つ SE が実施する必要がありました。

これに対して ProgrammableFlow では、「仮想ノード」という機能を用いて、ブリッジやルータのネットワーク機能を抽象化することで、ネットワークの追加作業を容易にしています。追加するネットワークの論理設計としては仮想ルータ、仮想ブリッジの設計・設定を行うだけで、個々の機器の設計や設定を意識する必要がありません。また、フローベースルーティング機能※が障害時に最適な経路の再計算を自動で実施するので、論理設計で冗長化に対する考慮は不要になります。さらに、最適な経路に基づき確実にフローが登録されるので、確認試験においては論理設計の設定に関するサンプリング試験をするだけでよく、作業工数を軽減することにもつながります。

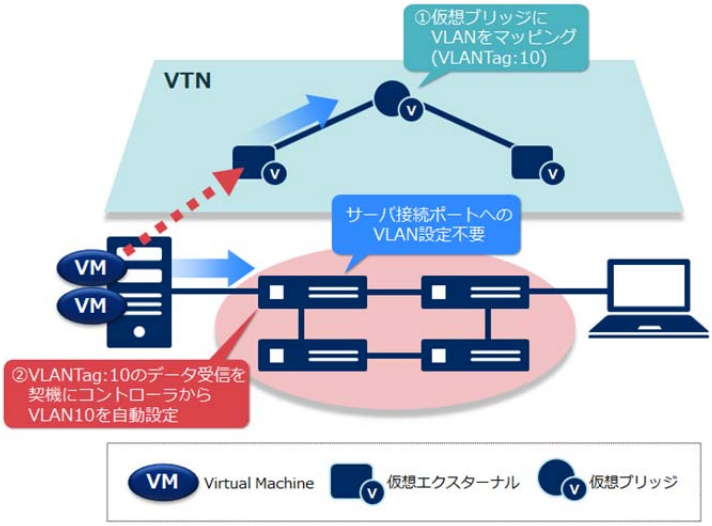
※フローベースルーティングとは L1/L2/L3/L4 の情報でフローを識別し、フローテーブルに従ってフロー単位でパケットを転送する機能です。各スイッチ内には、コントローラによって生成された最適なフロー情報が、フローテーブル上に格納されています。このフローテーブルは、仮想ルータの機能によって、1 台のスイッチで L1～L4 処理を実現します。また、シャーシスイッチなどの特定装置を経由することなく、すべてのエッジスイッチが L3 ルーティングを実現します。



ProgrammableFlow におけるネットワーク抽象化は、従来のネットワーク機能であるブリッジやルータを踏襲しているため、従来製品や従来技術から ProgrammableFlow への移行もスムーズに行うことができます。

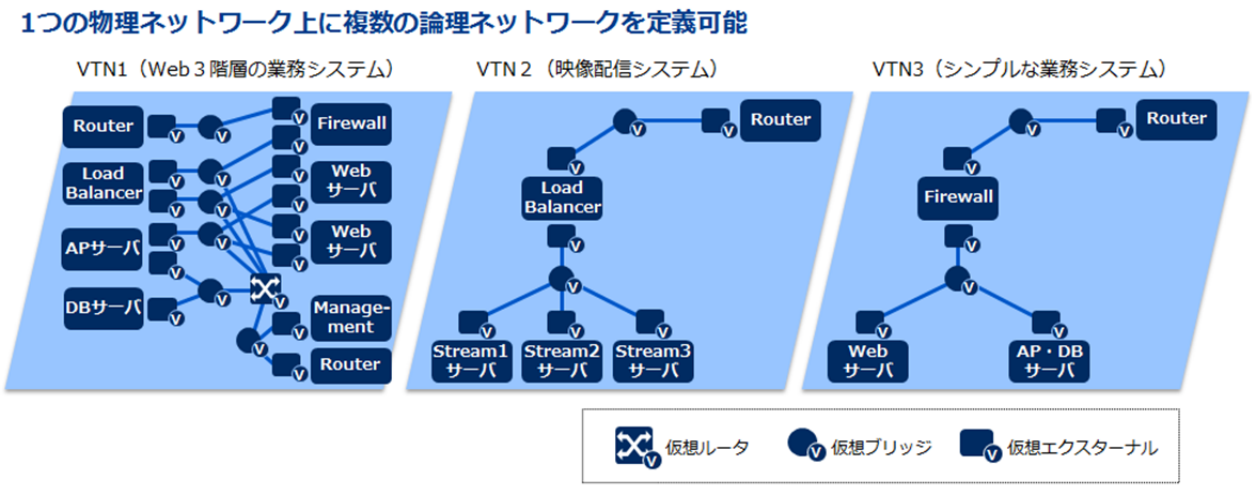
従来のネットワークの運用作業は高度なスキルを持つ特定の人やベンダーに依存していましたが、ProgrammableFlow は IT 技術者のような非ネットワーク技術者でも理解が簡単で扱いやすく、運用作業をお客様自ら実施することが可能です。

