SDN JAPAN 2012 プログラム(2日目)
テーマ：技術者・研究者から見たSDN/OpenFlow

Empowered by Innovation NEC

OpenFlowを用いたファブリック製品の実装例とクラウドマネージャの連携について

2012年12月7日

NEC
宮永 直樹

アジェンダ

- NECのSDNへの取り組み
- OpenFlowファブリックと他のファブリック方式との違い
- IaaS・仮想化基盤の運用を自動化するSDNソリューション

本セッションのフォーカス

- OpenFlowを利用した実装例を機能ベースでご紹介
  今後のOpenFlow製品の採用やSDNの実装のご参考に
- 現在のNECのOpenFlow製品はHop By Hop型
  →Hop By Hop型を中心としたユースケースのディスカッション
  ※今後Overlay方式にも対応予定あり
- 製品紹介や具体的なユーザメリットなどは本セッションでは割愛

【ご参考】

日本通運株式会社様
http://www.nec.co.jp/library/jirei/nittsu/contents.html

金沢大学付属病院様
http://jpn.nec.com/case/kanazawa/index.html

NECのSDNへの取り組み

NECの考えるSDN

ネットワークをソフトウェアでプログラマブルにすること、およびそのアーキテクチャ

これまで

- ネットワーク制御と通信処理が一体となった専用ネットワーク機器
- 個別のネットワークニーズに対応した専用機器を用いた垂直統合型のネットワークシステム

これから

- ネットワーク制御をソフトウェアで行うことにより、通信処理と分離
- ネットワークをサーバやストレージと同様に自在に制御し、システム変更に柔軟に対応

NECのOpenFlowへの取り組み

NECのOpenFlowへの取り組み

- 2007年、スタンフォード大学と共同研究を開始
- 2008年、コンソーシアム発足
- 2011年、Open Networking Foundation発足
- 2011年4月、世界で初の商用製品を販売開始

NECは標準化、および製品実装においてリード

UNIVERGE PFシリーズ

ProgrammableFlow

コントローラ

UNIVERGE PF6800

スイッチ

UNIVERGE PF5240

UNIVERGE PF5820

1年半でワールドワイドでキャリア様、DC事業者様、企業様で採用

今、「OpenFlow製品」できること/できないこと

おもにデータセンターネットワークむけに製品提供を開始

- IaaS基盤・仮想化基盤
- データセンターネットワーク
  仮想化されていないサーバの接続スイッチなど
- 企業LAN

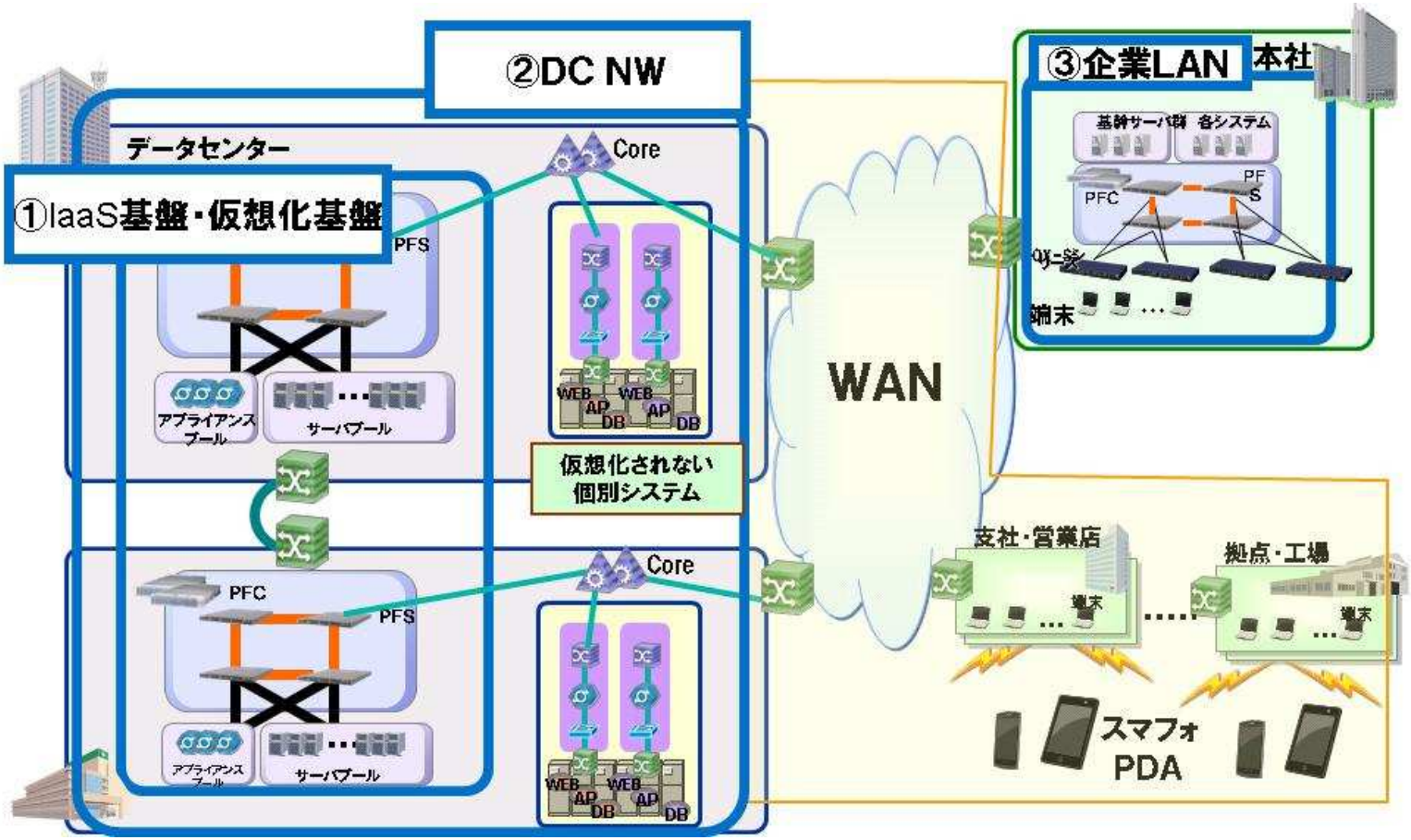
→本日は「OpenFlowファブリック」と呼ぶことにします。

現在の非適用領域(今後のR&D分野)

- DC間バックボーン
- 企業WAN
- モバイル端末
- キャリアのバックボーン

現時点のNECのOpenFlow製品の適用領域

IaaS基盤およびDCネットワーク、企業LAN向けに対し適用可能

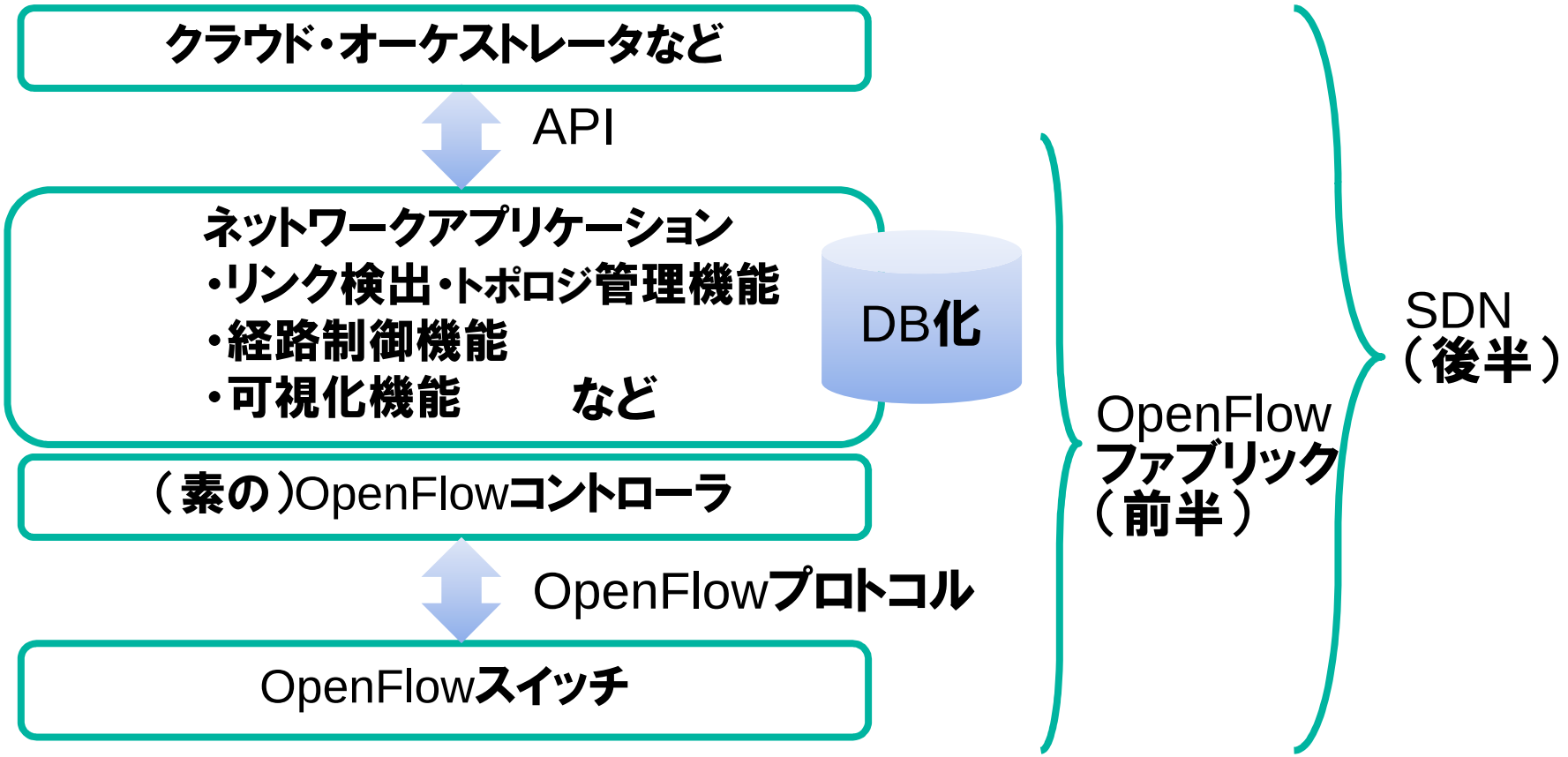


NECのOpenFlowファブリックと他のファブリック方式との違い

OpenFlowファブリックのイメージ

OpenFlowファブリック

- ネットワークアプリケーションを最初からバンドルした製品
- ユーザがOpenFlowのプログラムをする必要はない（隠蔽化）



データーセンターむけファブリック製品の主な特徴

マルチパス

- スパーニングツリーを使用しないこと
- 経路制御はTrillが一般的
- ECMP(Equal Cost Multi Path)の場合には複数経路を利用

集中管理

- １台のスイッチのように扱えること(MCLAG的な)
- 設定の集中管理(１台に設定を入れると他にも反映)
  - すべてのベンダで実現されているわけではない

基本的にL2SW

- L3機能・仮想ルータ機能を持つ製品もある

１管理単位のスイッチ台数:100台～200台程度

OpenFlowファブリックの特徴

マルチパス

- OpenFlowを採用。
- Shortest Path(デフォルト)の経路アルゴリズムにより「オートマ」化
- ECMP(Equal Cost Multi Path)の場合には複数経路を利用
- さらにOpenFlowによるポリシーの適用が可能

