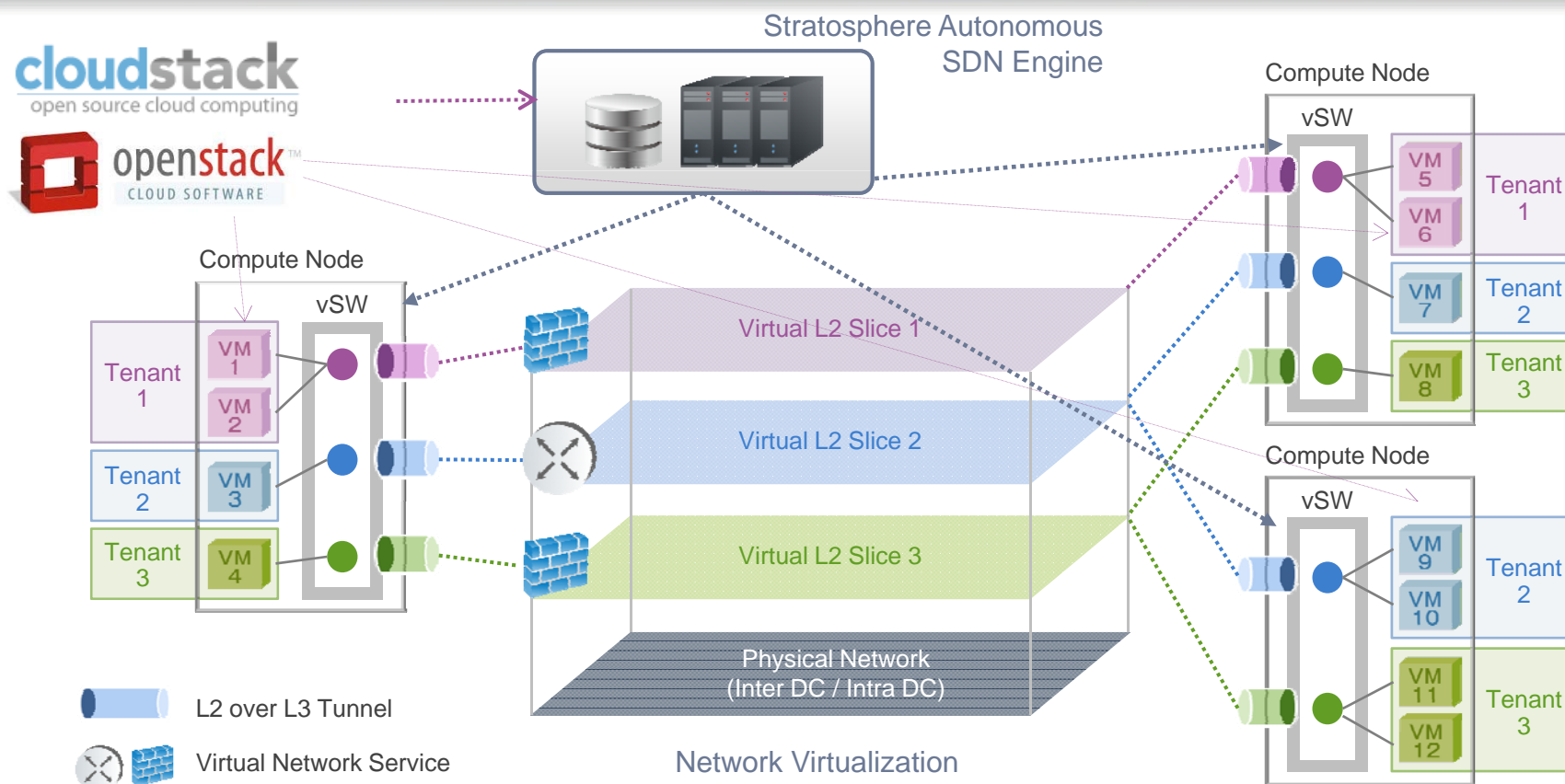


# Stratosphereが提供する SDN/OpenFlow技術の現在と未来

株式会社ストラトスフィア  
2013年11月19日  
[sirasaki@stratosphere.co.jp](mailto:sirasaki@stratosphere.co.jp)

- クラウド/データセンタソリューション
- ネットワークサービスプロバイダソリューション
- 仮想オフィスネットワーク

# Cloud/データセンタソリューション



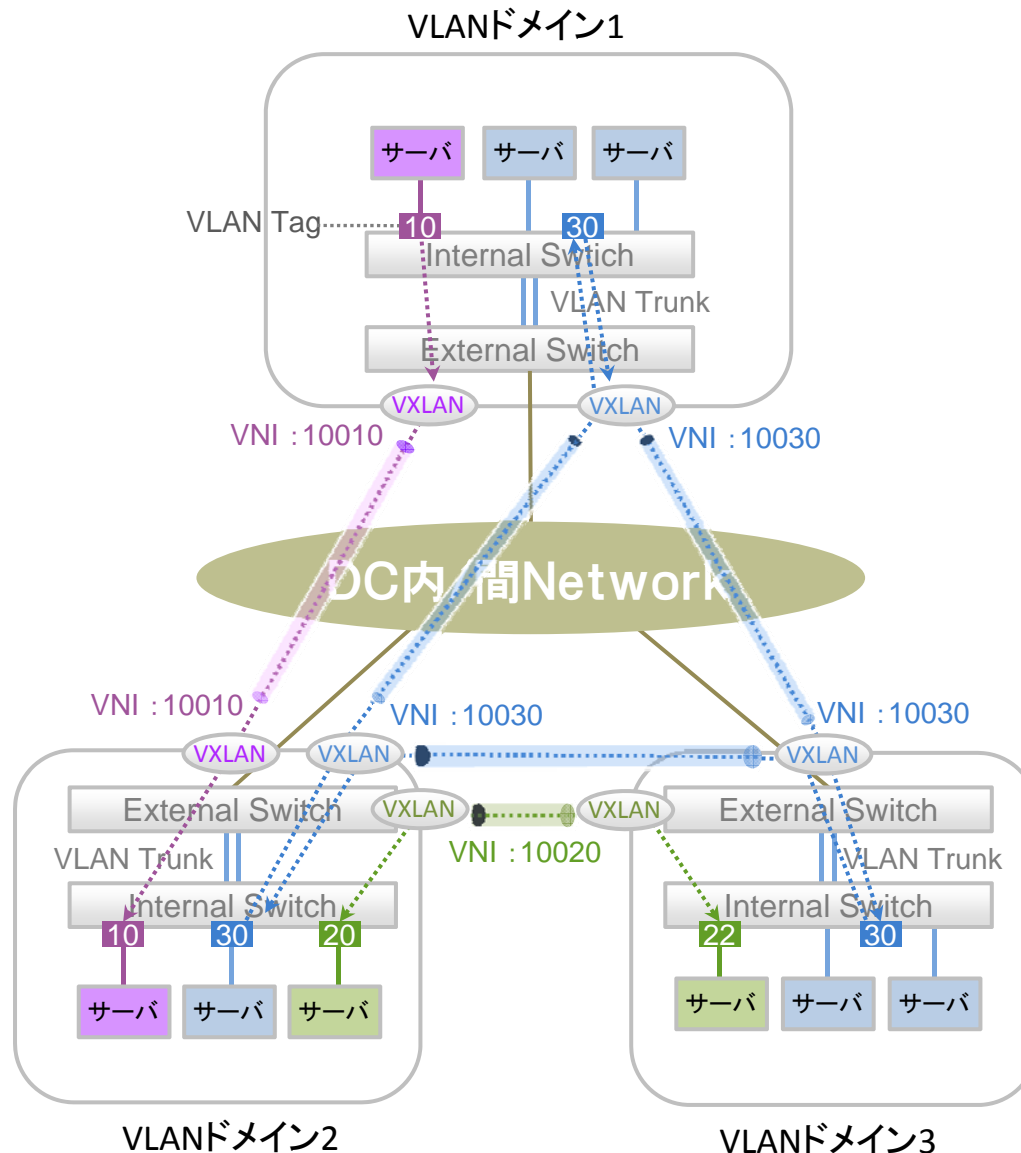
## ■ エッジオーバーレイ型SDN

- Virtual Switch間のIPTunnelでVirtual L2 Sliceを実現
- VXLAN, STT, NVGREの各種オーバーレイプロトコルに対応
- KVM, VMWare, XEN, HyperV等のHyperVisorに対応(予定)

## ■ SDNエンジンによる仮想ネットワーク環境の統合制御

- 各テナントVirtual L2 Sliceの構成・管理
- 物理ネットワーク上の論理ネットワークの展開、稼働監視
- vRouter, vFirewall等の多様なネットワーク構成機能の組み込み

## ■ cloudstackと連動



## 様々なネットワーク技術を活用した ハイブリッドアーキテクチャ

### ■ VLANの活用

- VLANドメイン内では、Internal SwitchがサーバにユニークなVLANタグを付与しテナントを識別
- VLANドメインは、1台の仮想化されたマシン内や1ラック内、1クラスター内など、柔軟に構成可能

### ■ 新しいオーバレイプロトコルで仮想NWを構成

- External Switchで、VLANドメインを他のVLANドメインとIPオーバレイ方式で接続
- VLANタグをVNI等のトンネルタグに変換することでID空間を拡張(VXLANの場合約1600万通りの仮想LANをサポート)
- DC内/間ネットワークで、ホスト間のIPリーチャビリティが確保できさえすれば利用可能