仮想ノードには、自動的に物理ポートと仮想ブリッジをマッピング（関連付け）する機能を実装しています。これはスイッチが、受け取ったパケットの VLAN TAG をみて、自動的にどの仮想ブリッジで取り扱われるべきかを判断するもので、従来のスイッチのような物理ポートへの VLAN 設定作業が不要になり、ネットワーク管理者の管理業務を省力化します。



2. マルチテナント

従来は、サーバ仮想化技術を使ってサーバ集約する際、ネットワークの仮想化・集約が困難だったため、業務システムごとに物理的に独立したネットワークを構築していました。これに対して ProgrammableFlow では、1 つの物理ネットワーク上に複数の用途（テナント）の仮想ネットワークを構築することができます。これを「マルチテナント」機能といい、それぞれの用途に応じた仮想ネットワークを VTN（Virtual Tenant Network）と呼んでいます。VTN では、アドレス空間やルーティング、QoS（Quality of Service）、パス制御、監視、管理者権限など独立したポリシーを持つ仮想ネットワークを個別に定義できます。マルチテナントを利用することで、物理的に独立した複数のネットワークを簡単かつセキュアに統合し、ネットワーク機器やメンテナンスにかかるコストを抑制することが可能となります。さらに、例えば、Web3 階層の業務システムを構築する場合、従来はシステムごとに複数の VLAN と、それらをまとめるルータが必要でしたが、ProgrammableFlow では 1 つの VTN 上に 3 階層のシステムを構築し、簡単に管理することが可能です。



従来ネットワーク技術と ProgrammableFlow の違い

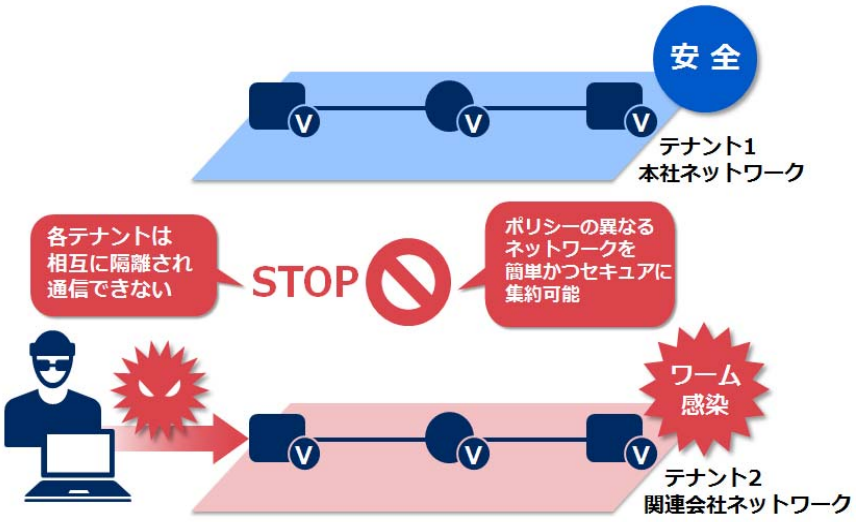
従来ネットワークでも仮想ルータや VLAN というようなネットワーク仮想化技術は存在しましたが、各レイヤにおいて個別の技術を組み合わせる必要があり、SE が全体の統一性を考慮しながら設計する必要がありました。そのため、ネットワーク構成が複雑になると、設計が複雑になりヒューマンエラーによる障害リスクが増し、システム追加の要求に対して迅速にネットワークを変更することが困難でした。ProgrammableFlow では、冗長性を自動化し、シンプルで統合的なモデルに抽象化できる点が大きな違いとなっています。

従来技術と ProgrammableFlow の対比

		従来技術	ProgrammableFlow
マルチテナント機能		なし	VTN
レイヤ 3	仮想化技術	仮想ルータ（VRF など）	仮想ルータ （冗長化は自動）
	冗長化技術	VRRP、ダイナミックルーティング （OSPF、BGP など）	
レイヤ 2	仮想化技術	VLAN、MPLS	仮想ブリッジ （冗長化は自動）
	冗長化技術	STP、LAG、スタック技術など	