集中管理

- 1台のスイッチのように扱えること(MCLAG的な)
- 設定の集中管理(コントローラに設定を入れると全SWに反映)
- 経路制御の集中管理・DB化

L3/FW/LBも含めてグループ化、テナントという概念を導入

- VTN※としてデータベース化しているところが一番の特徴

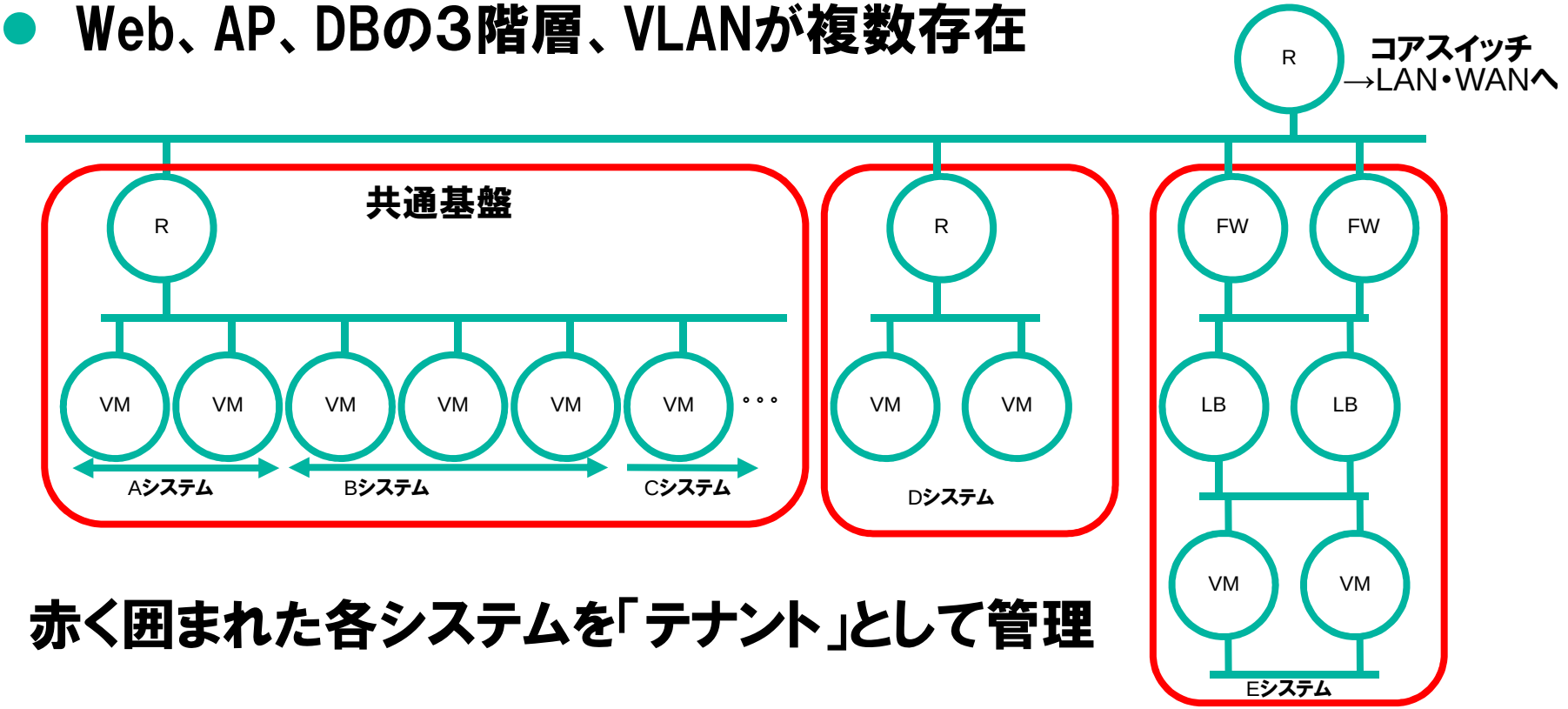
1管理単位のスイッチ台数:100台～200台程度

VTN:Virtual Tenant Network

VTNのイメージ(１)

プライベートクラウドでみられるような「システム」を想定

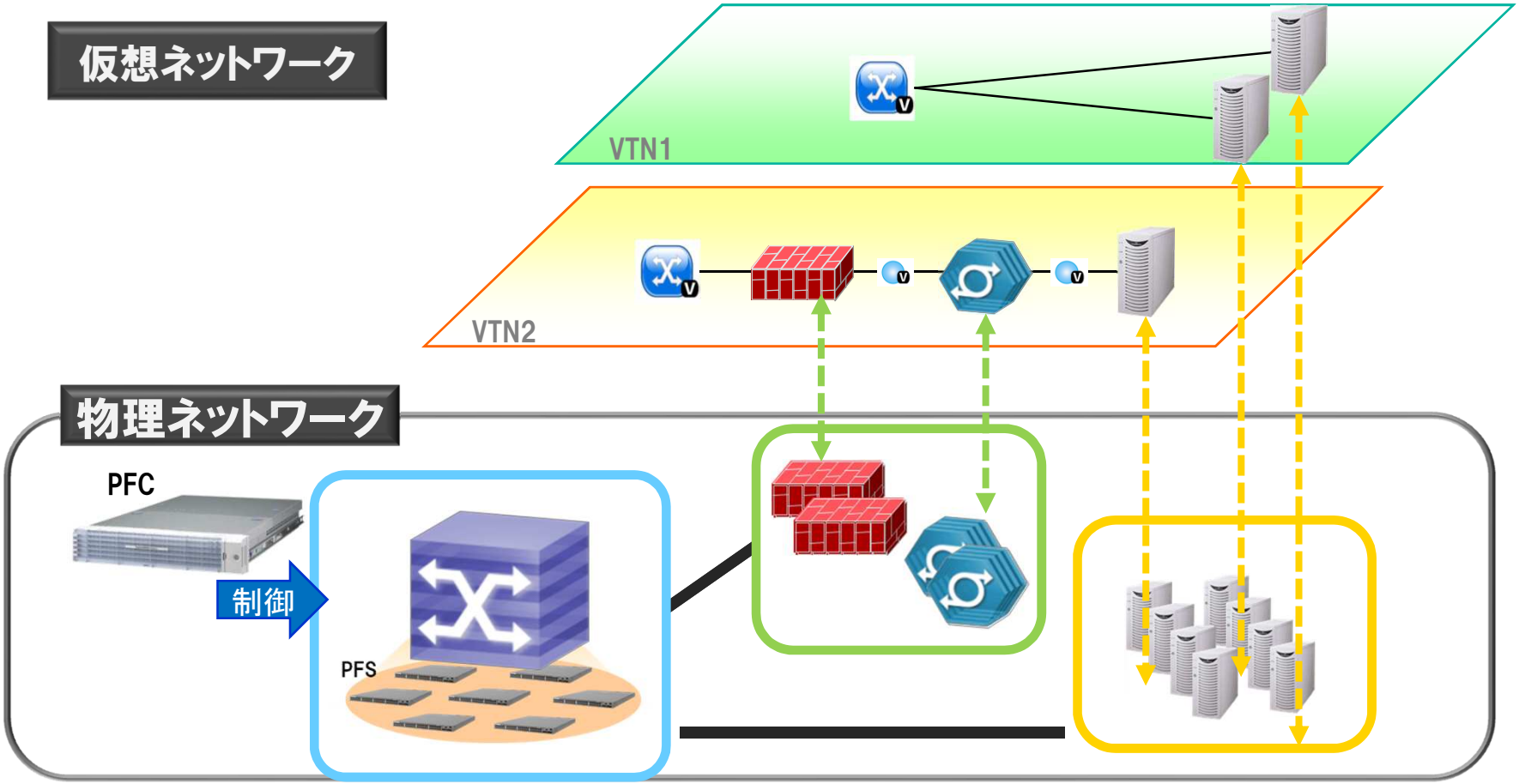
- アドレスが個別に割り当てられたシステム
- Firewall、Load Balancer、ルータが存在
- Web、AP、DBの3階層、VLANが複数存在



赤く囲まれた各システムを「テナント」として管理

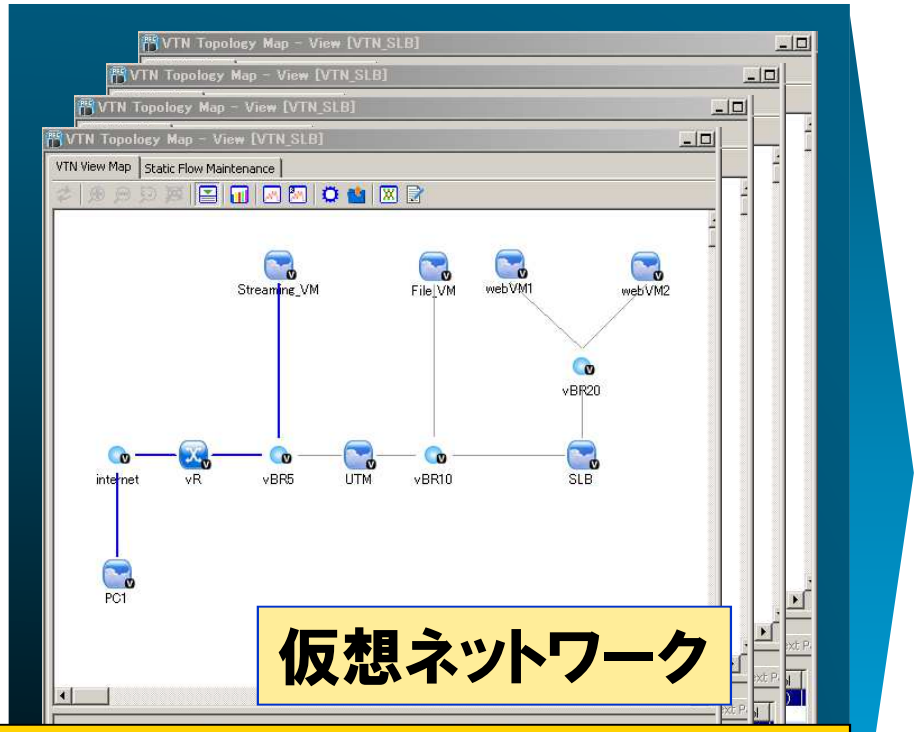
VTNのイメージ（２）

- システムごとのネットワークを「テナント」として仮想化
  サーバ仮想化のGuestOSのようなもの
- サーバ仮想化のように機器の点数・機器費用を削減

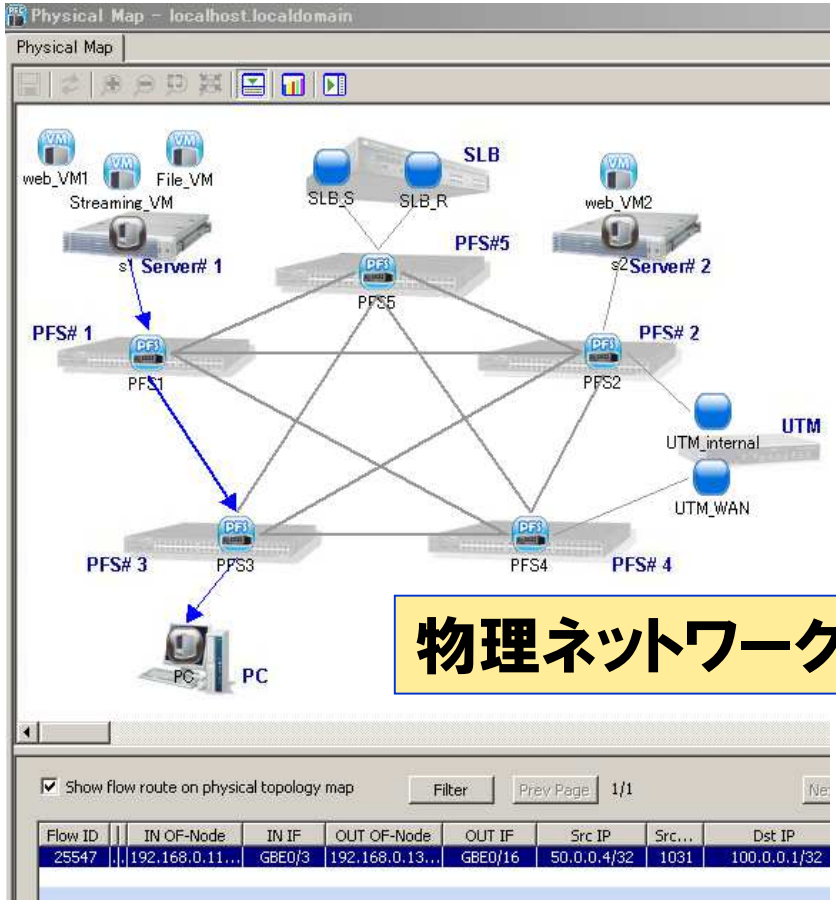


VTNのイメージ（３）

テナントごとに仮想ネットワークを作成、DB化される
仮想ネットワークはGUI・API・CLIで設定する
FW/LBは非OpenFlow対応だが、仮想FW,仮想LB機能を持つもの



