変える力を、ともに生み出す。
NTT DATAグループ

クラウド時代の新ネットワークアーキテクチャ

株式会社NTTデータ
ビジネスソリューション事業本部　ネットワークソリューションBU　課長　馬場 達也
技術開発本部　ITアーキテクチャソリューションセンタ　部長　磯部 俊洋

本日の講演でお伝えしたいこと

1. これからのクラウドには、ネットワークの仮想化と運用自動化の技術が重要となってきます。

2. ネットワーク仮想化と運用自動化を実現する技術として、「仮想アプライアンス」と「OpenFlow」が有効です。

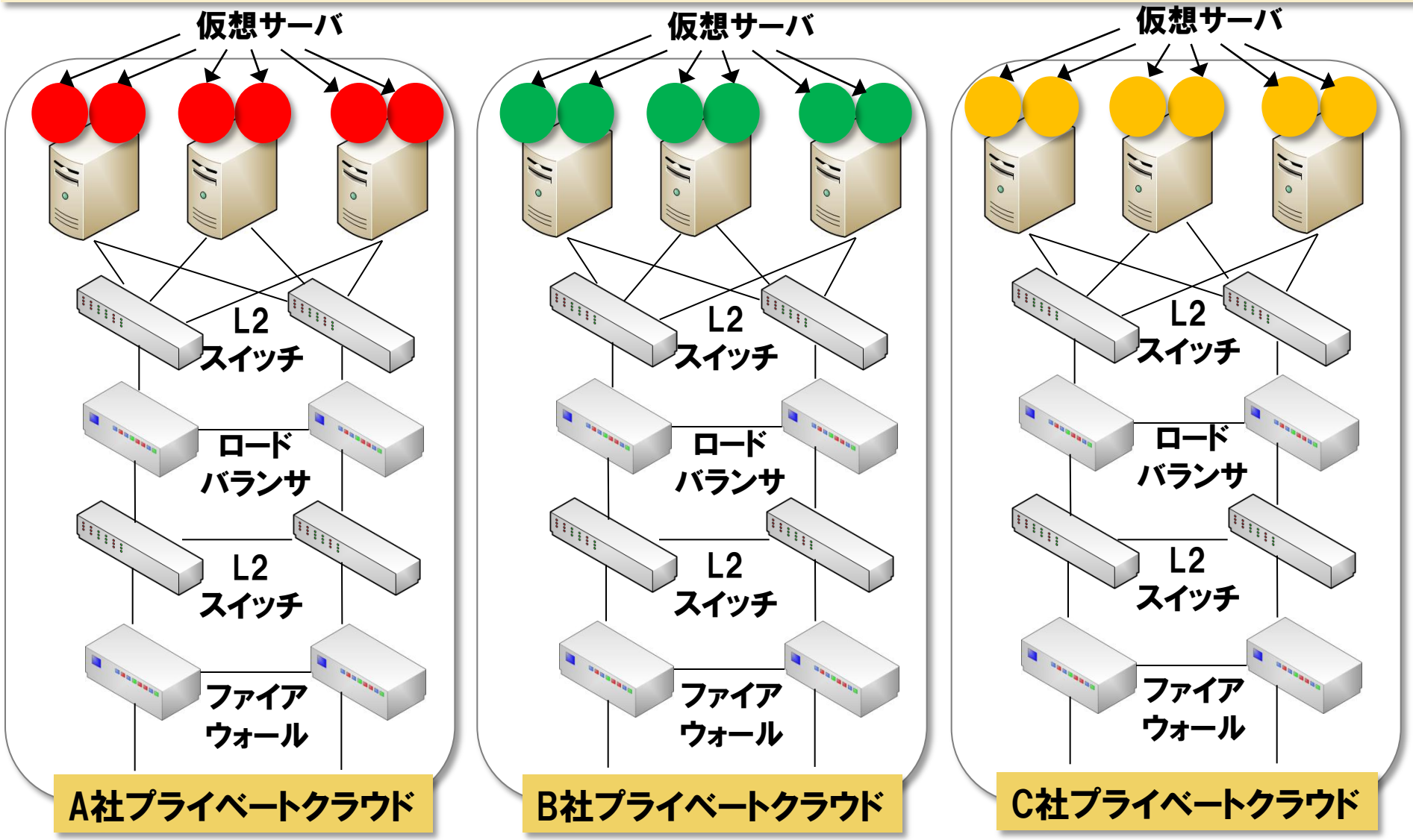
3. 「仮想アプライアンス」と「OpenFlow」を活用したクラウド環境の運用自動化の例を紹介します。