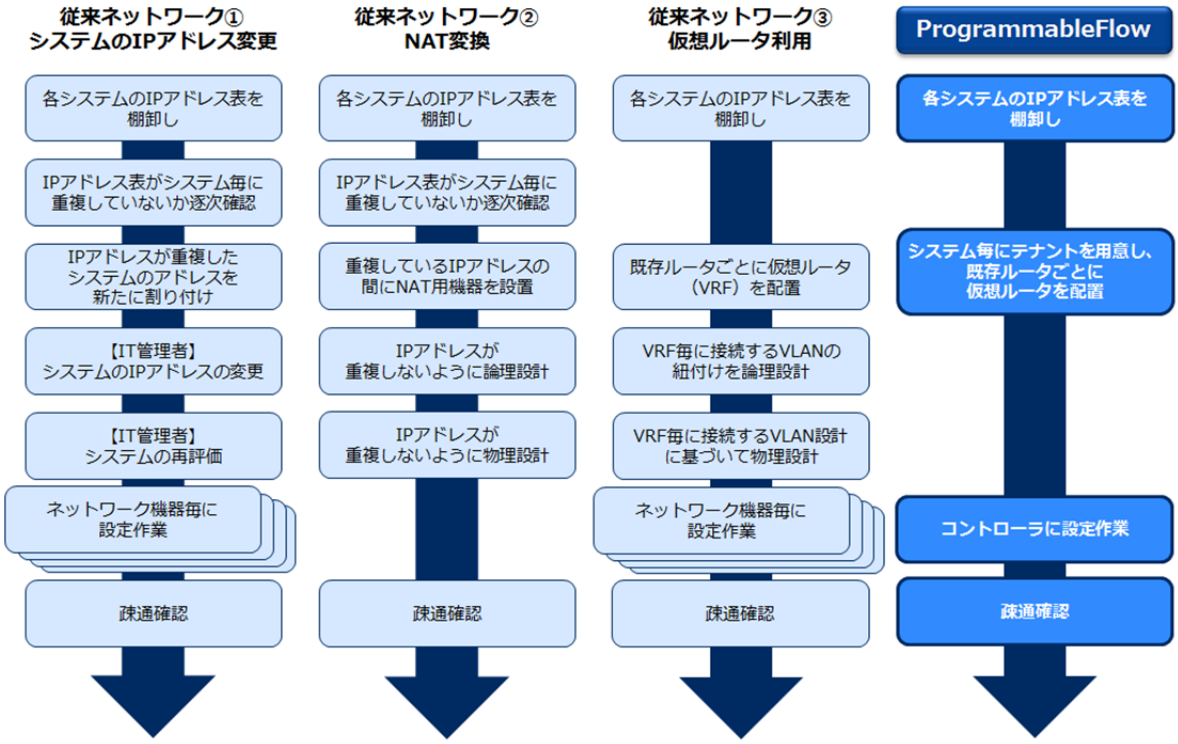
ネットワーク仮想化実用化技術のユースケース

ユースケース 1：複数のテナントをセキュアに分離



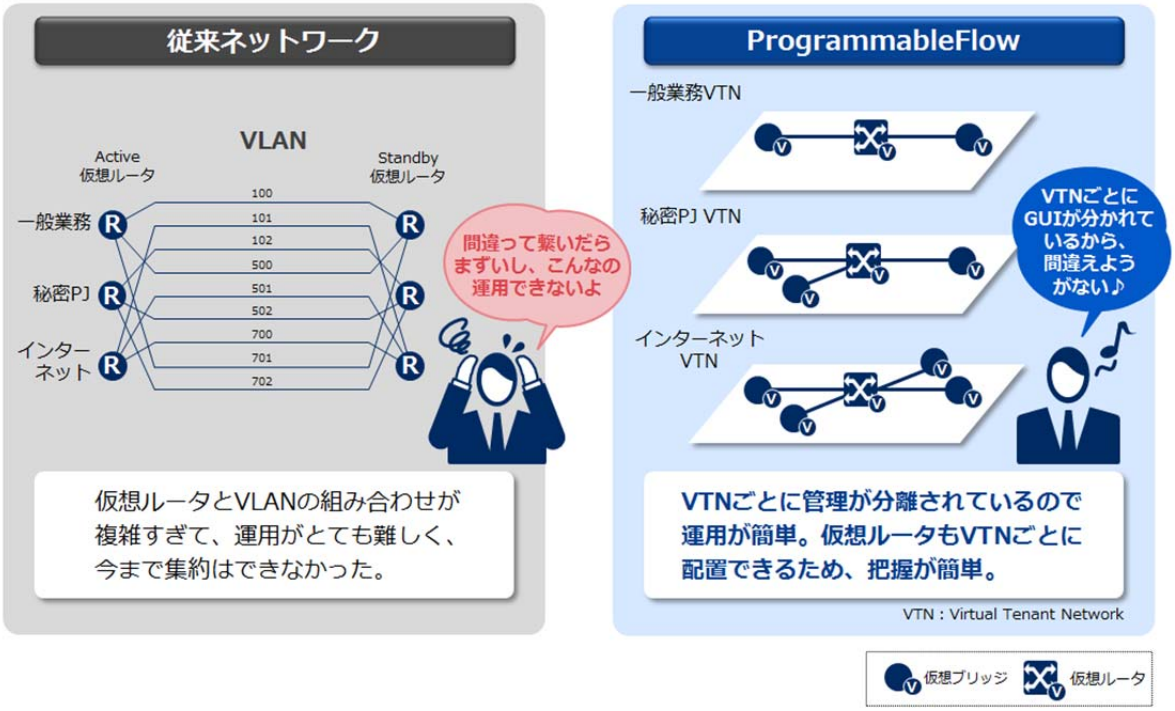
VTN は相互に隔離され、VTN 間の通信はできません。そのため、セキュアにかつ簡単にネットワークの集約が可能になります。例えば複数の顧客のネットワークを集約するケースにおいて、一方のネットワークからのワーム感染なども、VTN を利用して感染したネットワークを隔離することで相互の侵入を遮断し、セキュリティを確保できます。