仮想ネットワーク



物理ネットワーク

L2機能だけでなく、プライベートクラウドで利用されているL3機能や外部のFW/LBなどもグループ化

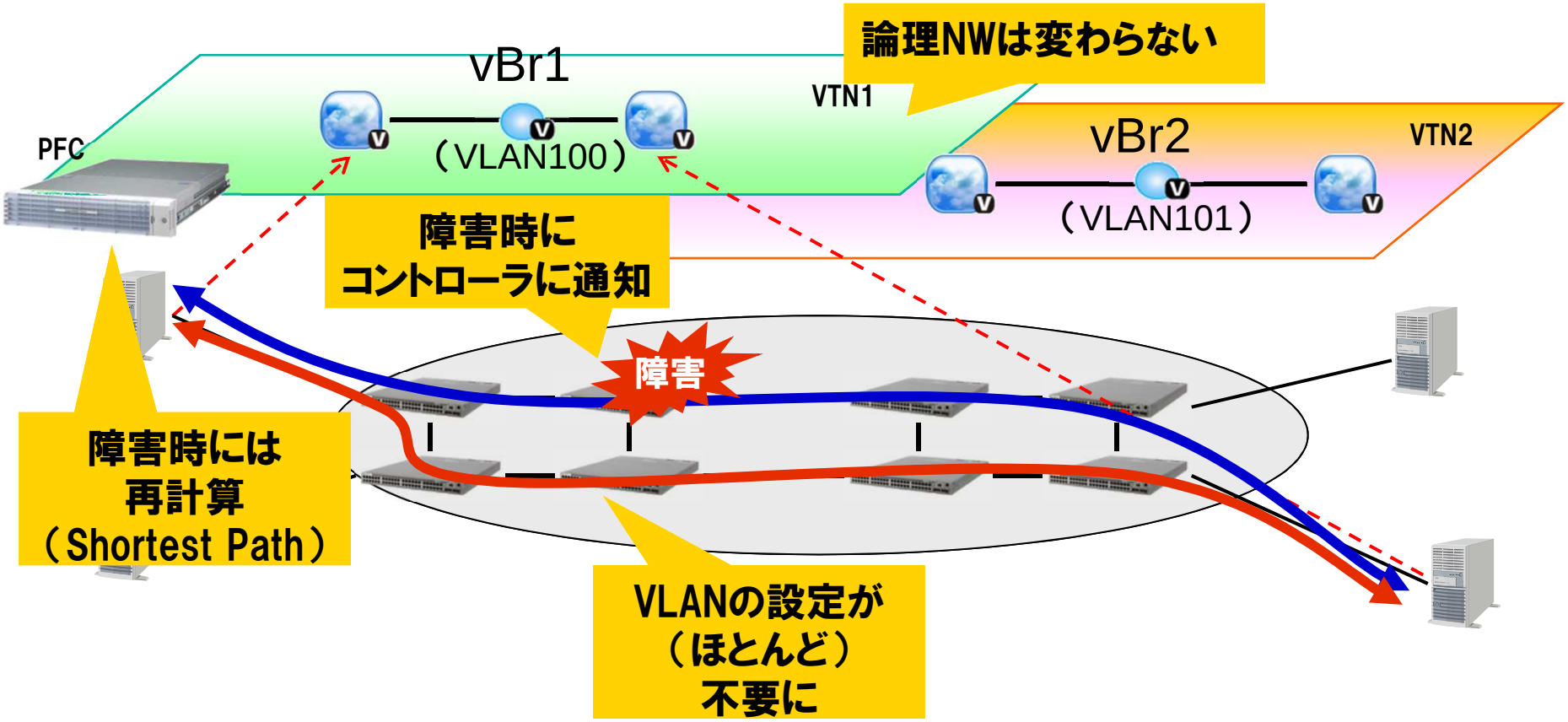
経路制御にみるDB化のうれしさ

Shortest Pathの経路制御アルゴリズムを標準搭載

DB化のメリット

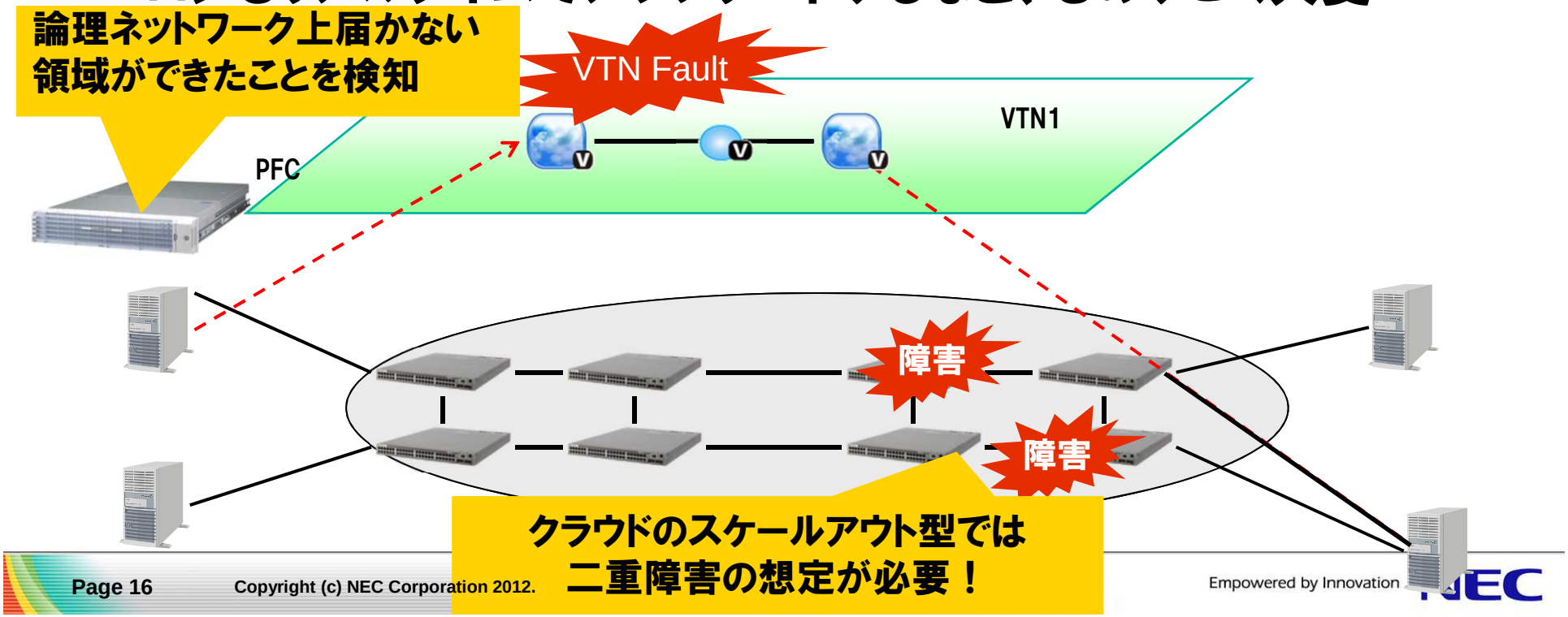
経路制御の「オートマ」化によりSTPのような冗長設計が不要

→ポートの“VLANの設定”が（ほとんど）不要に



論理層の監視にみるDB化のうれしさ

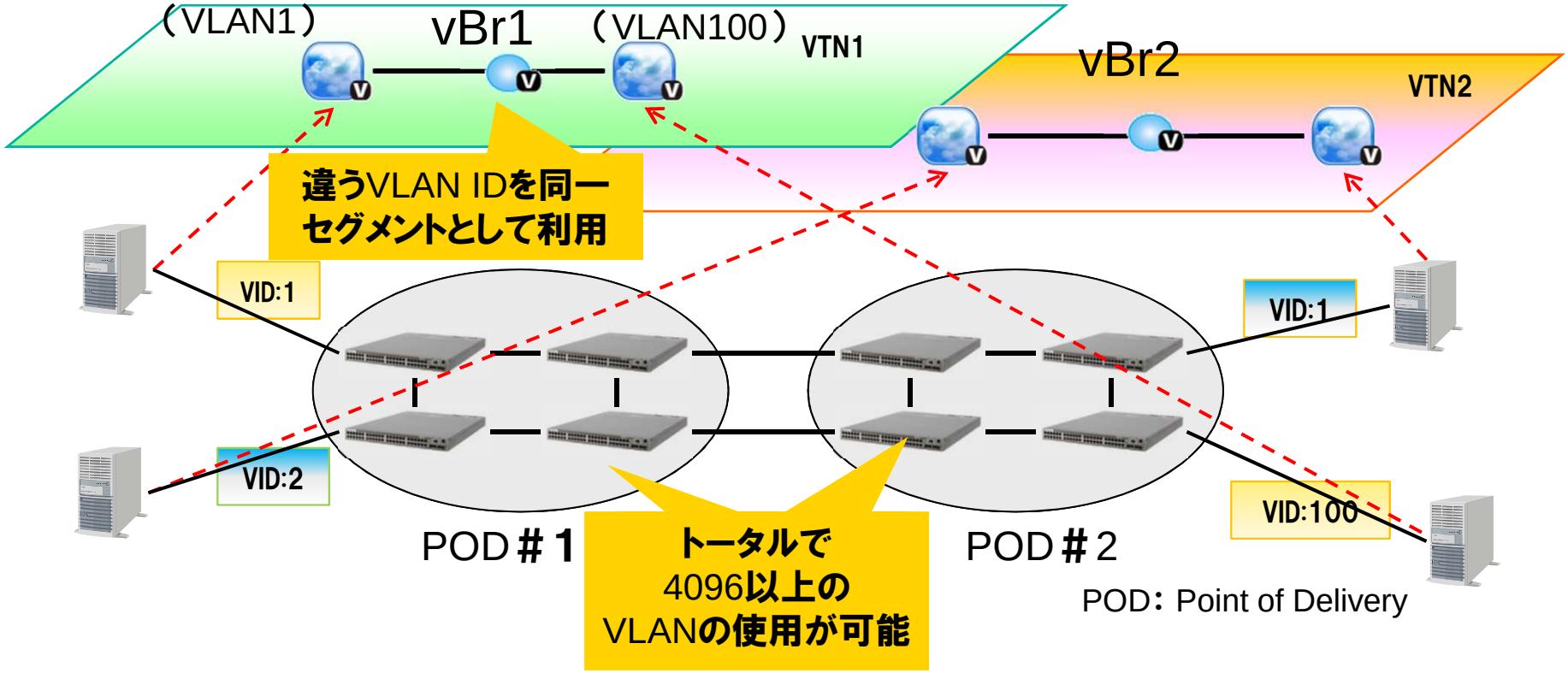
- VTN Faultというsnmp Trap
  - VTNの論理IF間で物理的な経路がなくなった場合に発生
- DB化のメリット
  - どのお客様のシステムに影響がでているかを瞬時に把握
  - NetConfやSNMPでやろうとすると、ユーザ側でDBを作成し、トポロジもリアルタイムでアップデートするなど、ものすごく大変



VLAN拡張(VLAN ID 4K超え)にみるDB化のうれしさ

VLAN 拡張の仕組み

- スイッチを物理プールでグループ化。物理プール間で異なるVLAND IDのVLANを接続することが可能。
- スイッチ間ではOpenFlowで定義されるMPLSのラベルを使用



VLAN拡張(VLAN ID 4K超え)にみるDB化のうれしさ

DB化のメリット

- vBRにスイッチの番号(Datapath ID)とVLAN IDのテーブルを登録
- MPLSのラベル番号などは自動的に割り付けられるため、ユーザは意識する必要が無い

テーブルの例					
vBridge	POD＃1		POD＃2		MPLS ラベル
	SW(Datapath ID)	VLAN ID	SW(Datapath ID)	VLAN ID	
vBr101	SW1(0000-0000-0000-0001)	101	SW3(0000-0000-0000-0003)	1101	16
	SW2(0000-0000-0000-0002)	101	SW4(0000-0000-0000-0004)	1101	16
vBr102	SW1(0000-0000-0000-0001)	102	SW3(0000-0000-0000-0003)	1102	17
	SW2(0000-0000-0000-0002)	102	SW4(0000-0000-0000-0004)	1102	17
vBr103	SW1(0000-0000-0000-0001)	103	SW3(0000-0000-0000-0003)	1103	18
	SW2(0000-0000-0000-0002)	103	SW4(0000-0000-0000-0004)	1103	18
:	:	:	:	:	:

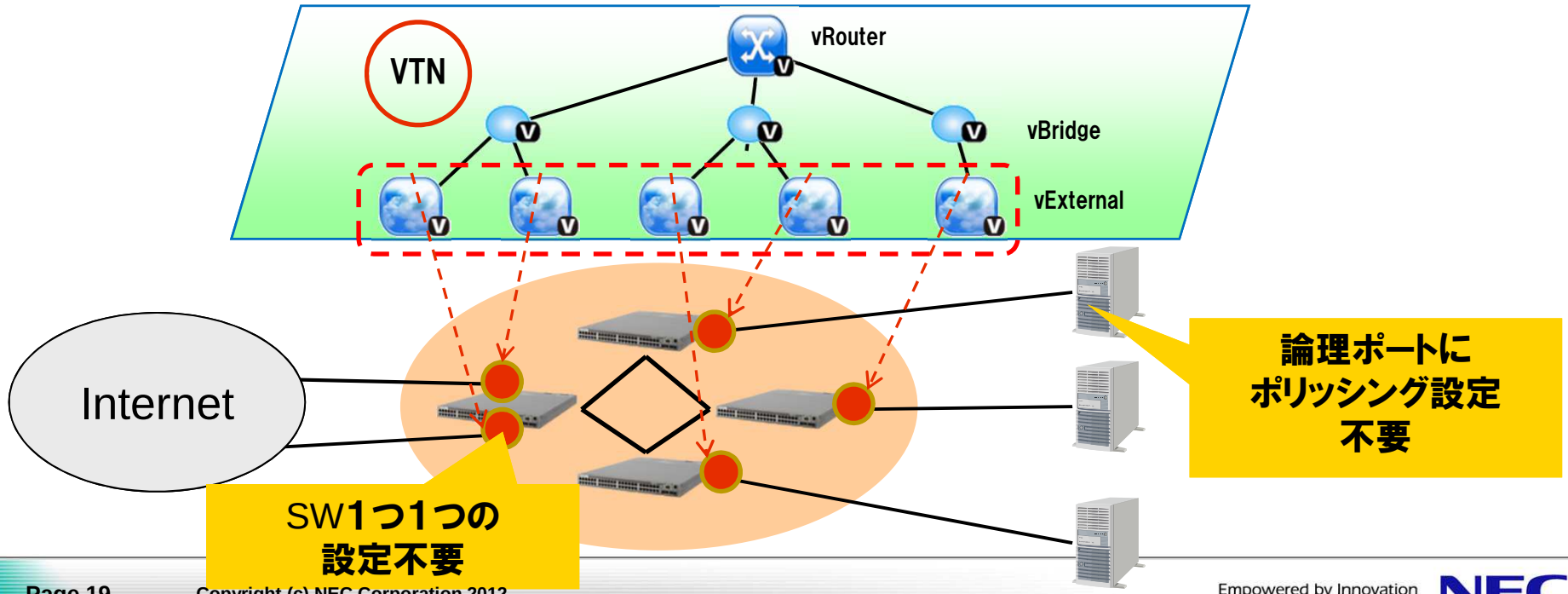
自動で割り付け

QOSの統合管理にみるDB化のうれしさ

VTN単位のQOS

- VTNに所属する全論理IFに設定することが可能(ポリッシング)
- あるお客様が帯域を占有し、他のお客様に迷惑かけることを抑制

- DB化のメリット
  - 論理のVTN単位で指定するので物理ポート1つ1つに設定不要
    (IFごとに帯域の足し算などの管理は必要)



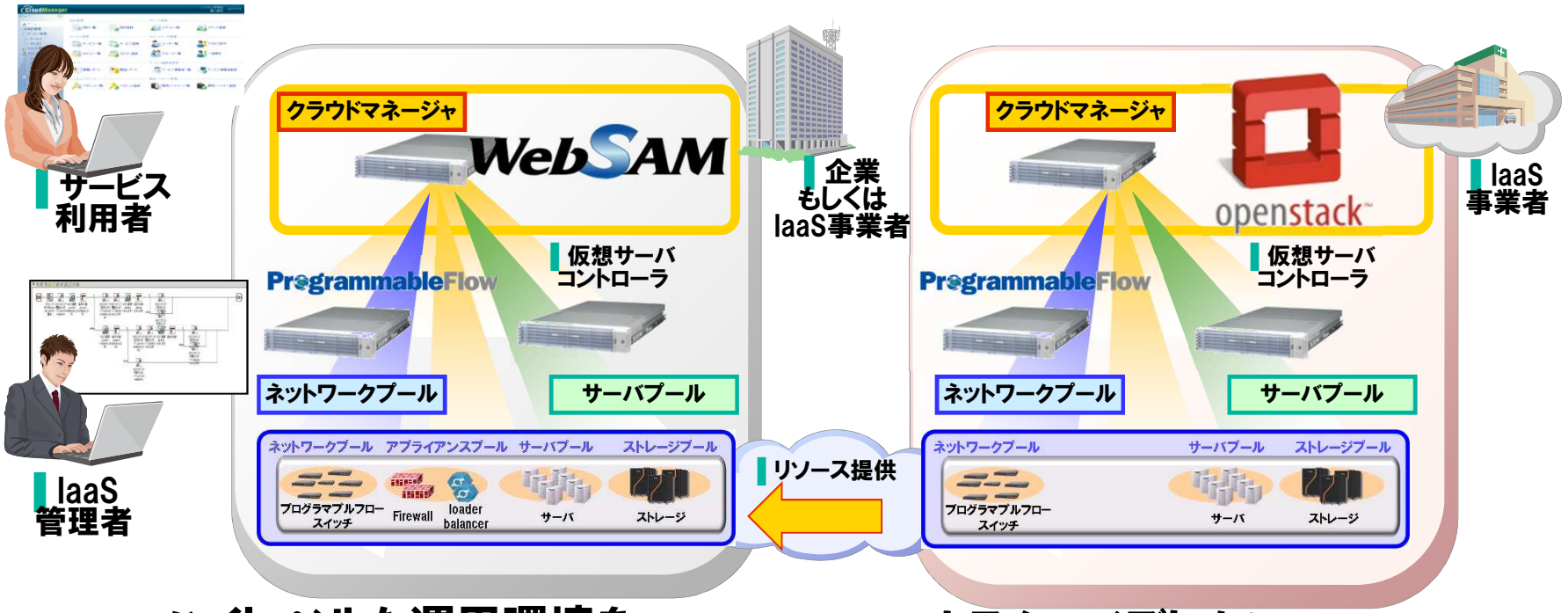
IaaS・仮想化基盤の運用を自動化する SDNソリューション

Interop Tokyo 2012 OpenFlow　ShowCaseデモ

OpenFlowを利用したSDNソリューションによるハイブリッドクラウドのデモンストレーション（実証実験※）

NECブース（プライベートクラウド）
WebSAM＋プログラマブルフロー

OpenFlow ShowCase（パブリッククラウド）
OpenStack＋プログラマブルフロー



～ハイレベルな運用環境を
実現したい企業・事業者様むけ～

～カスタマイズしたい
SI力のある事業者様むけ～

ご協力：A10ネットワークス株式会社様（ロードバランサ）、フォーティネットジャパン株式会社様（ファイアウォール）

※プログラマブルフロー/WebSAM連携は、2013年度1Q以降出荷予定です。

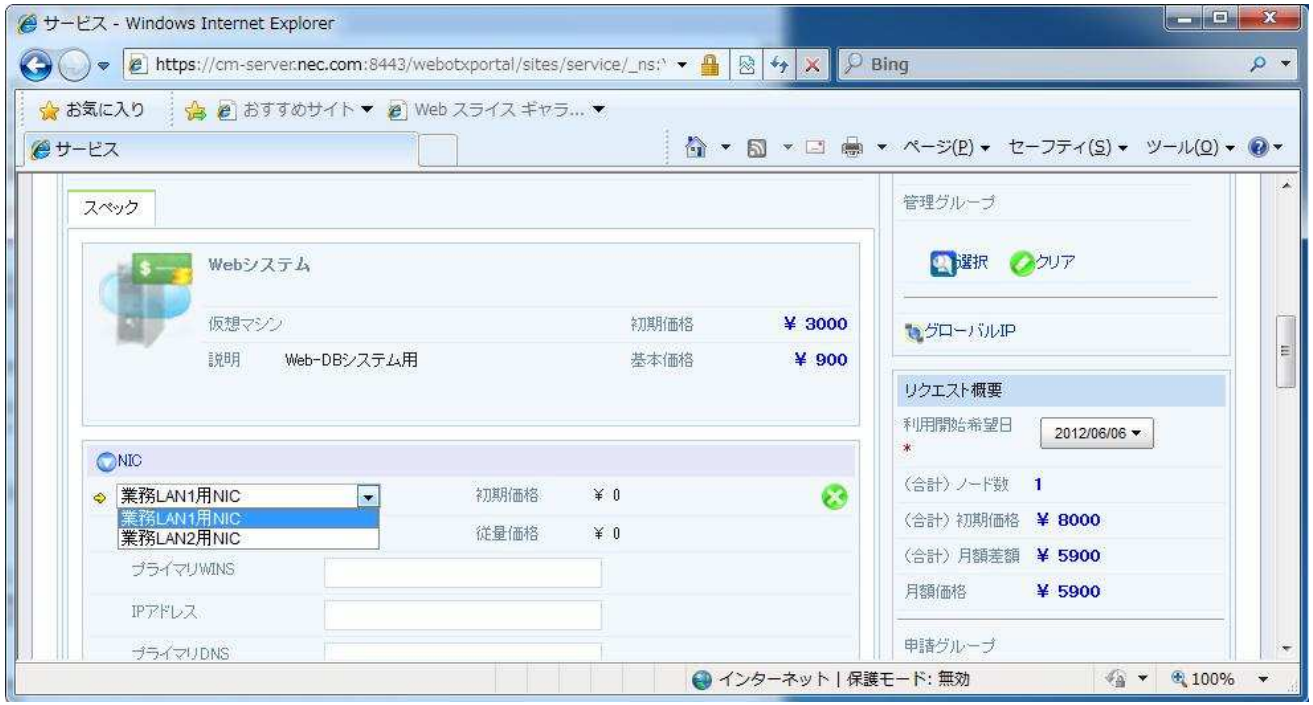
STEP1 利用者による操作イメージ(IaaS利用者)

WebSAM Cloud Manager

IaaS利用者はWebベースのCloud Managerに必要なリソースを入力
このとき、仮想ネットワークもいくつ欲しいかを入力しておき、各VMがどの仮想ネットワークに接続するかを指定