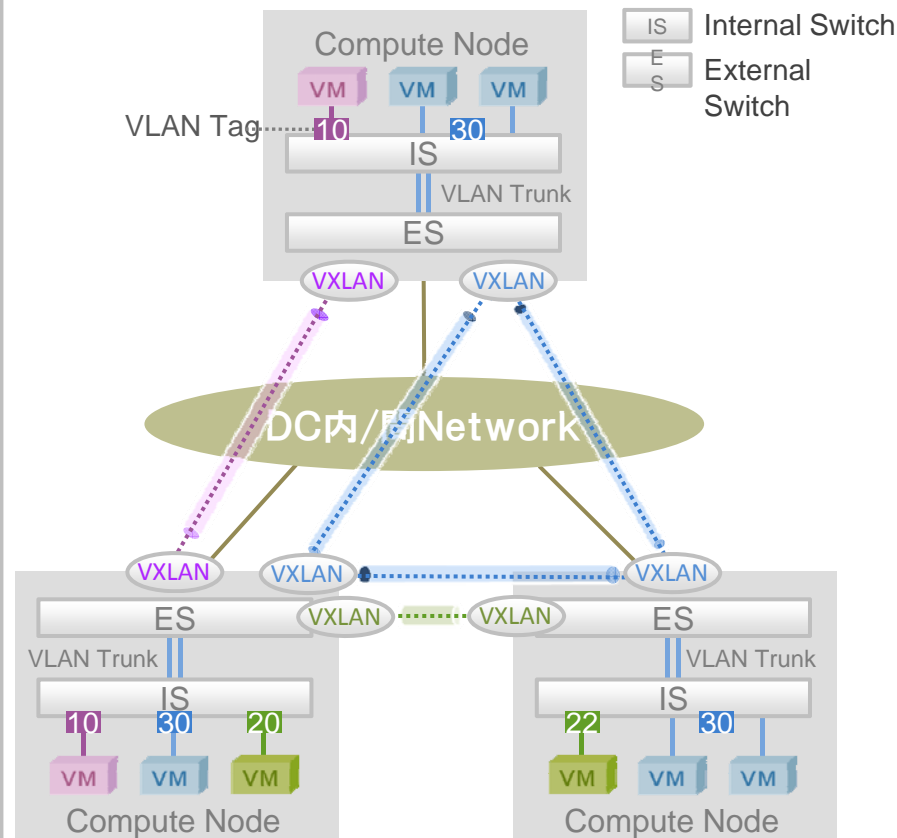
### ■ OpenFlowでの配送制御

- External Switchでのパケット配送制御にFlow Ruleを活用
- プロアクティブ制御でオーバーヘッドを最小化

### ■ 多様なL2プロトコルでDC内/間NWを制御(予定)

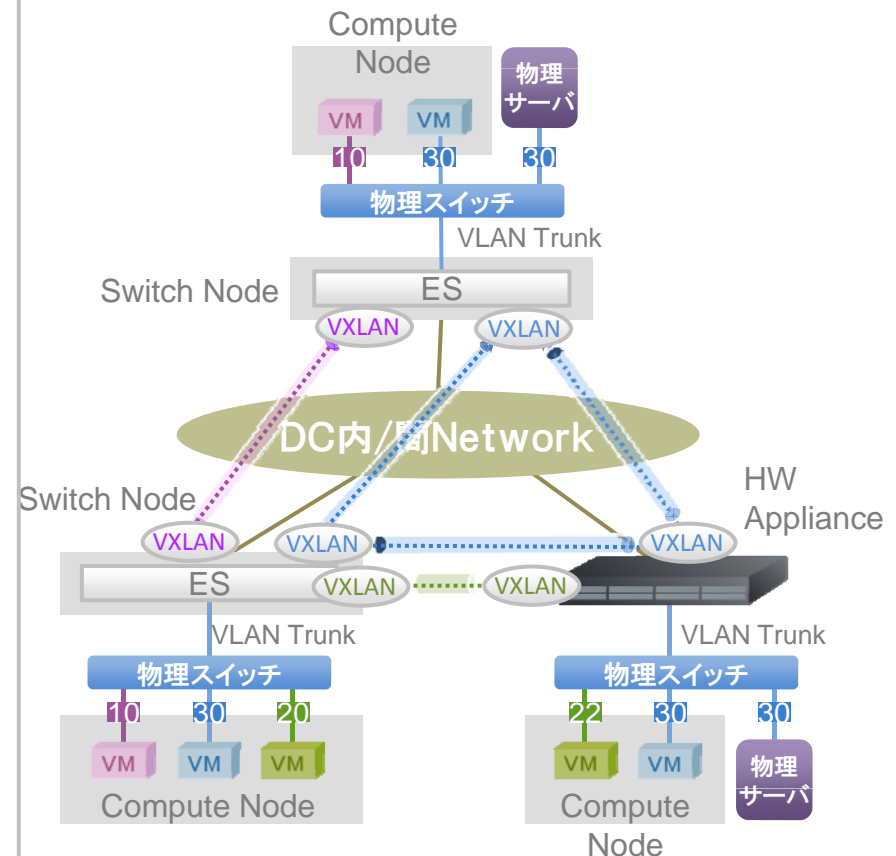
- External Switchで物理ネットワークレイヤを制御
- RSVP-TE/LDP、802.1ad/802.1ah、LLDP/TRILL

## ■ ビルトインモード



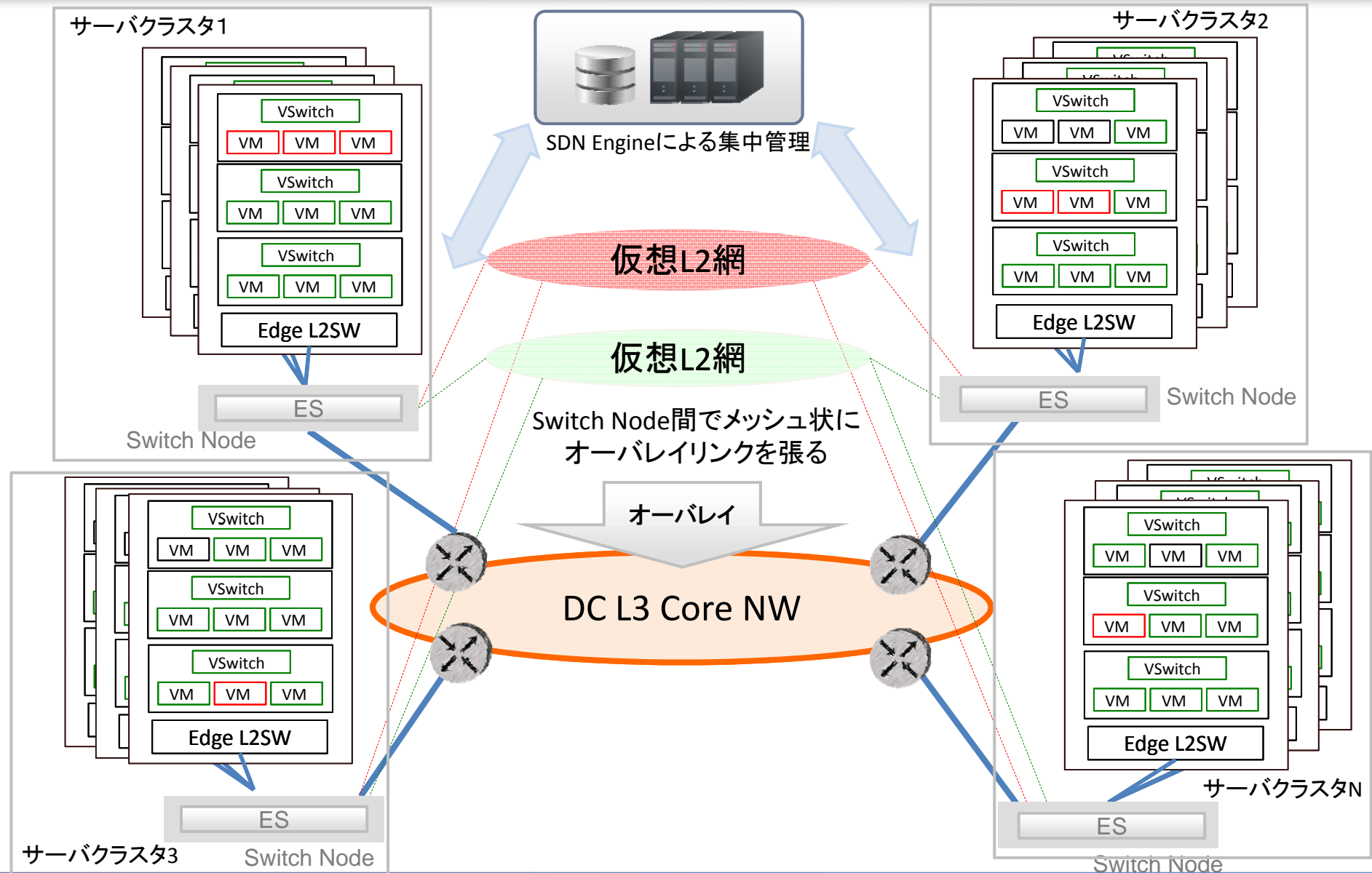
- Compute Node(仮想化サーバ)上で全ての処理を実施
- 追加のネットワーク機器が不要
- 対応Hyper Visor: KVM, ESXi

## ■ セパレートモード



- Compute NodeからSwitch Nodeを独立させ、スイッチ処理をオフロード
- 物理サーバの接続が可能
- HWアプライアンスによるハードウェア処理への拡張