ユースケース 2：システムの IP アドレスが重複するネットワークを集約



複数の業務システムのネットワークを集約する場合では、システムの IP アドレスが重複するケースがあります。こうした場合、従来のネットワーク技術では、どちらかのシステムの IP アドレスを変更するか、NAT（アドレス変換）を用いて重複を解消する必要があり、いずれにしてもシステム移行作業が複雑になりました。ProgrammableFlow では各システムを VTN に分けて収容することができるため、相互に独立した VTN によってアドレス空間を分離して、IP アドレスが重複したシステムの統合も簡単に実現することができます。

ユースケース 3：ルータが存在するネットワークの集約



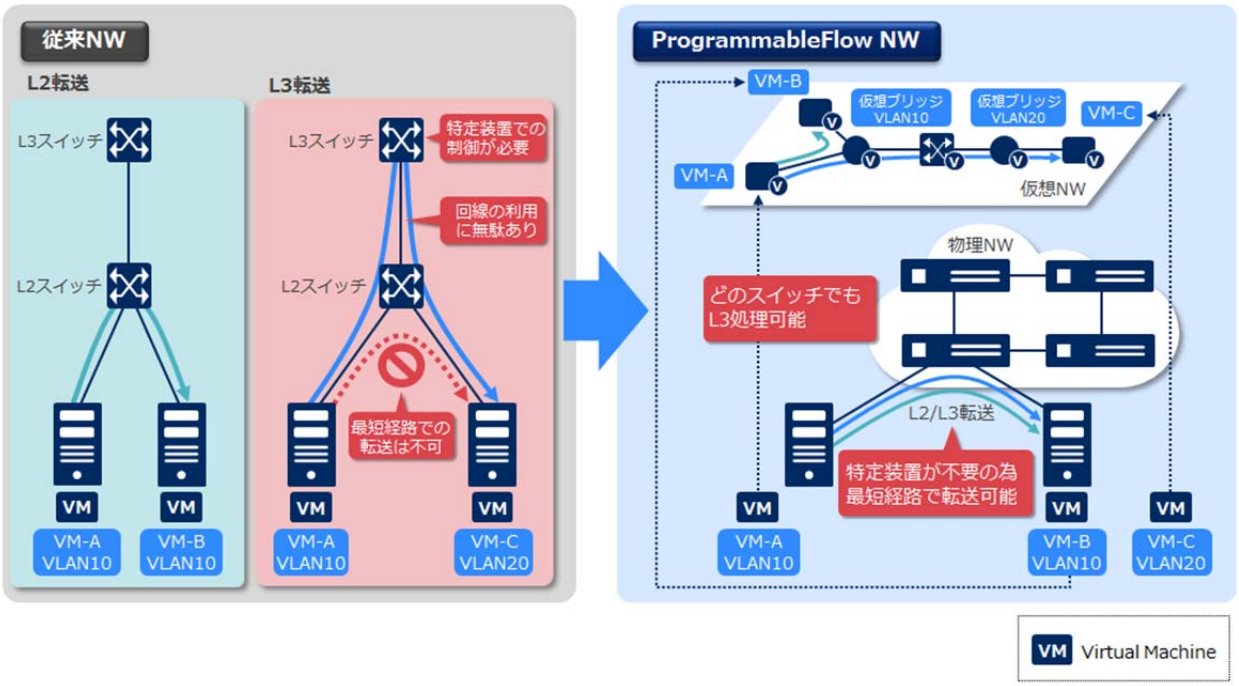
集約対象のネットワークにルータが存在する場合、仮想ルータを利用することができます。この場合、従来のネットワーク技術では、仮想ルータとそれに接続される VLAN を設計し、冗長性を考慮した上で、個々の機器の設計や設定を行う必要があります。具体的には、どの業務システムがどの仮想ルータを使用し、どの VLAN がどの仮想ルータに接続されているか、また接続してはいけない仮想ルータ間が接続していないかなど、留意点も多く、複雑な設計が必要となります。さらに、仮想ルータの数が多い場合には、不具合時の調査などネットワーク管理がとても煩雑になり、集約をあきらめるケースもありました。