セルフサービスポータル画面イメージ

※WebSAM Cloud Managerによる画面



IaaS利用者むけ

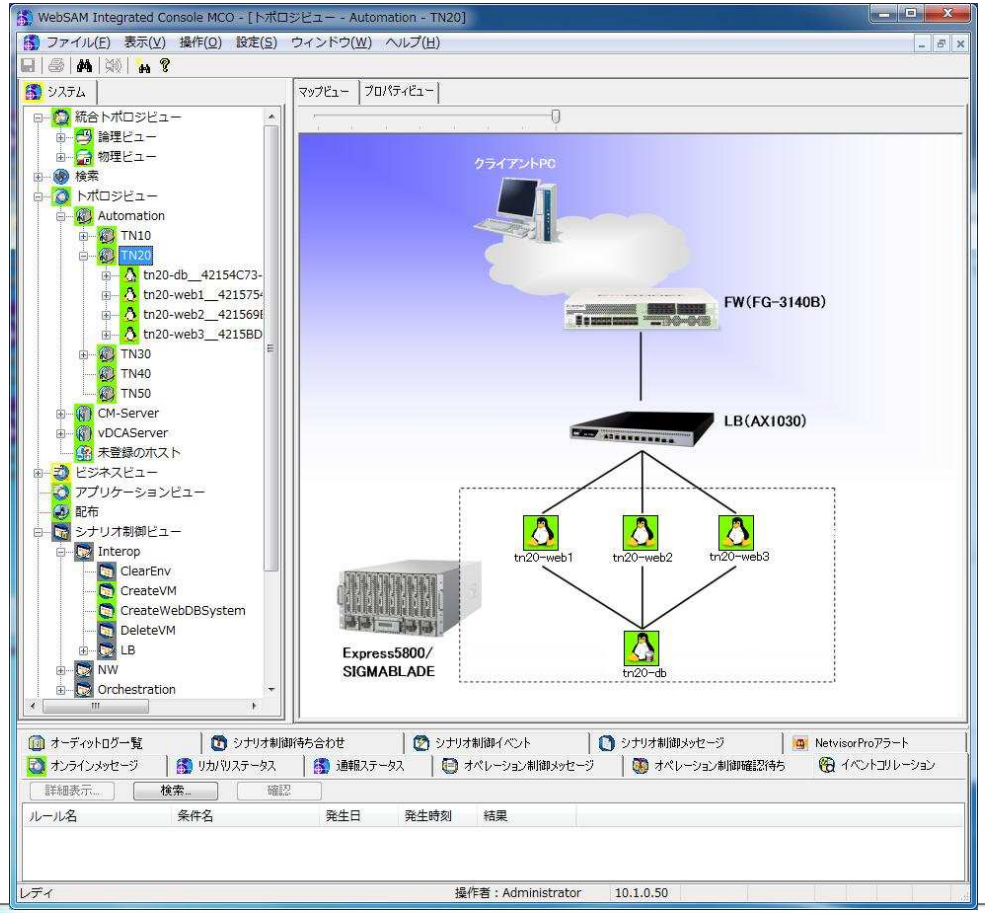
STEP2 プロビジョニングのイメージ(IaaS管理者)

WebSAM vDC Automation

vDC Automation はCloud Managerから要求されたリソース(仮想サーバ、ストレージ、ネットワーク)を用意

仮想マシン作成完成時のイメージ

※WebSAM vDC Automationによる画面



IaaS管理者むけ
(サーバ管理者)

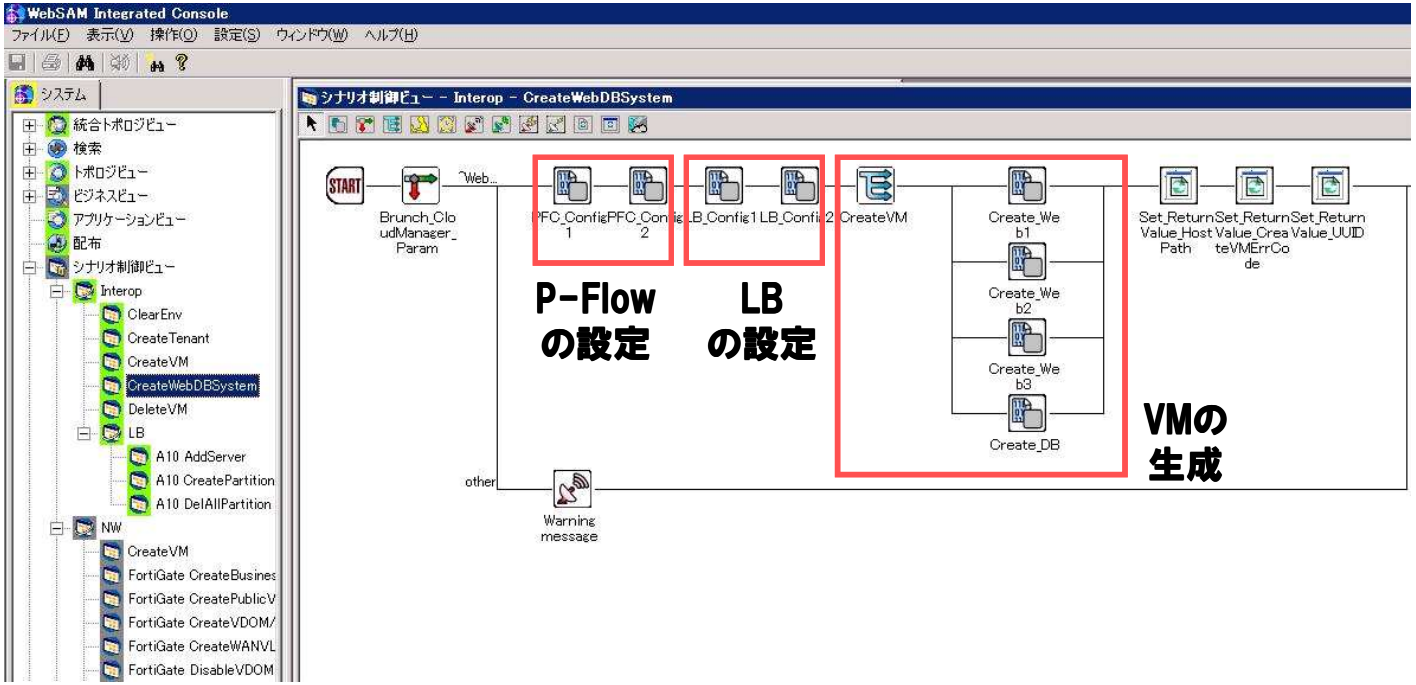
STEP3 NWシナリオのイメージ（IaaS管理者）

WebSAM vDC Automation

- ネットワーク設定のために、vDC Automationでネットワーク設定をスクリプトもしくはAPIによりシナリオ化
- IaaS利用者からの申請があった場合には、これに従いネットワーク機器の設定を自動的に行う

仮想マシン作成時のネットワークシナリオイメージ

※WebSAM vDC Automationによる画面

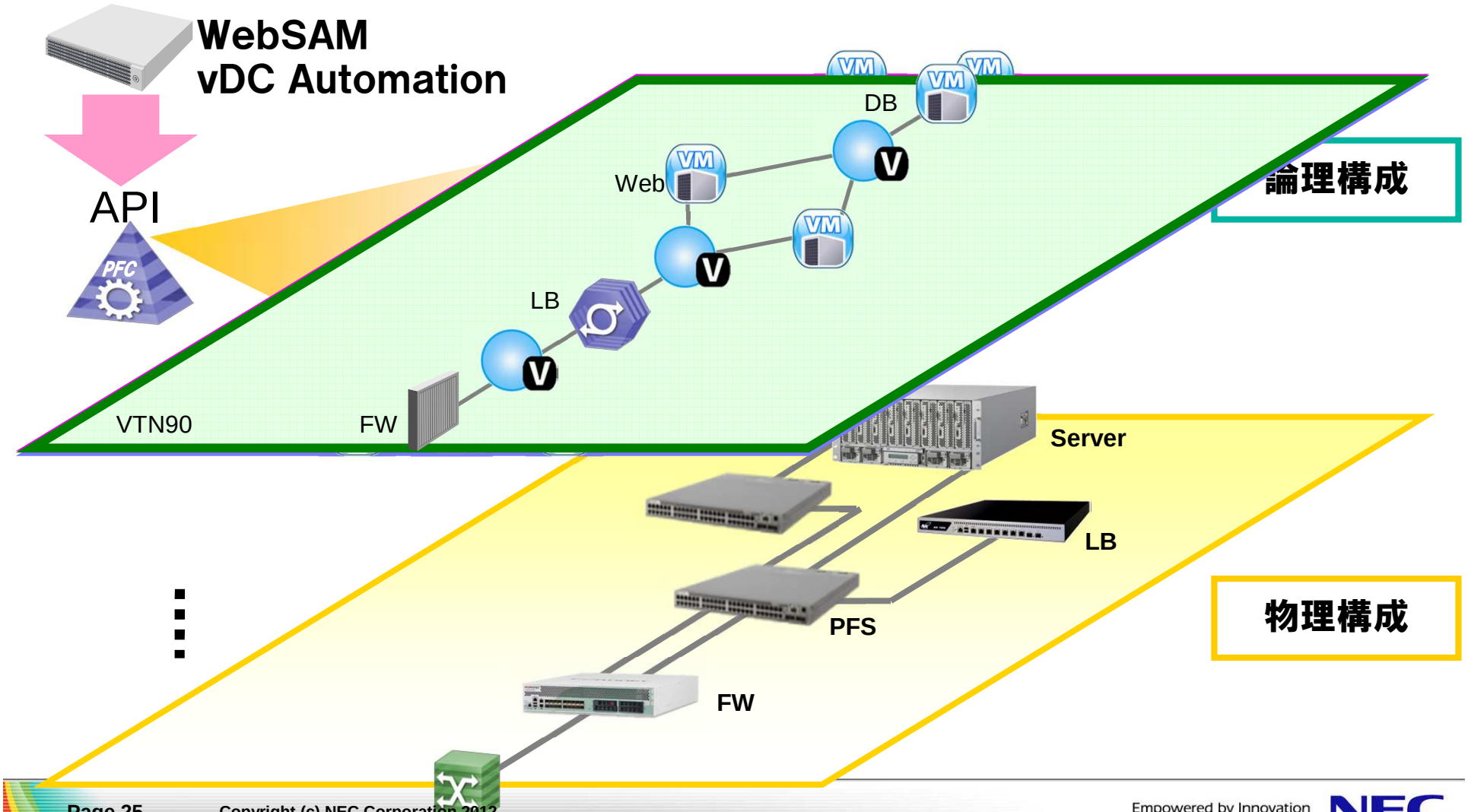


IaaS管理者

STEP4 ネットワークの仮想化のイメージ

ProgrammableFlow

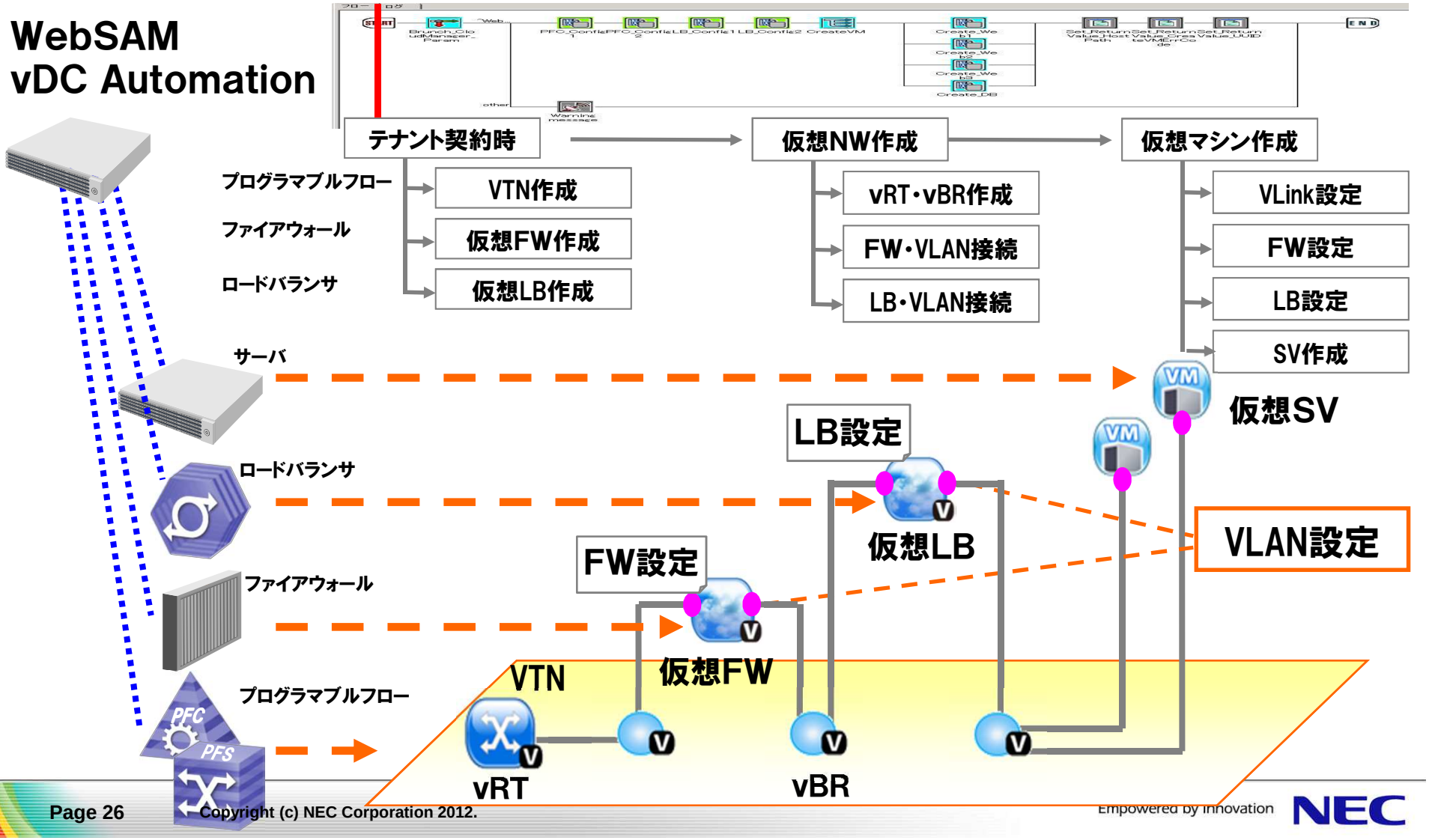
ユーザからのリクエストに応じて、オーケストレーションサーバからの指示でOpenFlowネットワーク上に仮想ネットワークを設定