# クラウド/DCへの適用（1 クラスタ = 1 VLANドメイン） Stratosphere



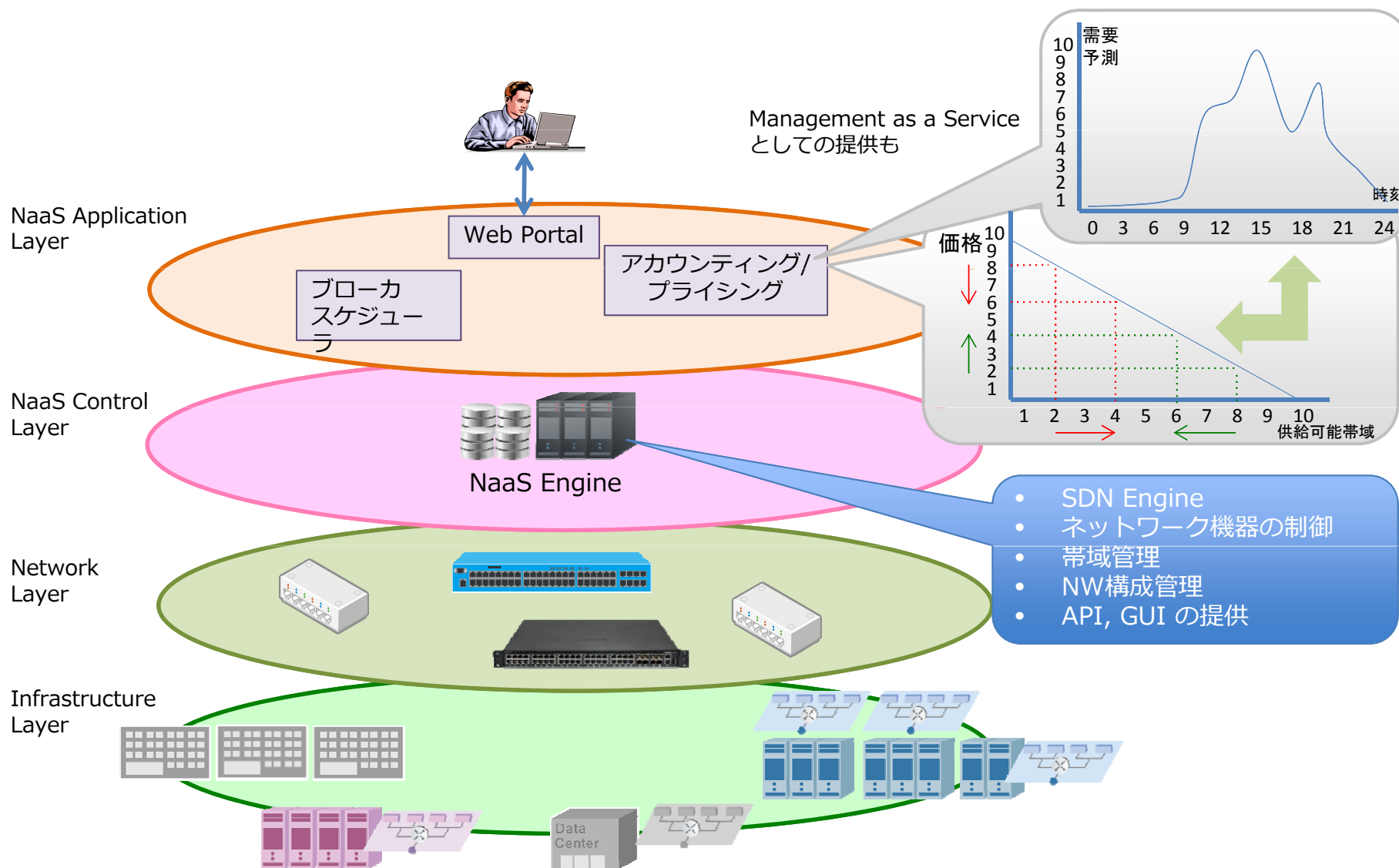
# ネットワークサービスプロバイダソリューション WAN/LANへの拡張とサービスの基盤化

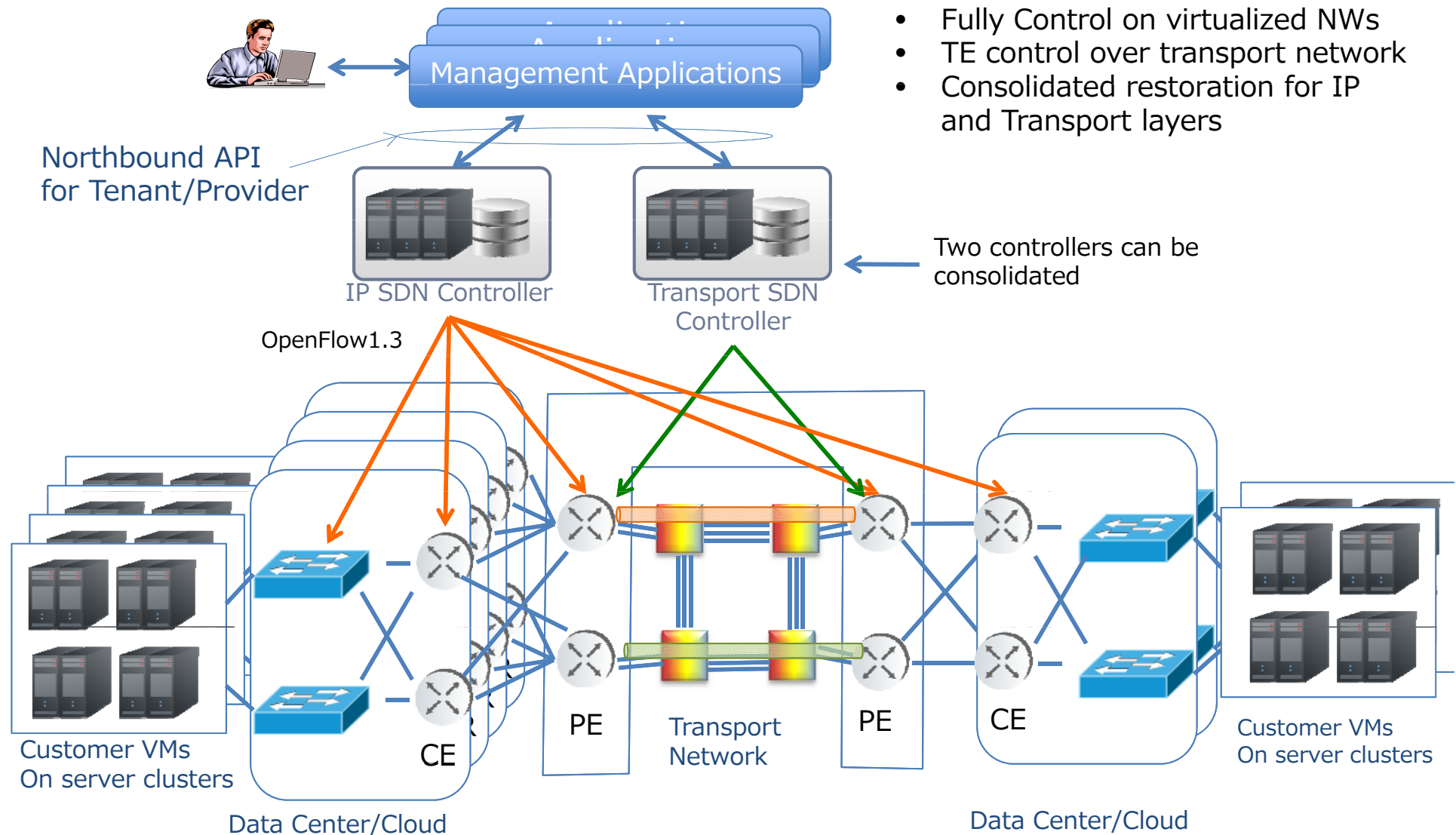


## Network as a Service (NaaS)

- 利用したいネットワーク機能を、**ユーザがソフトウェアからオンデマンドでプロビジョニング可能**とする
- ネットワークインフラが提供する高度なネットワーク機能を利用する**サービス基盤の提供**
  - 多様なネットワークインフラを対象とする
  - WAN, LANさまざまなインフラをまたぐ“スティッチング”
  - 階層化、プロテクション、帯域制御などキャリアインフラに求められる制御の実現
  - 複数回線/ポリシー制御も可能
  - ソフトウェアによるハードウェアの制御
- Cloud/DC, オフィス/家庭, WAN/モバイルなど様々な環境が対象
  - Cloud to Cloud, Cloud to Office, Cloud to Public
  - Office to Office, Office to Public
  - Public to Public