これに対して ProgrammableFlow では、システムごとに VTN を割り付け、VTN ごとに仮想ルータや仮想ブリッジを作成することができるため、シンプルなネットワーク設計が可能です。また、どの業務システムがどの仮想ルータ、どの仮想ブリッジを使用しているかについても、CLI（Command Line Interface）や GUI（Graphical User Interface）を使って簡単に確認することができます。

フロー制御実用化技術

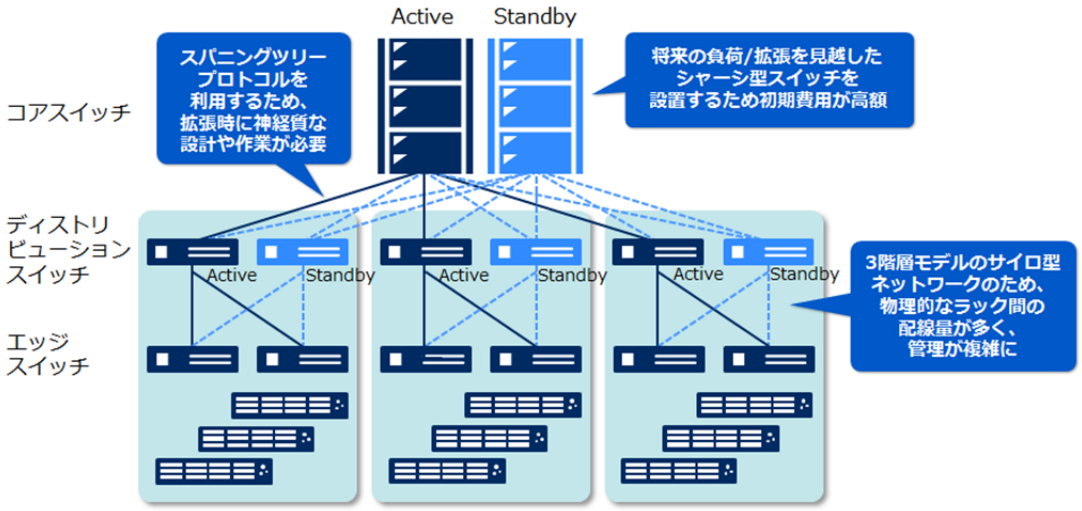
3. 分散仮想ルータ

ルータにはサブネットを分割するという機能がありますが、これはパケットがルータを超えるときに MAC アドレスの書き換えを行うという処理で実現されます。従来、このルータのサブネット分割機能を利用するには、トラフィックが集中する L3 スイッチに大きな負荷がかかるため、高価な L3 スイッチを配置する必要がありました。これに対して ProgrammableFlow は、フローに従った動作（アクション）として、パケットが到達した最初のスイッチで MAC アドレスの書き換えを実施します。これを「分散仮想ルータ」技術と呼び、複数のスイッチで、同じ組み合わせのサブネットをまたぐことができるようにするものです。これによって物理的な複数のルータを設置する必要が無くなり、ネットワーク内のルーティング設計がいらない、シンプルな運用を実現できます。



4. マルチレイヤファブリック

従来のネットワークでは、サブネットをまたぐトラフィックがコアスイッチに集中し、ボトルネックが発生する可能性がありました。そのため、ネットワークの中心にあるコアスイッチにあらかじめスケールアップを想定した高価な L3 スイッチを設置し、ツリー型（サイロ型）のトポロジを構成していました。