仮想プライベートクラウドとネットワーク仮想化
～Datacenter as a Serviceの時代へ～

サーバ仮想化によるプライベートクラウドの構築

変える力を、ともに生み出す。
NTT DATAグループ

プライベートクラウドでは、サーバ仮想化により物理サーバ台数を削減



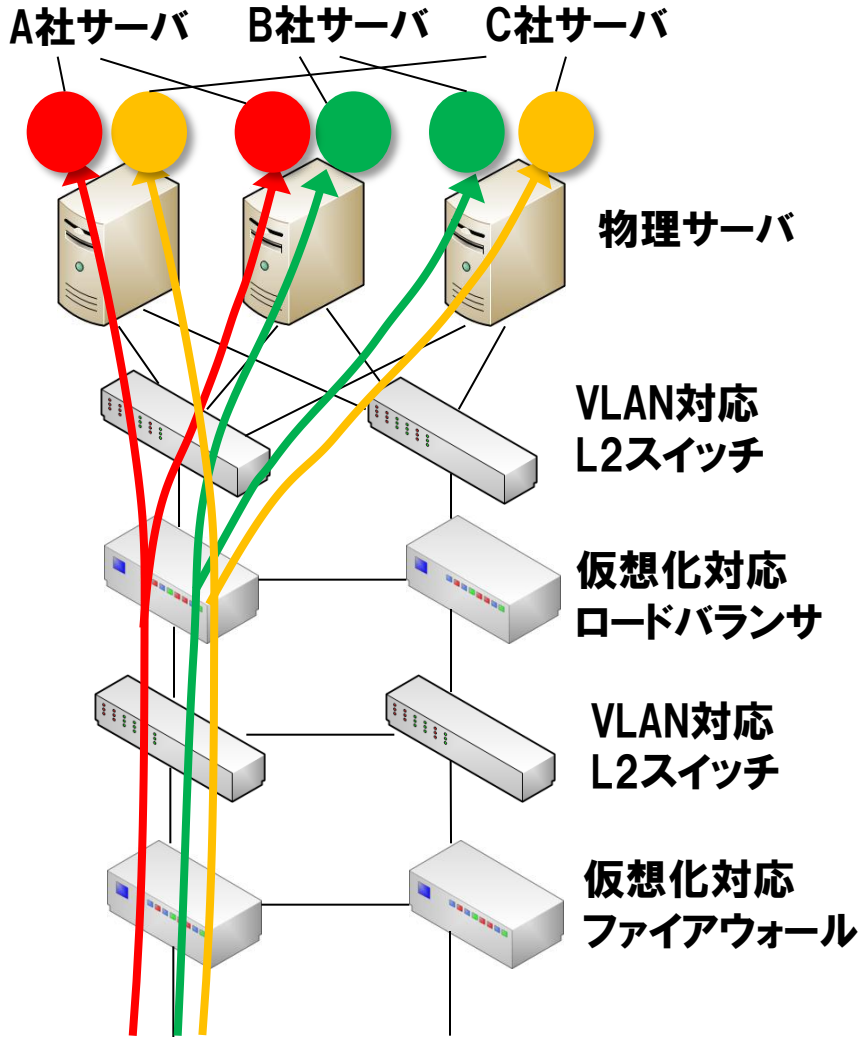
「仮想プライベートクラウド」の実現

仮想プライベートクラウドでは、サーバ仮想化、ストレージ仮想化に加えて、ネットワーク仮想化が重要となる

サーバだけでなく、データセンタ、ネットワークを他社と共有することにより、さらにコスト削減

同じ物理サーバに異なる企業の仮想サーバを相乗りさせることにより、さらにリソースを効率利用