STEP5 シナリオに基づいた仮想化NW生成・設定

ProgrammableFlow

事前にシナリオを設定しておくことで、Firewallやロードバランサも含めて、仮想ネットワークの生成や設定を自動化

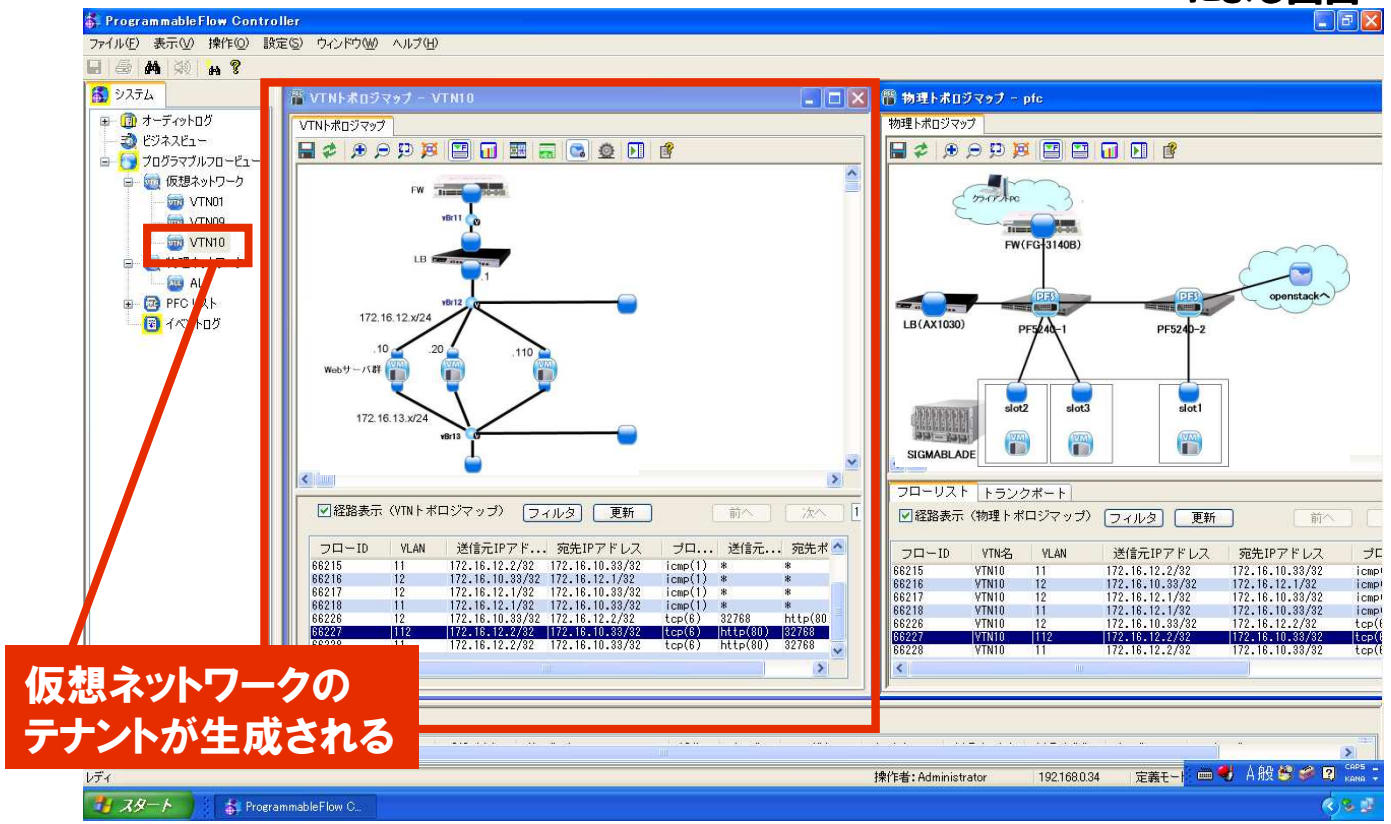


STEP6 できあがったネットワーク（NW管理者）

今までの作業により、仮想ネットワークが自動的に完成
仮想ファイアウォール、仮想ロードバランサもすぐに使用すること可能

物理・仮想ネットワーク図のイメージ

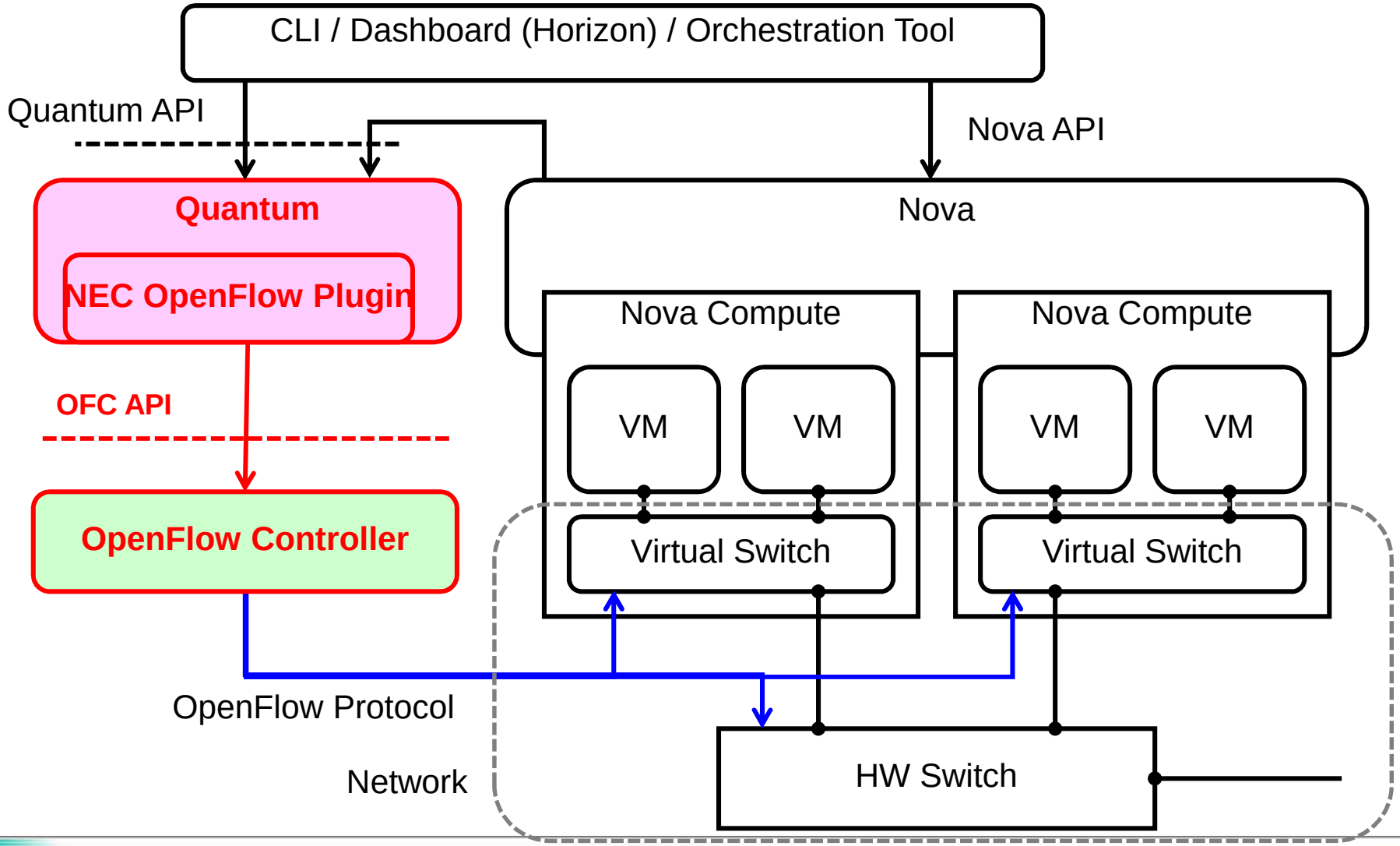
※プログラマブルフロー・コントローラによる画面



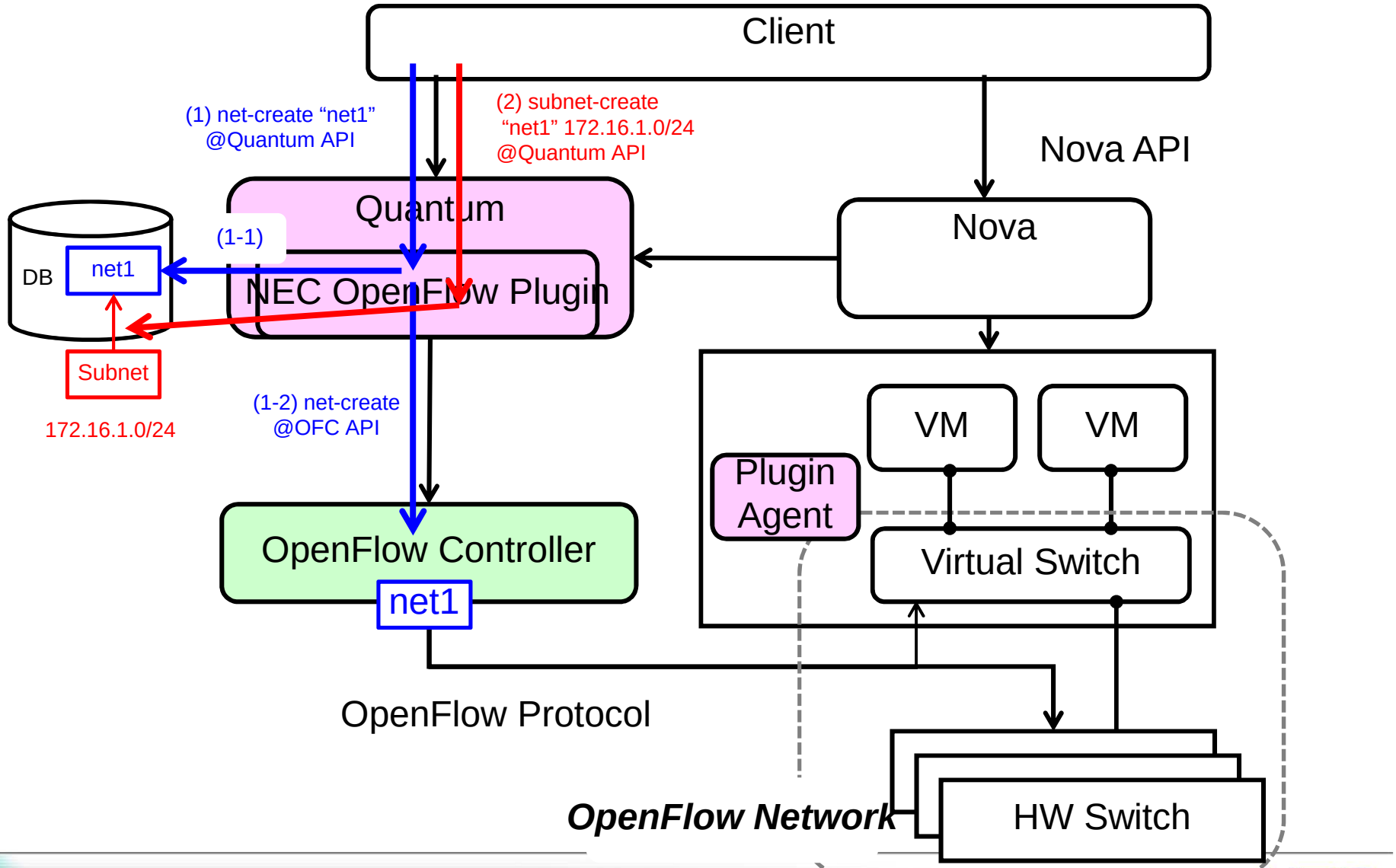
IaaS管理者
（NW管理者）

OpenStack と OpenFlow の連携(１)