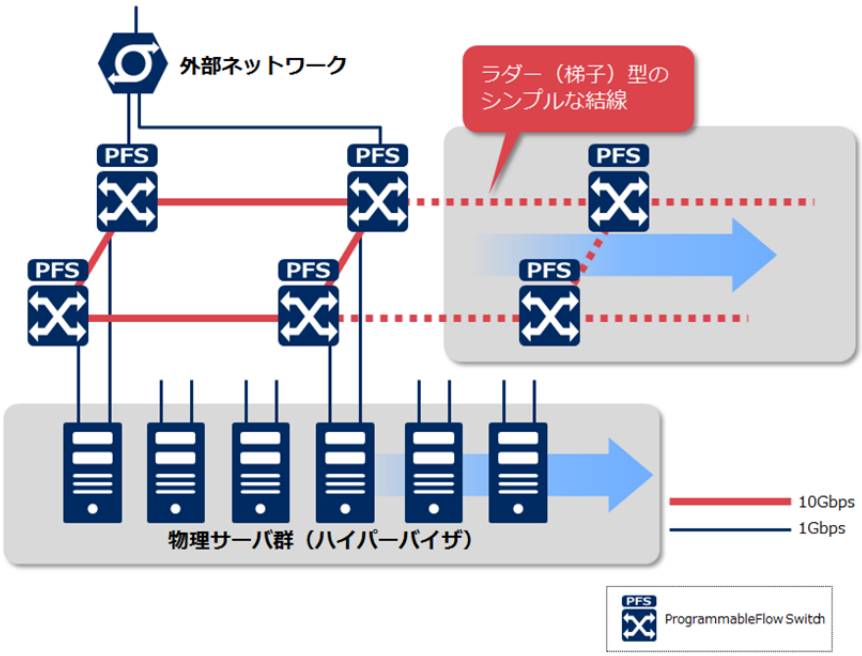


また、スタック技術を利用するケースもありますが、接続できるスイッチの台数が 10 台程度という規模の制限に加え、拡張時にはネットワークの停止を伴うため、拡張しにくいという問題がありました。

これに対して ProgrammableFlow では「分散仮想ルータ」技術によって、従来のネットワークのように、サブネットをまたぐトラフィックがコアスイッチに集中してボトルネックが発生することがありません。そのため、ツリー型のトポロジを構成する必要もなく、特定の物理的なトポロジに制約されない柔軟なネットワーク構成を組むことが可能です。その結果、帯域や耐障害性、物理的な制約などの要件に応じた最適なトポロジの採用や複数のトポロジを組み合わせやスケールアウト型のネットワーク構成も容易になりました。従来から、レイヤ 2 のトラフィックを制御するファブリック技術はありましたが、NEC はレイヤ 3 のトラフィックも柔軟に制御するマルチレイヤファブリックの技術を実現しました。

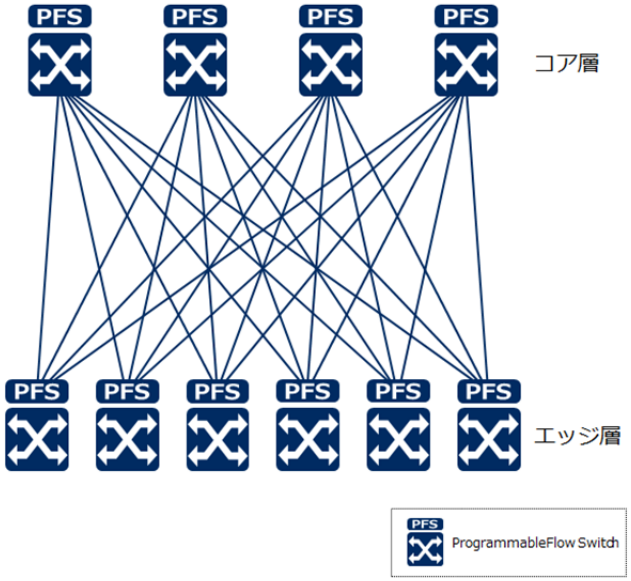
フロー制御実用化技術のユースケース

ユースケース１：スケールアウト型ネットワークの構築



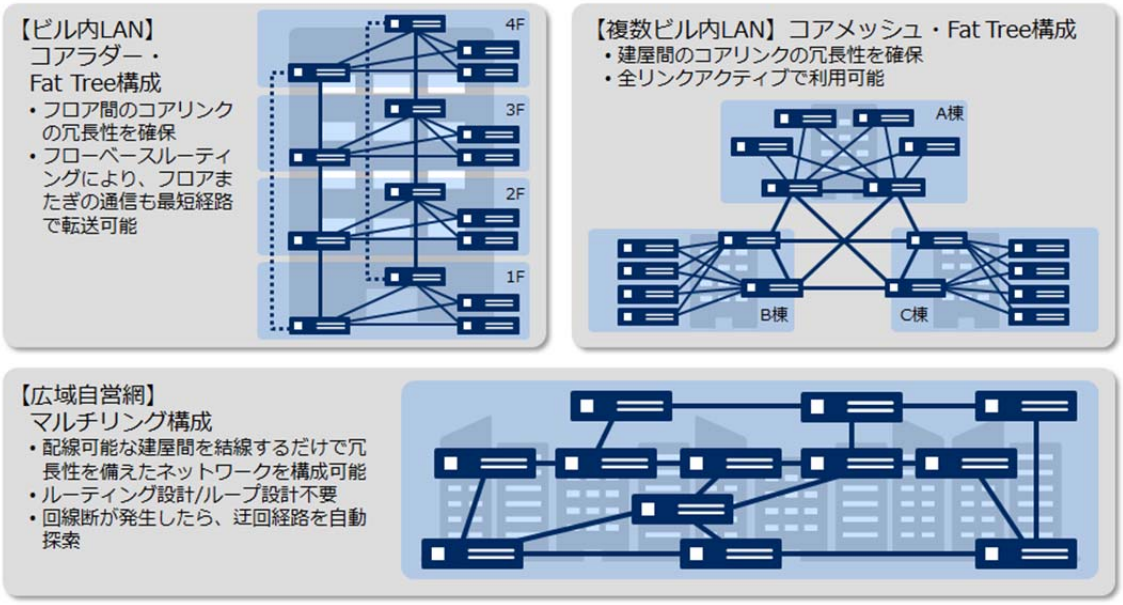
データセンターの移設やシステム統合において、ネットワークをスケールアウト型で構成することにより、初期費を抑制し、システムの拡大に合わせてネットワークを柔軟に拡張することができます。比較的小規模な仮想化基盤のネットワークにおいて用いられるラダー型のトポロジは、スケールアウト型のシンプルなネットワーク構成を実現できる上、機器間の煩雑な接続ケーブルの削減にもつながります。