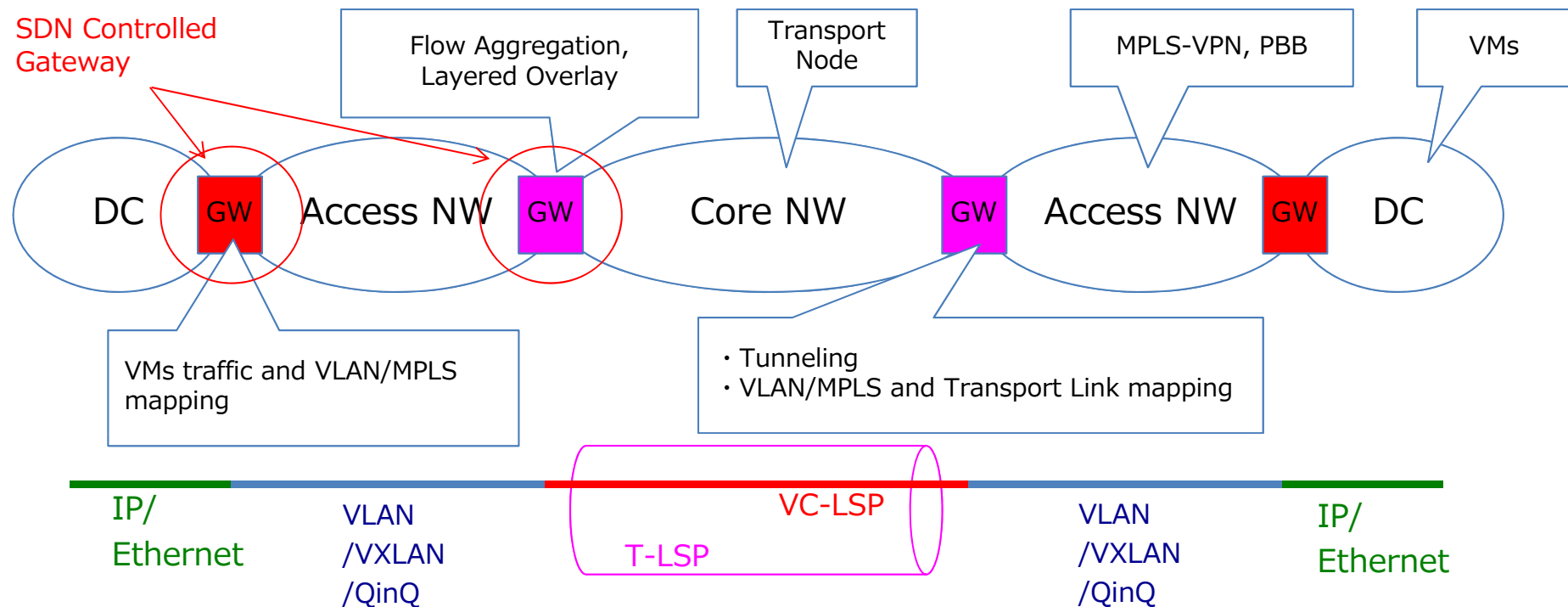
# NaaS イメージ





GWで物理レイヤとのマッピングを制御し、仮想ネットワークを繋いでいく

- DC-DC間に仮想 L2 回線を設定
- 回線のポリシー毎にグルーピング (VLAN等を活用)
- 放路制御は、VXLAN等のIPオーバーレイやLSP等で実装可能
- GWでのオーバーレイトラフィックの集約と階層化



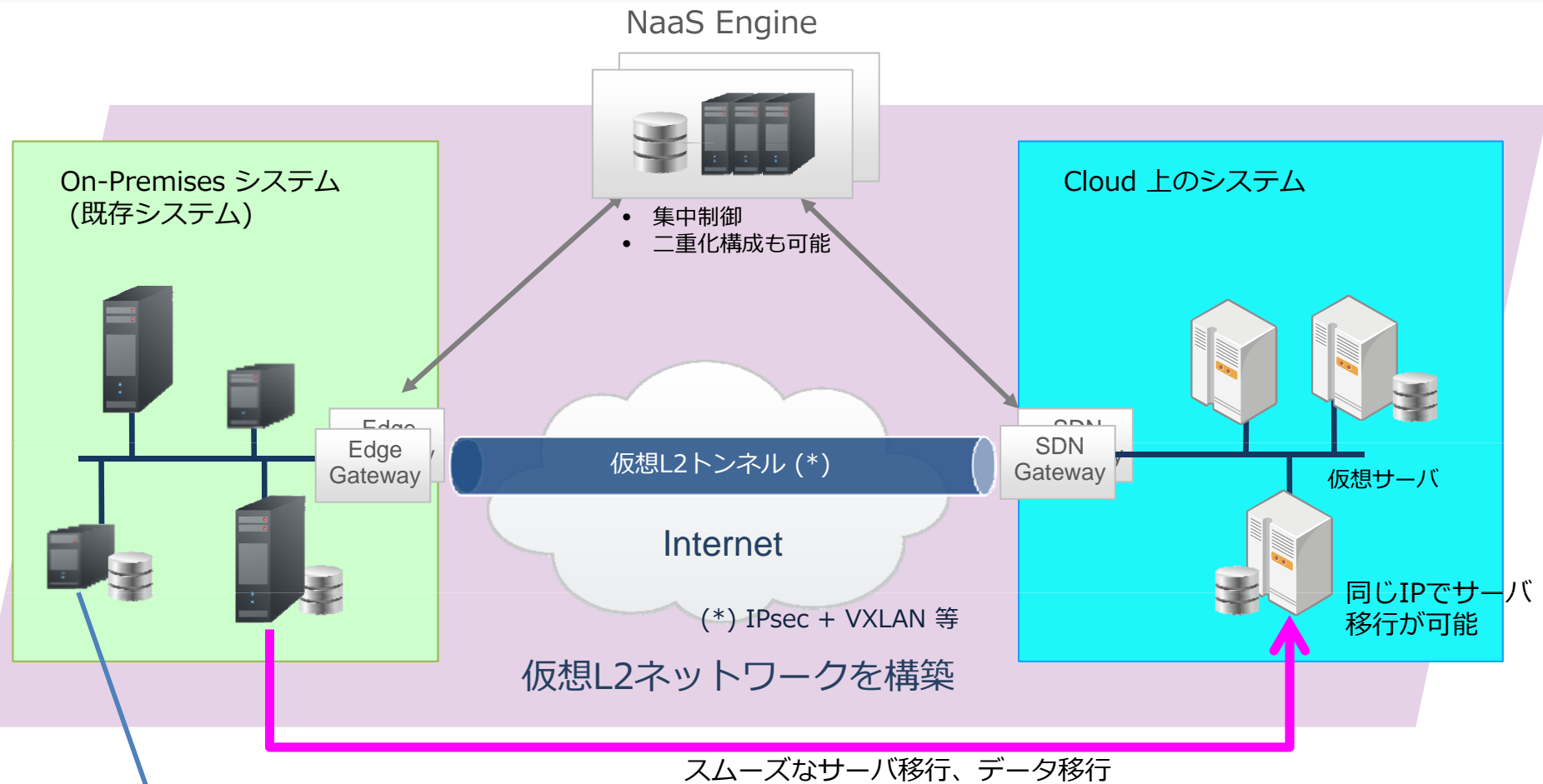
## Common Problems in ISP and Carrier

- 顧客のピークトラフィックが、特定時間に集中する
  - 明け方のストレージバックアップ等による集中
  - ピーク時にあわせた機器選択やネットワーク設計が必要
    - 裏を返せば、ピーク時以外は設備が空いてしまう
- ユーザニーズに応ずるための、煩雑な構成と運用
  - ユーザの Time to Service (TTS) 改善に応じきれていない
  - SDN技術等を使って運用方法は改善したいが、既存の設備はすぐには置き換えられない



## Stratosphere の NaaS で解決

- ピーク抑制とオフピーク活用
  - ユーザが使用時間を変更してくれやすいサービスを提供
  - リソース状況に応じた柔軟な構成変更
- ユーザ自身の簡単な操作によるネットワーク運用が可能
  - 時間帯指定によるネットワーク構成の動的な変更
  - ネットワーク毎に帯域指定も可能
- 既存のネットワーク機器とのスマートな連携、既存からのスマートな移行