OpenStackとOpenFlowの連携のモデル図

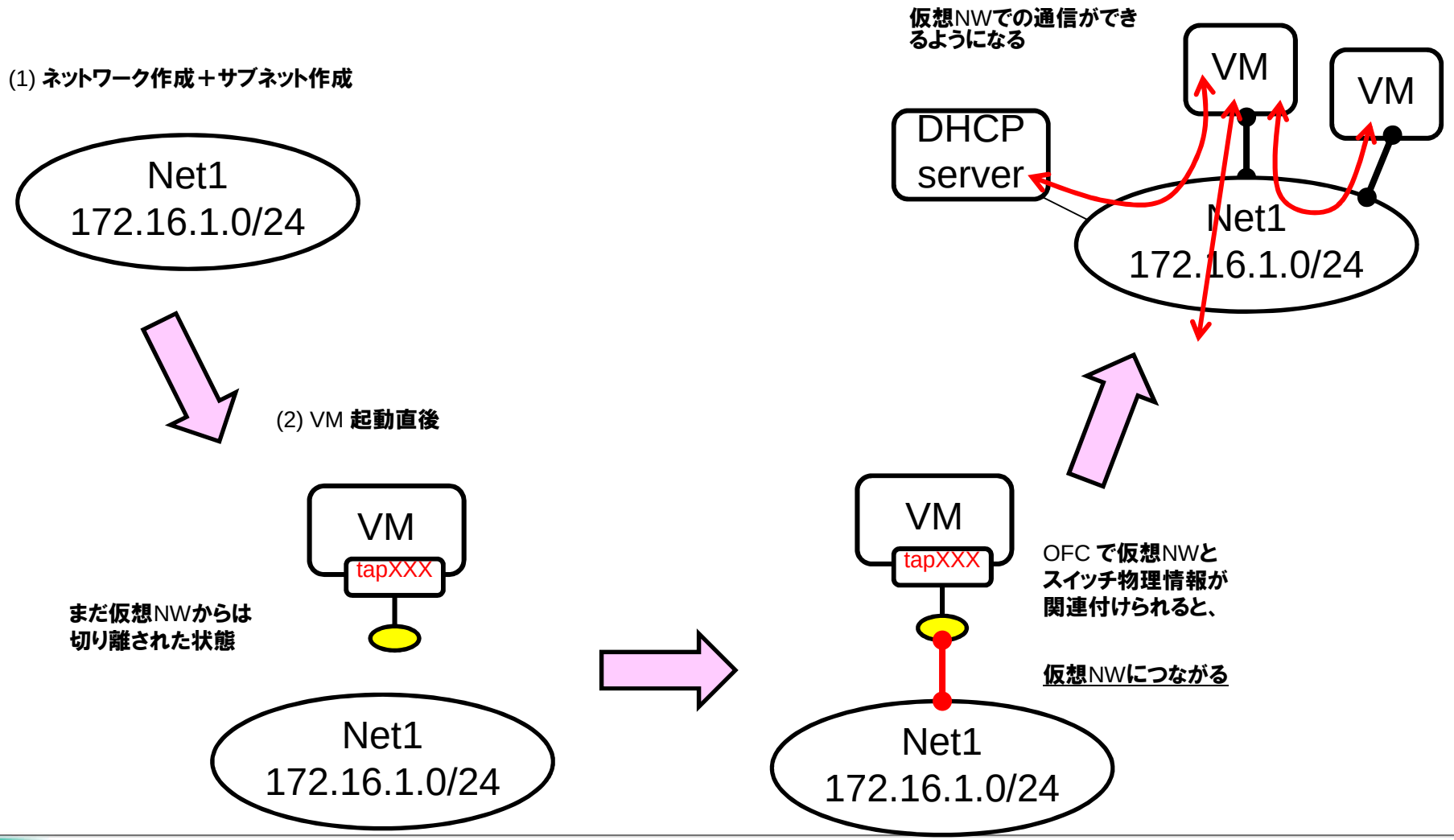


OpenStack と OpenFlow の連携(２)



OpenStack と OpenFlow の連携(３)

仮想ネットワークの観点で見ると、



Quantum NEC OpenFlow Plugin

- Quantum で作成された論理L2ネットワークを、OpenFlow Network 上の仮想ネットワークとして実現
- OpenFlow Controller (OFC) の Northband API として、仮想ネットワークを操作する REST API を定義
  - Sliceable Network Management API
  - https://github.com/trema/apps/wiki
  - テナント、ネットワーク、ポート の CRUD を定義
- Quantum Plugin は OFC REST API を呼び出す。
  - PluginはQunatumとOFCのIDマッピング、OFC側で必要な情報の収集を行う
- 対応 OpenFlow Controller
  - Trema Sliceable Switch (OSS)
  - ProgrammableFlow Controller (NEC 製品)

＜ネットワークリスト＞

```
GET /tenants/tenant-1/networks

HTTP/1.1 200 OK
Content-Type: application/json
[
  { "id" : "net-1", "description" :  "QuantumID=xxxxxx" },
  { "id" : "net-2", "description" :  "QuantumID=yyyyyyy" }
]
```

＜ポート作成＞

```
POST /tenants/tenant-1/networks/net-1/ports HTTP/1.1
Content-type: application/json
{
  "datapath_id" : "0x0000000000001234",
  "port" : 5
}
```

まとめ

OpenFlowファブリック

- OpenFlowを利用した製品はNWアプリケーションを搭載済み
  プログラムを組まなくても、すぐ使用することが可能
- 仮想ネットワークをVTNという概念でデータベース化
  経路制御のオートマ化、論理面の監視、スケーラビリティ向上、
  管理の自動化などSDNらしい機能ができつつある
- OpenFlow製品はネットワークアプリケーションの実装次第

クラウド基盤のSDNソリューション

- サーバ・ストレージとあわせてプロビジョニング、設定作業の削減
- VLAN IDやIPアドレスの管理作業も自動化
- 迅速性を提供

【ご参考】
UNIVERGE PF導入実績・事例

導入事例

日本通運株式会社様 ～世界初、業務システムへの導入～

導入の背景

- ICTリソースの効率化・ガバナンス強化のため、全社サーバ統合による プラットフォームの共通基盤を整備
- サーバ統合後に仮想サーバの増設、移動毎にネットワークの再設計、設定が発生。ネットワークの運用コストが増大

お客様の導入目的

お客様の要望 ： 運用コストの軽減
① ネットワーク運用の文化を変更したい
② 移行に関わる運用・保守コストを削減したい

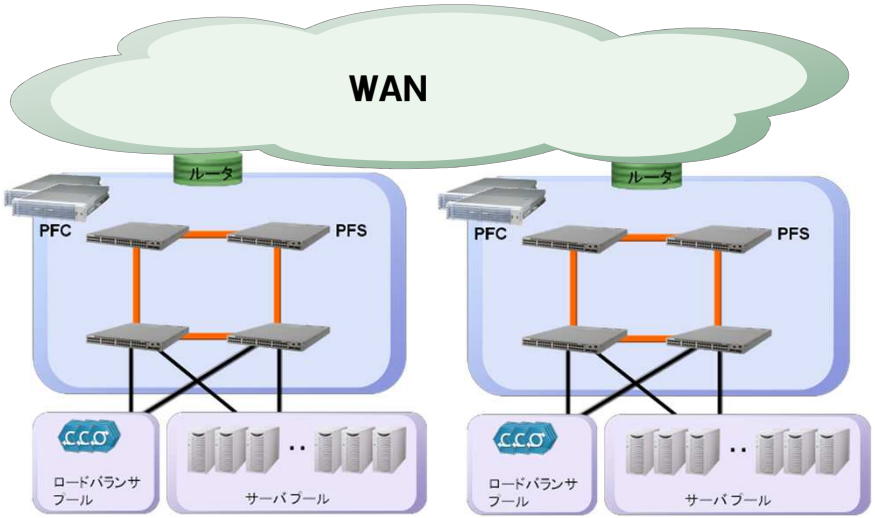
新しい切り口のご提案

- ネットワークを集中管理して**シンプル化** し、運用業務の負荷を飛躍的に軽減
- **ネットワーク可視化** で通信経路異常や品質低下などの障害箇所を視覚的に把握
- 物理的な制約なくマルチテナントで**ネットワーク仮想化** 環境を容易に実現

導入事例

日本通運株式会社様 ～世界初、業務システムへの導入～

日本通運様　構成イメージ



メインデータセンター

DR／BPC
バックアップセンター

プログラマブルフロー導入による効果

- ネットワーク設定の変更には1回あたり100～200万程度のコスト（2010年度は年間3回実施）がかかっていたが、プログラマブルフローの導入によって、物理構成の変更が容易となったため、自社の社員で作業が可能になり、設定・変更費は実質無料。
- ネットワーク構築のリードタイムが、通常2ヶ月のところ10日で可能となった。
- シンプルなNW構成を実現可能なため、ハウジング費用およびNW運用管理費用を大幅に削減（消費電力80%、設置面積70%削減）

プログラマブルフローへの今後の期待

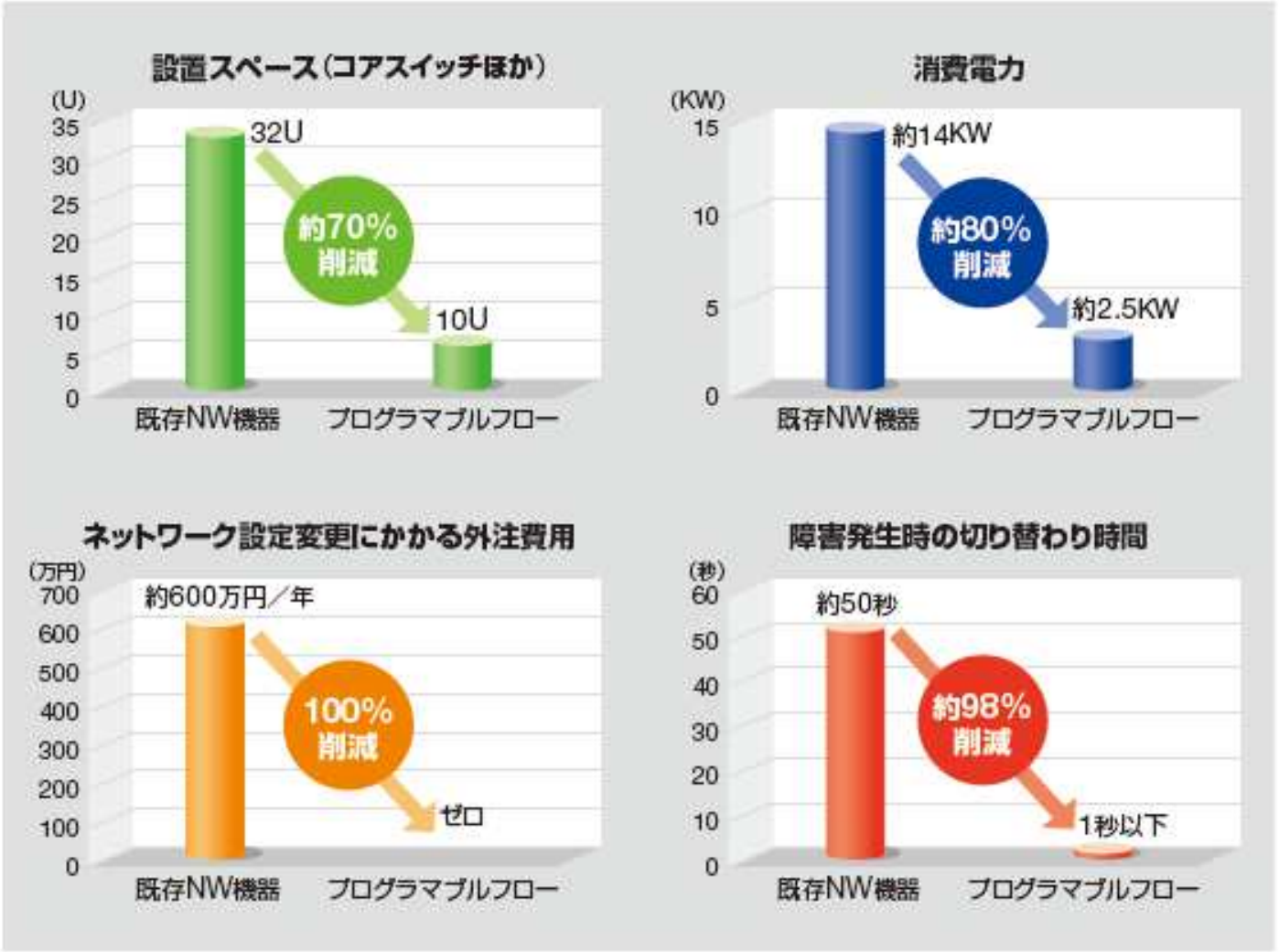
- 全システムの標準化の基盤としての利用
  パブリッククラウドとプライベートクラウドを共有し、利用者が意識しないで利用できる環境を、プログラマブルフローで構築したい