ユースケース 2：信頼性向上のためのシステム 4 重化



販売システムなど、システムダウンがそのまま売上に直結するようなシステムにおいては、ダウンタイムを抑制できるネットワークの構築が求められます。ProgrammableFlow では、従来のネットワーク技術ではできなかったシステム 4 重化のネットワーク構成も実現できるため、システム可用性を飛躍的に向上させることができます。

ユースケース 3：柔軟なネットワーク運用



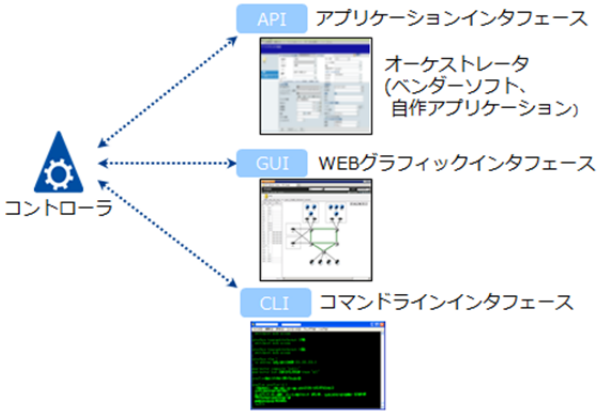
複数のフロアにまたがるデータセンターや、複数の棟を持つ工場や大学キャンパスなどでは、将来的なネットワークの需要に合わせて、ループを段階的に追加した柔軟な拡張が可能です。

集中制御実用化技術

5. 集中管理

ProgrammableFlow を搭載するコントローラは、ユーザインタフェースとして CLI、GUI、API（Application Programming Interface）の 3 種類を提供します。GUI では、コントローラが制御対象としているネットワークおよび機器の状態を視覚的にかつリアルタイムに把握することができ、操作性と併せてネットワーク管理者に安心感を与えています。

ProgrammableFlow は、個々のスイッチに対する設定情報が少なく、ユーザインタフェースも、従来のネットワークのユーザインタフェースと比較して簡単な作りになっています。これによって設定や変更作業のミスは大幅に削減され、ネットワーク設定作業者の負荷も軽減されます。さらに API を利用したネットワーク制御のアプリケーションを開発するときにも、物理的な構成を意識することなく、また、個々のスイッチに設定を投入する必要もなく、アプリケーション開発を実現できます。従来型ネットワークのアプリケーション開発と比較してコードも短くなり、保守性も高く、部品化や、アプリケーションの再利用がしやすいことも大きな特長です。



6. 高拡張性

OpenFlow は通信経路制御とパケット転送を分離した技術ですが、NEC は OpenFlow 登場前からこうした技術に取り組み、以前から多くの実装技術を持っていました。これまで培ってきた高拡張性のための実装技術を応用した ProgrammableFlow は、コントローラへの負荷を軽減、大規模ネットワークでの利用を可能にしています。

OpenFlow では、事前に通信のフローを設定しておく「プロアクティブ型」と、発生した通信に対して都度フローを設定する「リアクティブ型」の 2 つのフロー制御方式を定義しています。リアクティブ型はプロアクティブ型に比較して、細かな通信経路制御が可能な反面、コントローラの負荷が高く、小規模ネットワークでしか利用できないという制約がありました。ProgrammableFlow では、プロアクティブ型を基本として、リアクティブ型をハイブリッドで利用することにより、細かな通信経路制御を実現しながら、大規模ネットワークへの適用を可能にしています。