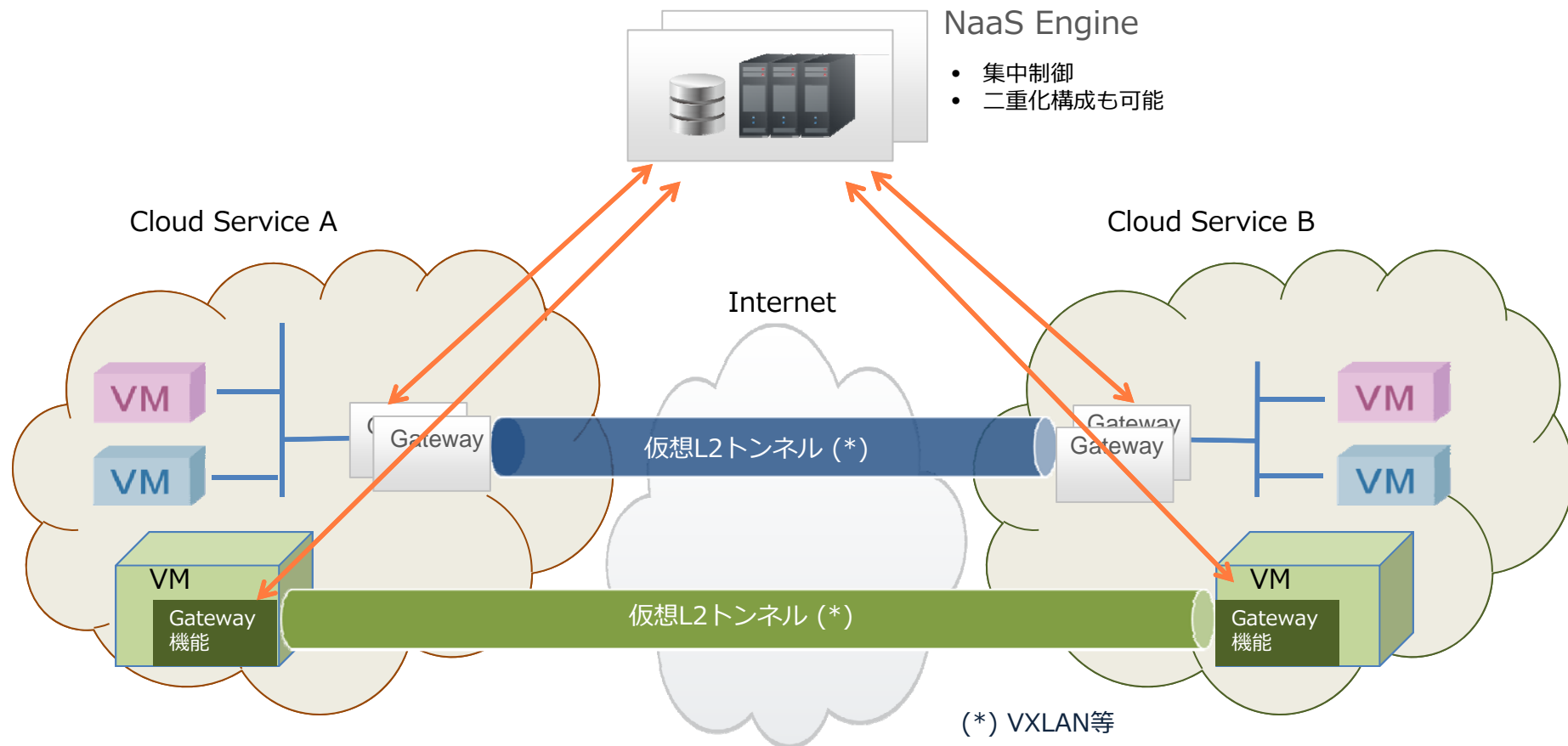


On-premises側に残さざるを得ないサーバ/サービスも、Cloud側とL2で接続可能

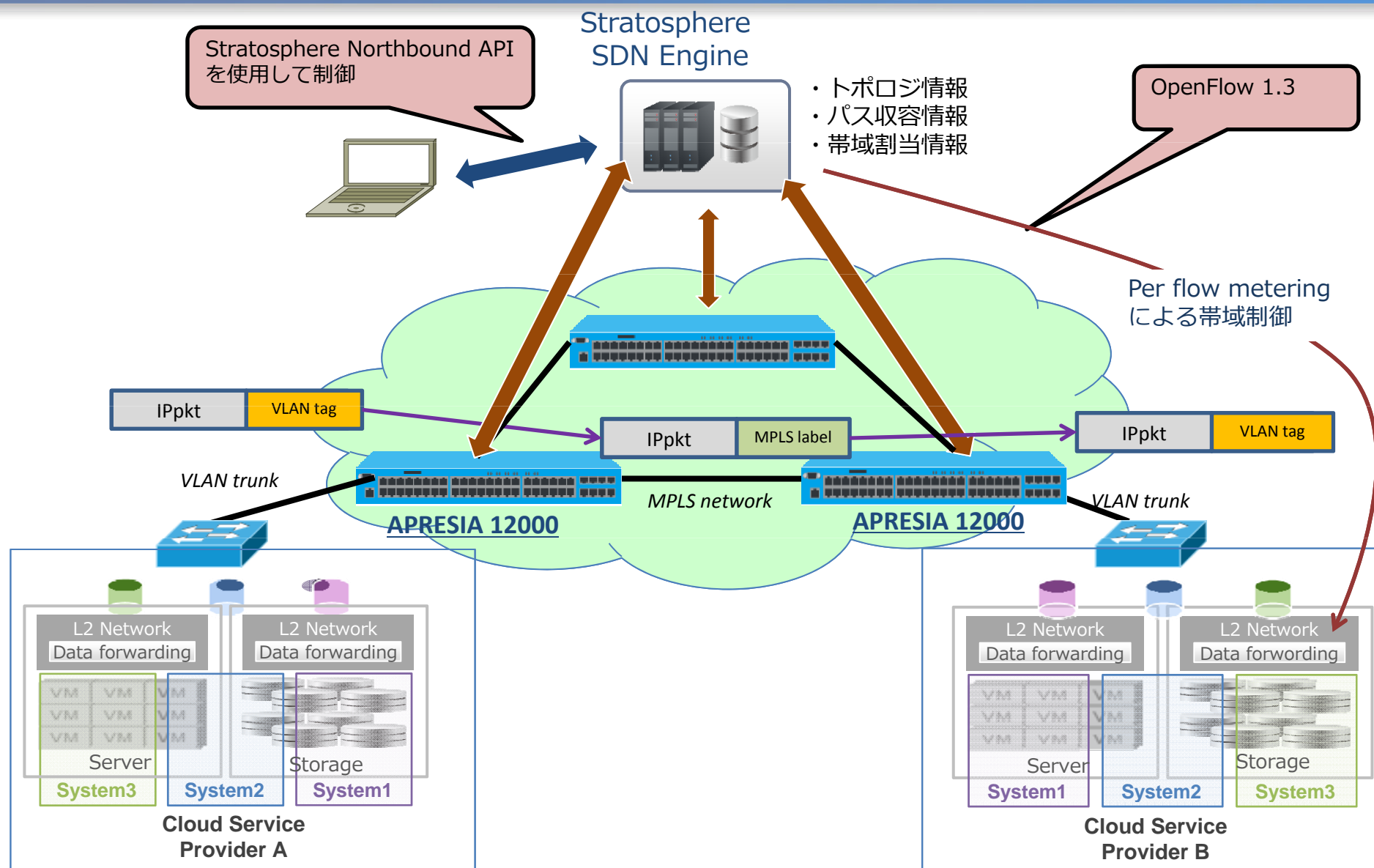
ユーザが意識すること無く、サービスの移行が可能

## Cloud 越しに VM 同士を L2 接続

- サービスのスケラビリティ向上
- クラウド間でのリソースの共有
- クラウド間でバックアップ構成も構築可能



# 異なるネットワーク間の接続 (NaaS 実装例)





# 仮想オフィスネットワーク OmniSphere

根本的な問題：  
組織変更やレイアウト変更のたびに繰り返されるネットワーク再設計と再構築

## 無線 LAN の課題

- AP 設置時には、電波干渉・電波強度を考慮する必要あり
  - ✓ マルチテナントビルの場合は調整は難しい
- ネットワーク構成を柔軟に変更できない
  - ✓ ネットワーク毎に AP (Access Point) 設置が必要
- 場所によって無線LANのSSIDを選ぶ必要がある
- 誰がアクセスしているかわからない
- ユーザへの帯域割当に不公平が生じることも
  - ✓ 特定端末が帯域を占有

## 有線 LAN の課題

- フロアレイアウトとパッチポートの調査
- 組織変更に合わせて仮想ネットワーク再構成
  - ✓ VLAN による部署毎、プロジェクト毎のネットワーク分離が基本。各フロアスイッチの再設定が必要
  - ✓ 規模が大きくなれば設定工数増大。設定ミスを誘発
- 変更前後のネットワーク規模に合う適切なスイッチ（MACやVLAN学習数など）選定の問題
  - ✓ 場合によっては、取り替えも

## 共通の課題

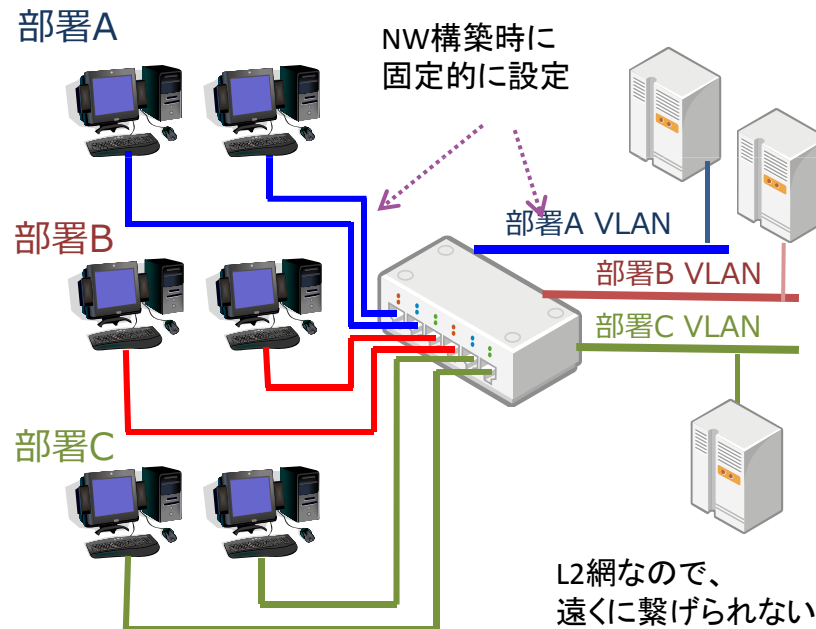
- 例えばオフィスでは、自席や所属部署サーバにアクセスするためにPCのネットワーク設定を変更する必要がある
- 場所（部屋、フロア、オフィス）を移動するとアドレスが変わる

## オフィスLAN で SDN

- スイッチポートとVLAN IDの対応管理による、端末のネットワークへの収容と、ネットワーク間のトラフィック分離ではなく、**仮想ネットワーク (VLANやVXLAN) 技術を用いた管理を実現**
  - ✓ ユーザは、PCを接続するスイッチやポートを意識する必要がない。接続箇所によるPC設定の変更も不要
  - ✓ シンプルなスイッチ構成と配線設計