導入事例

導入効果

バックアップサイトのハウジング費用を大幅に低減
NW運用費用を削減および可用性を大幅に向上

● 日本通運様のプログラマブルフロー導入効果



日通様のバックアップサイトを　既存NW機器とプログラマブルフローで構成した場合の比較図
構成詳細：　プログラマブルフロー：　コントローラ×２台　スイッチ×４台　L2SW×２台

導入事例

金沢大学附属病院様

金沢大学 KANAZAWA UNIVERSITY

急速に進歩する医療技術の発達に追従できる安定したNW基盤の構築

導入の背景

- ネットワークを含めた共通基盤の構築を、既存のネットワークはそのままに統合し、且つセキュリティも確保したい・・・
- 医療機器の導入のたびに、ネットワークの設定や更新を実施しない安定したネットワーク基盤を構築したい

プログラマブルフロー導入による効果

- プログラマブルフローのネットワーク仮想化を使用することで、既存のネットワークはそのままに統合共通基盤に接続することが可能
- SDNによる集中管理により、柔軟にネットワークを構築可能

導入事例

金沢大学附属病院様（企業LAN）

金沢大学 KANAZAWA UNIVERSITY

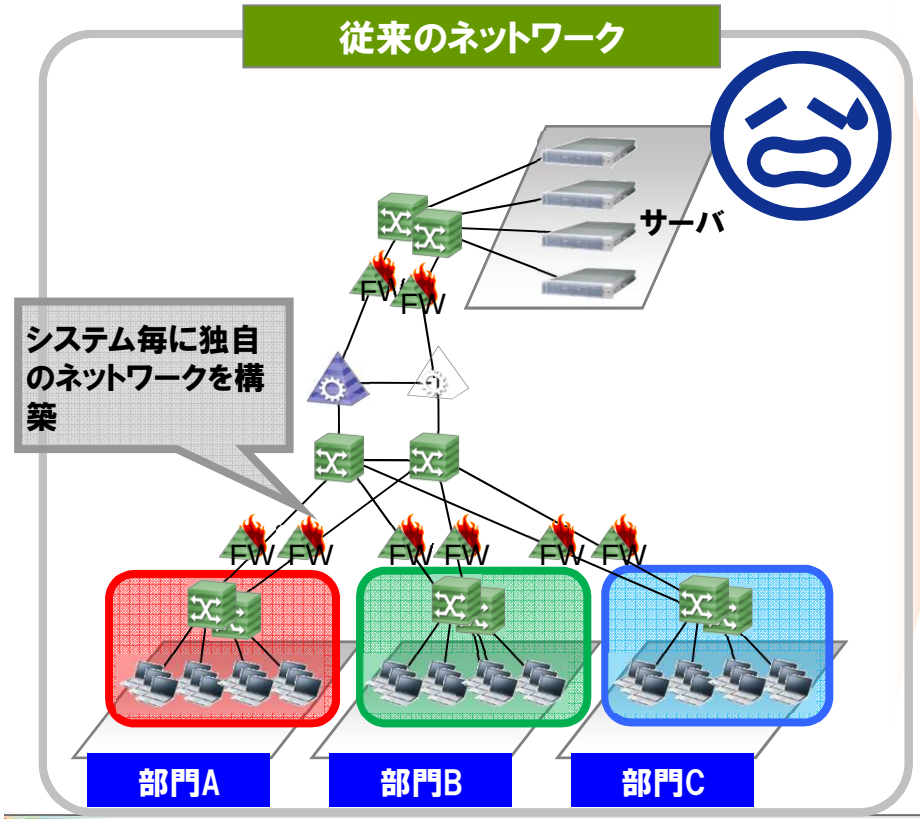
既存のネットワークに影響を与えず、セキュアな統合・共通基盤を構築

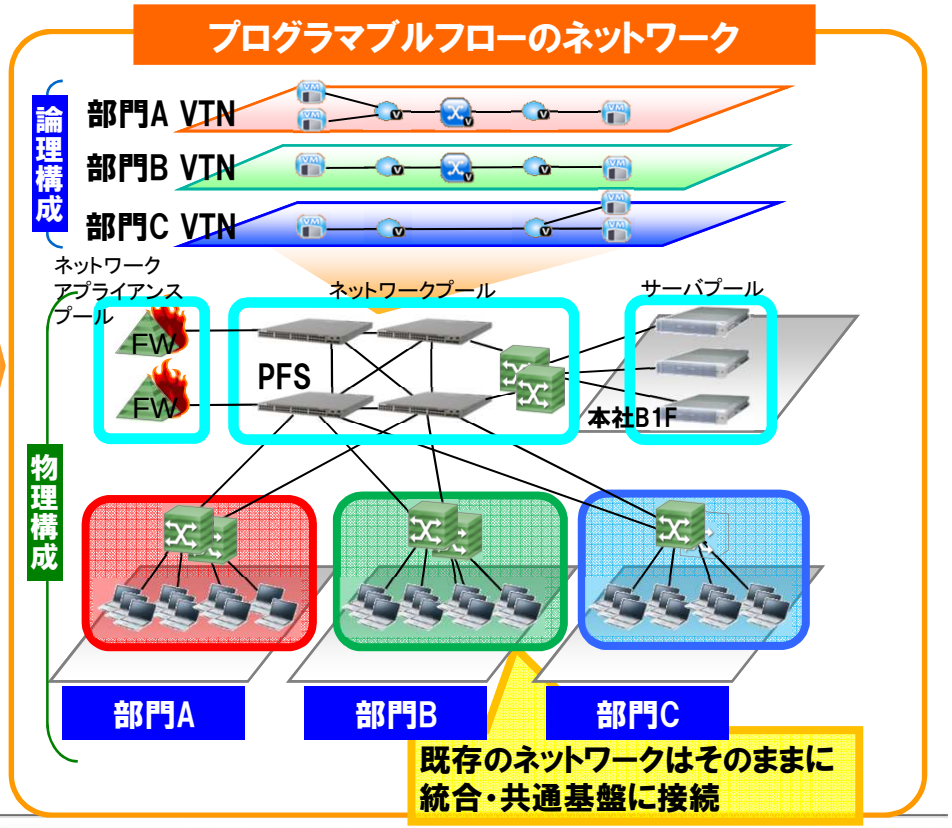
課題

ネットワークを含めた統合・共通基盤を構築を、できるだけ既存のネットワークはそのままに統合し、且つセキュリティも確保して実現したい・・・

ProgrammaleFlowでできること

プログラマブルフローのネットワーク仮想化を使用することで、既存のネットワークはそのままに統合・共通基盤に接続することが可能です



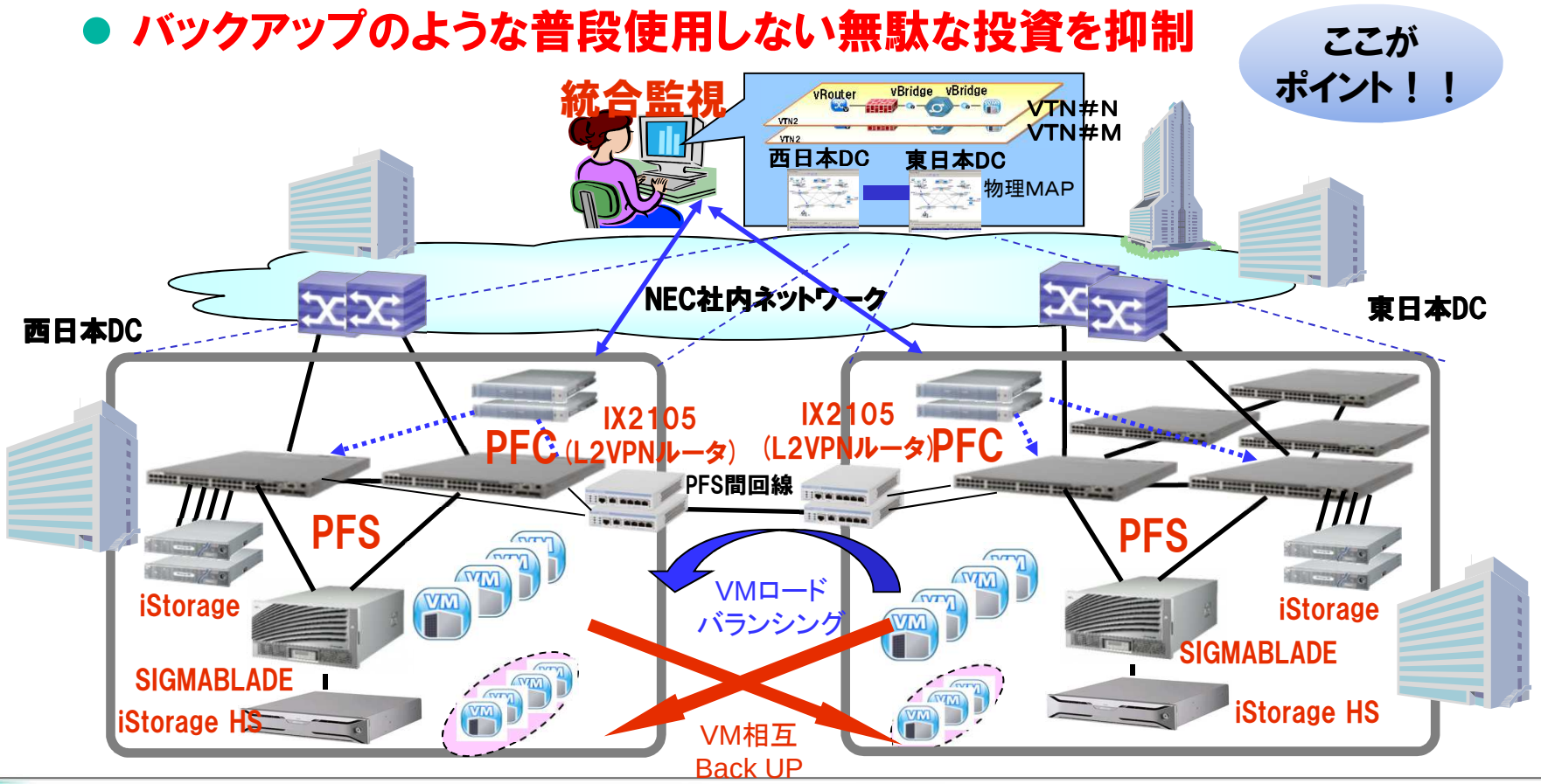


導入事例

社内クラウド基盤への導入事例

NECのクラウド型ソフトウェア開発基盤への適用

- 東日本大震災を契機に、開発環境の基盤整備を実施
- ソフト開発環境（資産、実行環境、検証環境）を仮想化して集約
- BCP/DR対策、負荷分散を複数DC（東西DC）構成にて対応
- **バックアップのような普段使用しない無駄な投資を抑制**



NECグループビジョン2017

人と地球にやさしい情報社会を

イノベーションで実現する

グローバルリーディングカンパニー

Empowered by Innovation