さらに、ProgrammableFlow では、フロー制御情報のデータベース（FlowTable）をスイッチのメモリ上に実装することで、通信処理を高速化しています。またコントローラ側で個別に処理するのが一般的なブロードキャスト・マルチキャストパケットについても、転送経路をスイッチに静的に設定することで、スイッチからコントローラへの問い合わせを省き、コントローラの負荷を軽減しています。こうした高速化処理、負荷軽減によって、1 式のコントローラで数百台のスイッチを制御することを可能にしています。

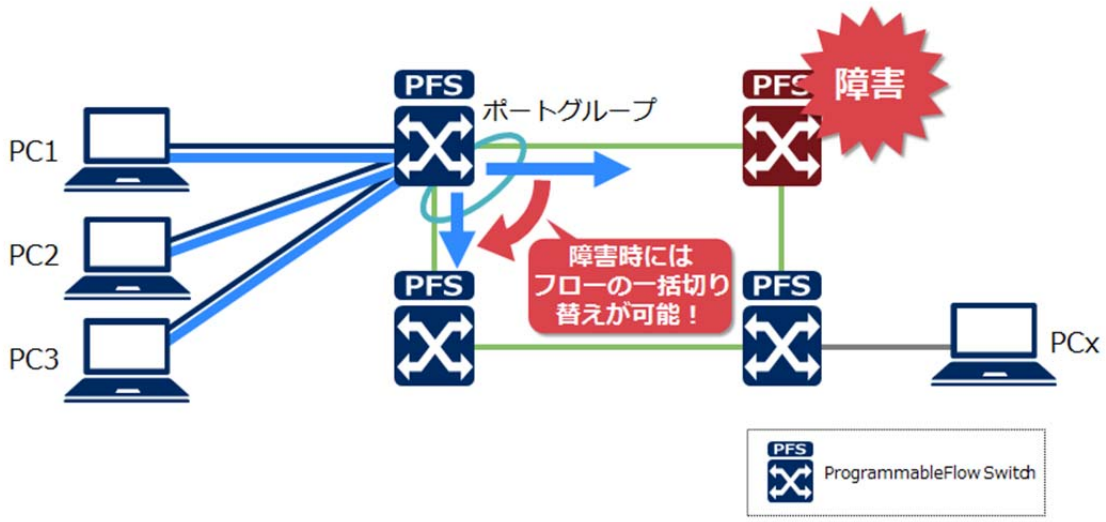
ProgrammableFlow では、大規模ネットワークの制御のため、コントローラを階層化することができます。複数のコントローラにまたがる VTN を 1 つの VTN として管理することで、VTN に関する設定を集中管理し、従来のネットワーク技術ではできなかった大規模なネットワークの統合管理を実現します。

7. 高信頼性

ProgrammableFlow は、通信をフローとして登録するときに、対象のフローがコントローラとスイッチの間で不一致とならないよう、都度確実に登録されたかを確認します。さらにすべての通信について定期的に最適経路の再計算を行うことで、通信の確実性を向上させています。

OpenFlow を用いたネットワークでは、障害時にコントローラで経路の再計算を行うため、パスの切り替えに時間がかかることがあります。ProgrammableFlow では、「ポートグループ」※という NEC の実用化技術によって、コントローラへの問い合わせや経路の再計算、フロー再設定などの手間と時間を省略し、スイッチ側で瞬時にフローの切り替えを可能としています。さらにコントローラの信頼性を高めるために、通信キャリアなどで実績のある高速なメモリ同期技術を採用しています。これによってコントローラはクラスタ化され、コントローラ障害時には、スタンバイのコントローラに高速に自動で切り替えが行われます。こうして障害時にも高い信頼性を実現する ProgrammableFlow は、高いネットワーク品質を実現します。

※ポートグループとは障害発生時の経路切り替えを高速化するためのしくみです。OpenFlow1.0 では、経路の切り替えはコントローラがフローエントリを一つ一つ書き換えることで行いますが、NEC のポートグループ機能は OpenFlow1.3 の「グループテーブル」を利用してスイッチが自律的に一括して経路を切り替えることを実現します。



おわりに

ここで紹介した ProgrammableFlow 技術は、現在(2016 年 3 月)で、国内外で 250 社以上のお客様で実証システム・商用システムに導入いただき、その効果を認めていただいております。また、NEC は、保有する SDN 最先端技術・先行する IT・ネットワーク技術の実績に基づいて開発した NEC SDN Solutions を通じて、柔軟かつシンプルな ICT ソリューションを提供しています。この ICT ソリューションの提供を通じてお客様のビジネスをより素早く柔軟にし、事業拡大や新ビジネスの創出をご支援させていただきます。

お問い合わせは、下記へ

NEC SDN 戦略本部

〒108-8001東京都港区芝5丁目7-1（NEC本社ビル）
E-mail： inquiry@sdn.jp.nec.com
※貴社にお伺している NEC の営業・SE の者にお声がけいただいてもかまいません。