### 従来:

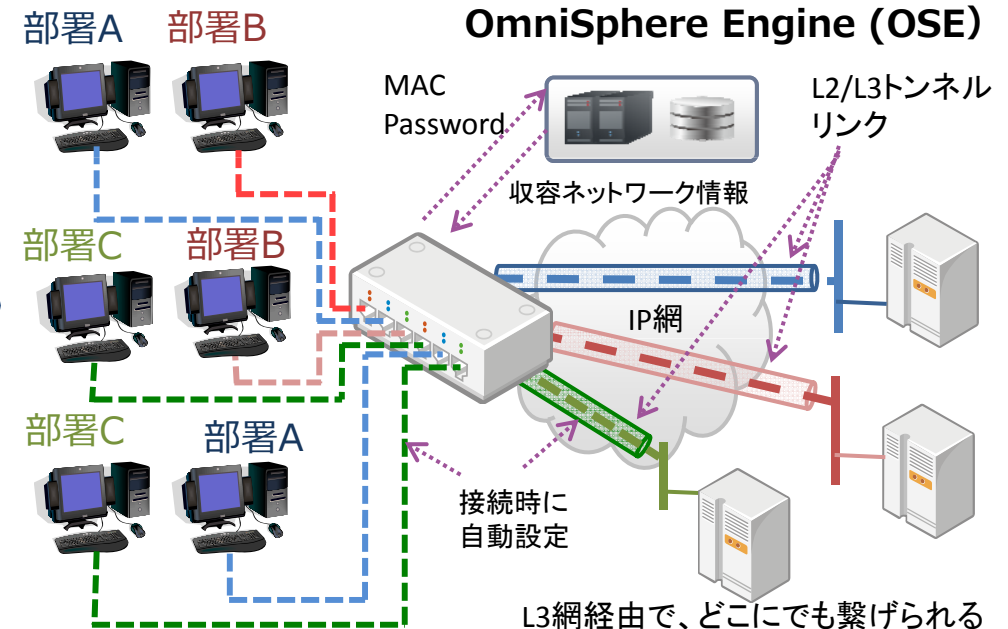
PCを接続するポートは予めVLANが設定されており、特定の部署のVLANにのみ接続される



- ユーザ端末のMAC address やユーザにより、L2/L3トンネルで繋ぐネットワークを自動設定する
  - ✓ 端末単位でトラフィックのフローを制御可能。QoSも
  - ✓ 接続箇所、接続ユーザを把握可能
  - ✓ 端末識別はMAC認証とユーザ認証(ユーザ名とパスワード) の、いずれか、もしくは両方
  - ✓ 検疫システムとの連動も
  - ✓ OpenFlowによる機器コントロール

### OmniWarp Wired:

PCが繋がれたポートは接続時に自動設定され、L2/L3トンネルで任意の場所に“ワープ”！



## 無線LAN もワープ！

- 従来のSSIDによるネットワーク分離／トラフィック分離ではなく、**仮想ネットワーク (VLANやVXLAN) による分離**

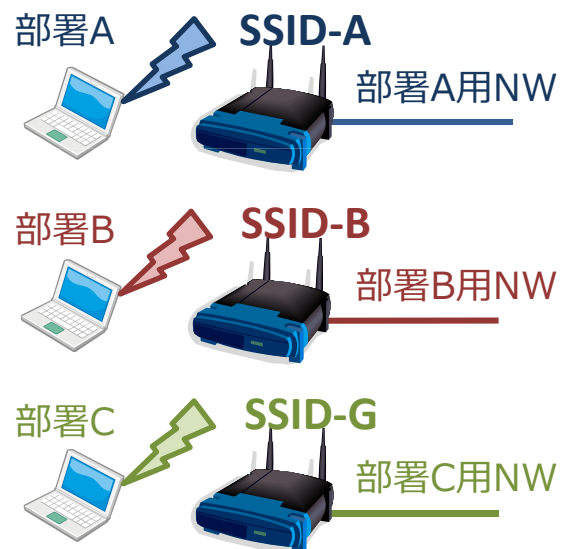
- ✓ ユーザは、接続先であるSSIDを区別する必要がない (1つのSSIDで構築可能)。接続箇所によるPC設定の変更は不要
- ✓ 自由度の高い無線AP配置設計
- ✓ 1つのSSIDで複数の仮想ネットワークをカバー

- ユーザ端末のMAC address やユーザにより、L2/L3トンネルで繋ぐネットワークを自動設定する

- ✓ 端末単位でトラフィックのフローを制御可能。QoSも
- ✓ 接続箇所、接続ユーザを把握可能
- ✓ 端末識別はMAC認証とユーザ認証(ユーザ名とパスワード) の、いずれか、もしくは両方
- ✓ 検疫システムとの連動も
- ✓ OpenFlowによる機器コントロール

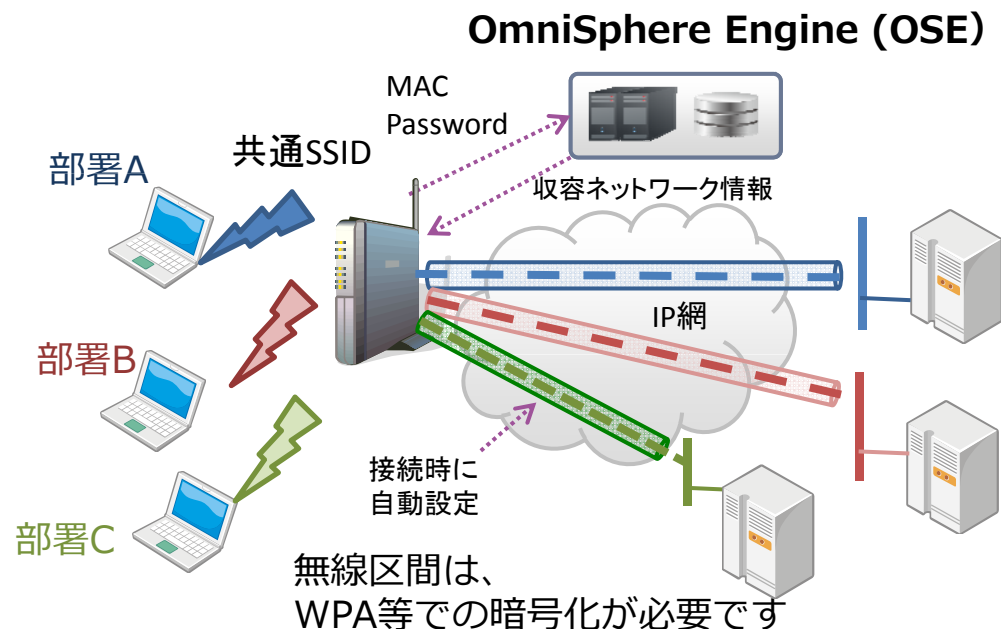
### 従来:

部署NW毎に SSID が必要



### OmniWarp Air:

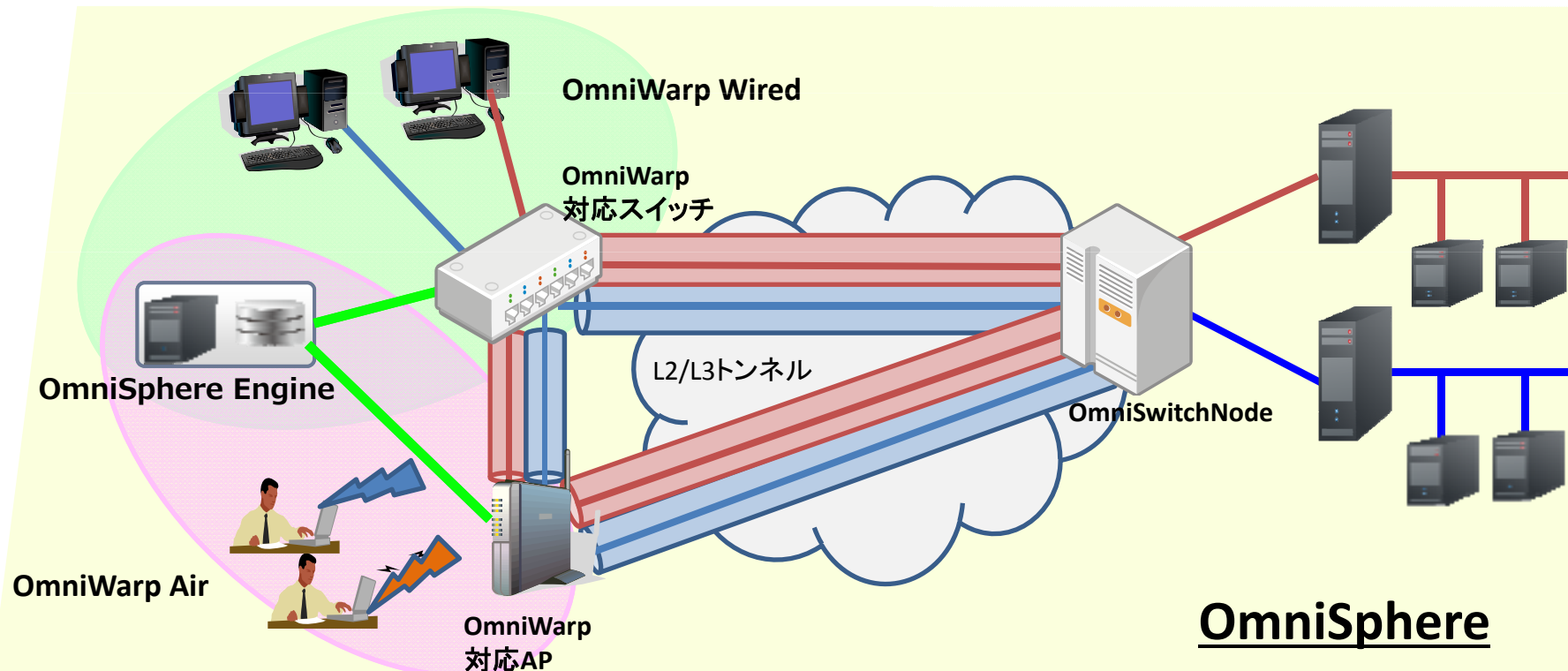
一つの SSID で全ての部署のNWを管理

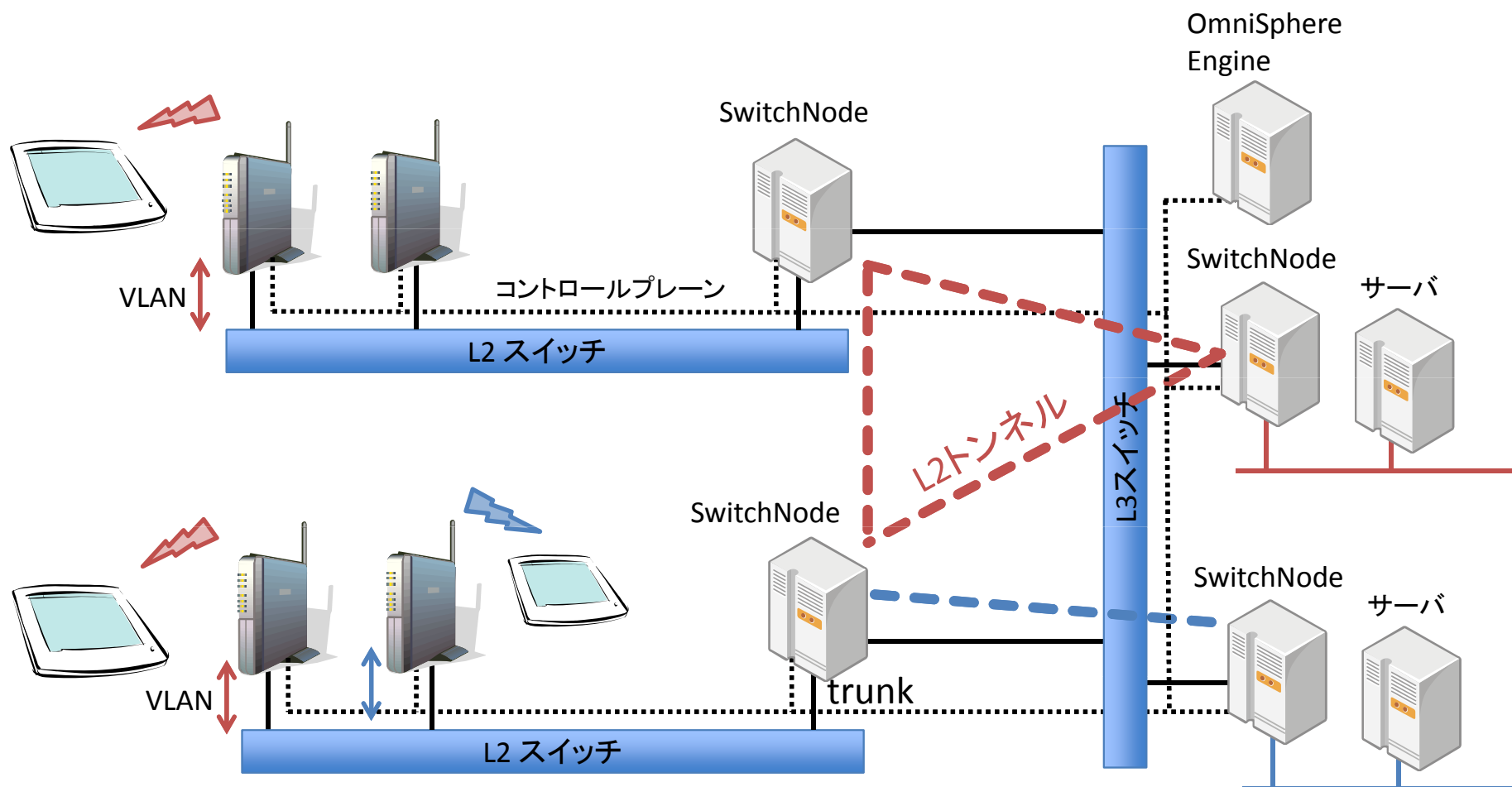


## SDN 技術による 仮想L2ネットワーク

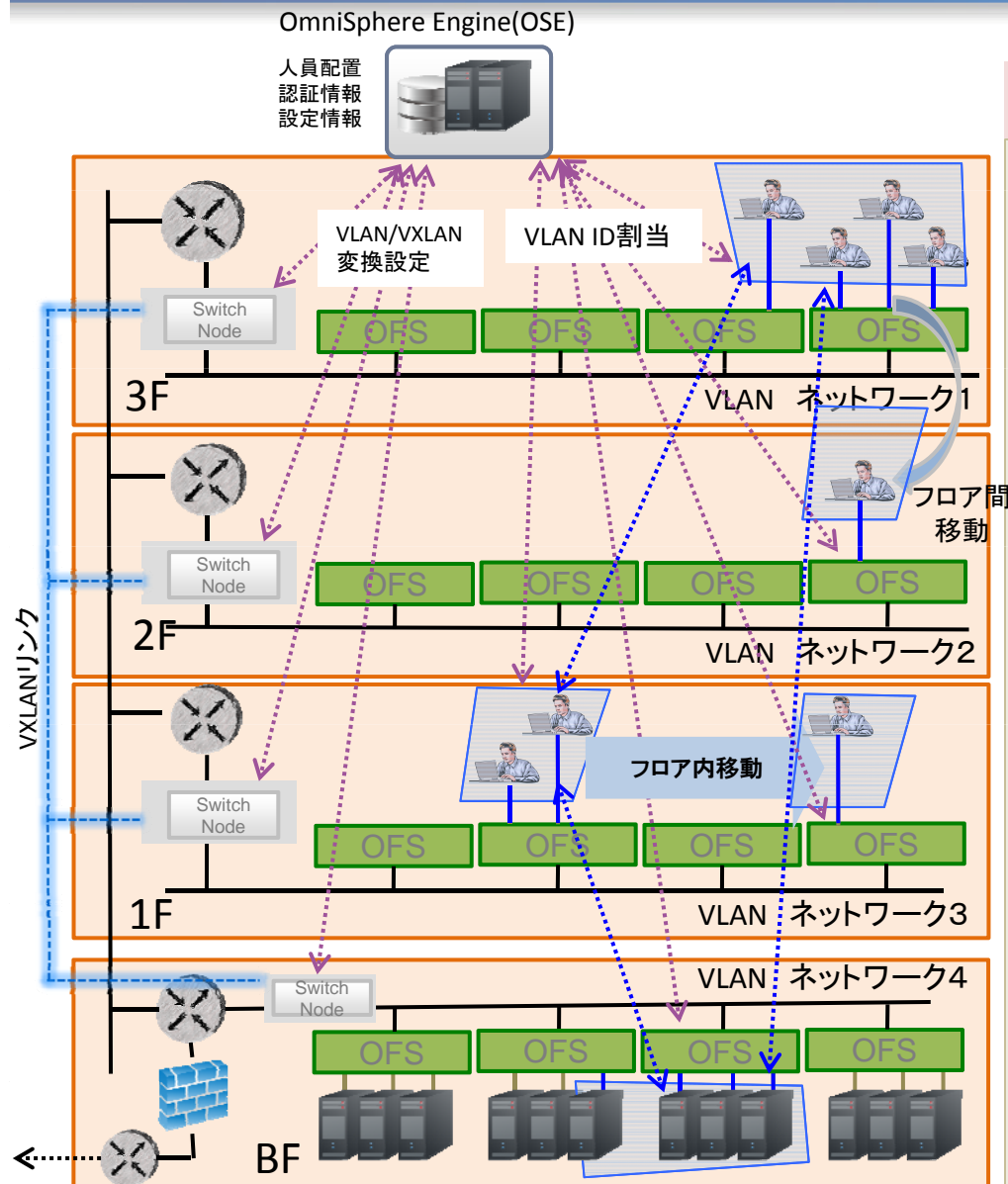
- 物理ネットワーク上に仮想L2ネットワークを構築
- AP - スイッチ間は **L3 接続**
  - ✓ 離れたネットワークとの接続も容易に
- ユーザ通信は **L2/L3 トンネル** で
  - ✓ ユーザはいままで通りに容易に使用可能
- ネットワーク毎の無線 AP 設置が不要
- **ユーザ側に追加アプリをインストールする必要無し**
- **ユーザ側のデバイス、OSは不問**

- ユーザ端末のMAC address と 仮想ネットワーク (VLAN, VXLAN等) を紐付ける
  - ✓ 端末単位でトラフィックのフローを制御可能。QoSも
  - ✓ 接続箇所、接続ユーザを把握可能
  - ✓ 端末識別はMAC認証とユーザ認証(ユーザ名とパスワード) の、いずれか、もしくは両方
  - ✓ 検疫システムとの連動も
  - ✓ OpenFlowによる機器コントロール





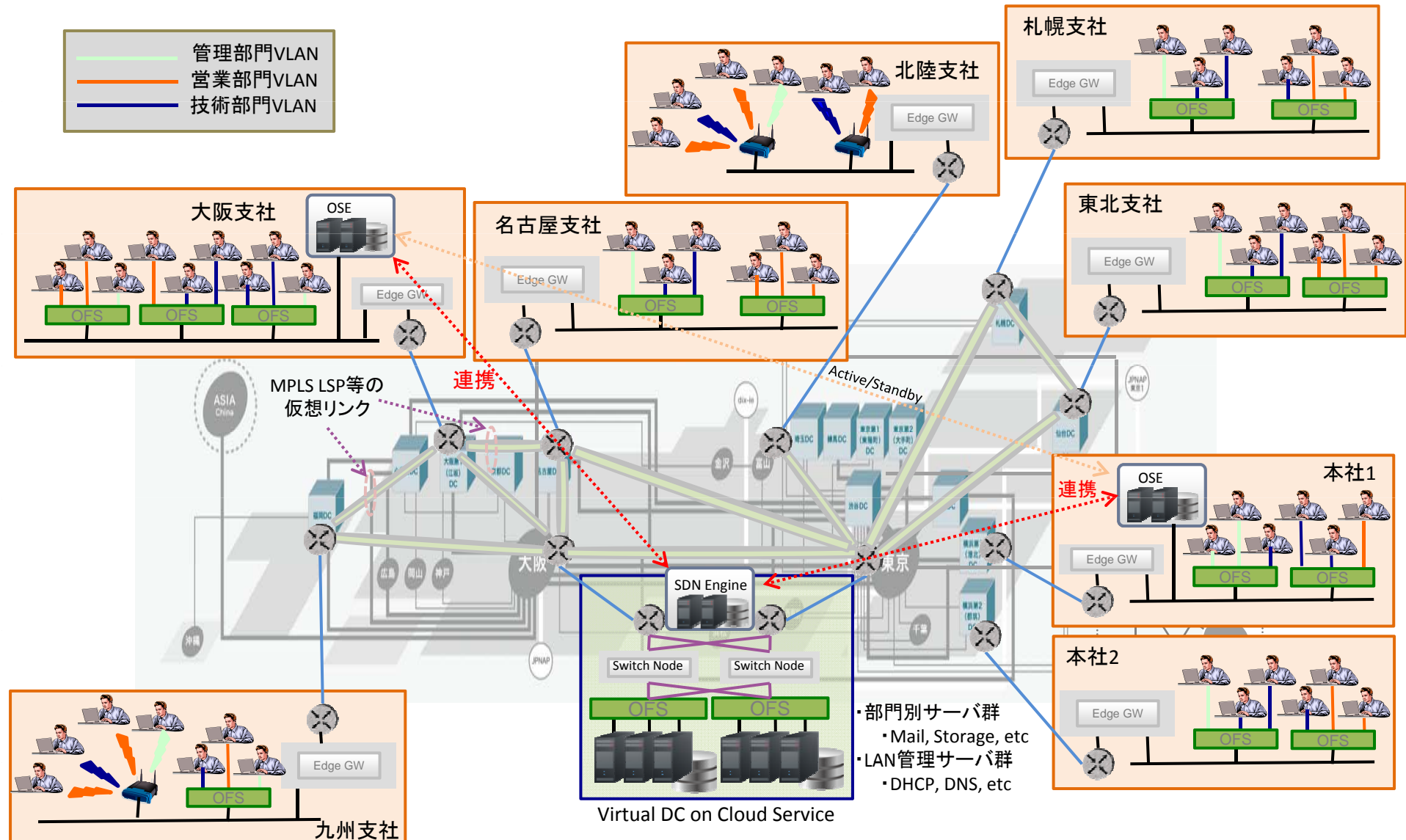




## オフィスビルネットワーク管理の例

- シンプルな構成で物理ネットワークを構築
  - フロア間はルータ経由でL3接続
  - 各フロア内をL2で構成。部署毎にVLANを切る
  - Omni Switch Nodeで各フロアのVLAN同士をオーバレイ接続
    - L2とL3の境界は任意に設定可能
- 論理ネットワークは、物理ネットワーク構成とは独立に、オーバレイネットワークで構築
  - 物理ポートに接続したユーザを、どのVLANに接続するかは、OmniSphere Engine(OSE)が集中管理
    - MAC認証／パスワード認証で、自動的に繋いだポートのVLAN IDを設定
    - Omni Switch Nodeで各フロアのVLAN IDとVXLAN IDを自動変換
    - フロア内、フロア間の人員移動にも自動対応
      - スイッチポートへのVLAN IDの設定の変更
      - Omni Switch NodeのVLAN/VXLAN変換設定の変更
  - サーバ室に部門別のDHCPサーバを設置しておけば、ユーザの端末には常に同じ設定が可能
- OFSとOmni Switch NodeはOSEが自動設定
  - SW設定の簡略化
    - 基本的に同じ設定で全てのSWを管理可能
  - SW設定のロジックをOSEに集約
    - 設定変更時の変更箇所はひとつだけ

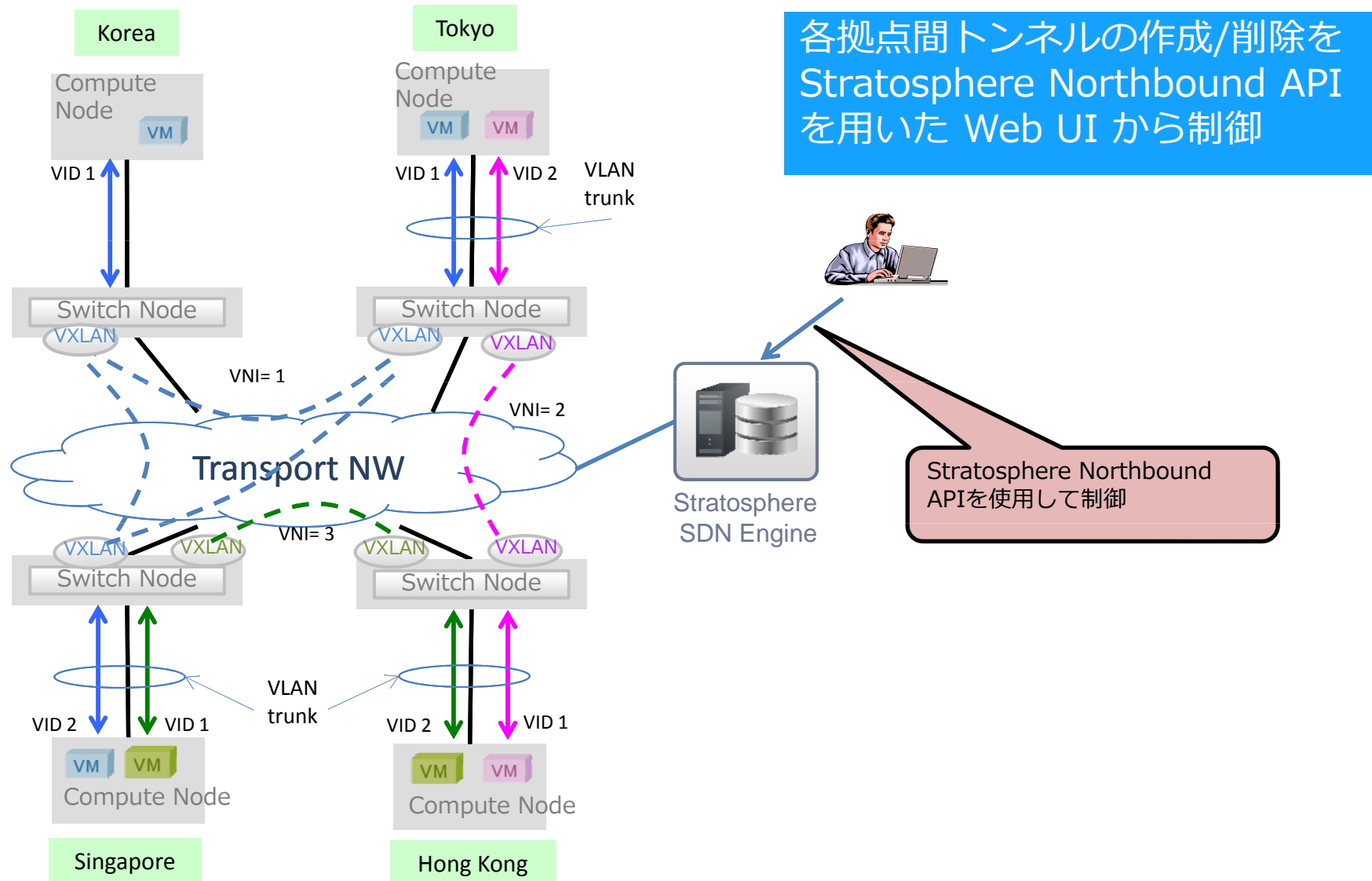
# Cloud + SDNによるVirtual IT 未来イメージ





# NaaS デモ

## OmniSphere デモ



1. デバイス(MAC)情報とアカウント情報をOmniSphereEngineに登録
2. 初めて Wifi 接続したデバイスは隔離セグメントに接続
3. MACとアカウントによる認証
4. 紐付けられたセグメントに再接続