ネットワークはレイヤ2レベルで論理分割することにより、セキュリティレベルを保持/IPアドレスの重複を許可



これからのクラウド基盤を支える ネットワークの要件

クラウド環境におけるネットワークの背景

変える力を、ともに生み出す。
NTT DATAグループ

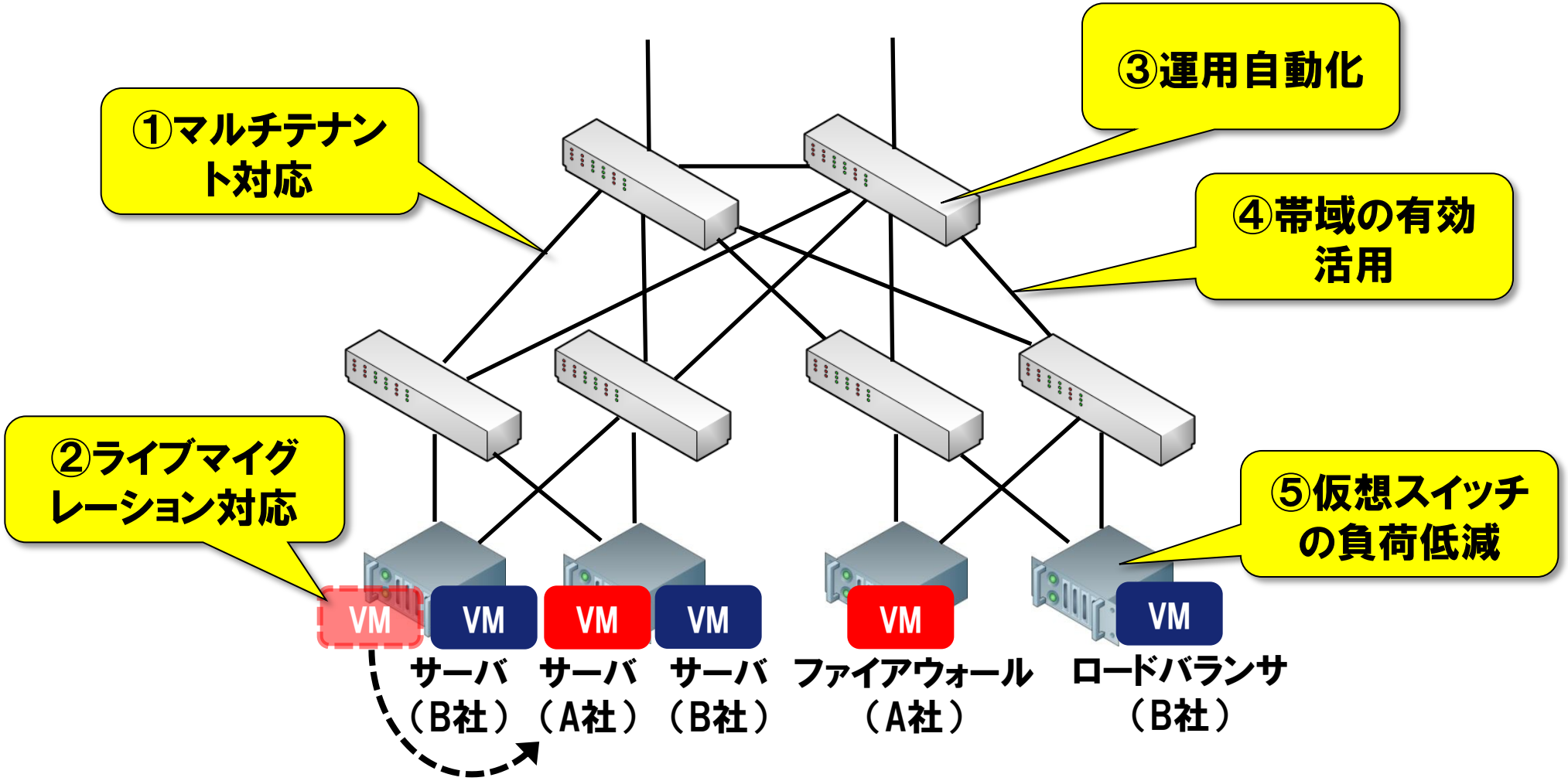
「サーバ統合」から「データセンタ統合」へと進むにつれ、ネットワーク側の対応が重要となってきた

- サーバ統合だけでなく、データセンタ統合のニーズが高まり、**ネットワーク構成を変更することなく、インフラを統合**する必要が出てきた
- 仮想サーバのライブマイグレーションが活用されるようになり、移動しても同じネットワークに所属させるために、移動に合わせて**VLAN設定を変更**する必要が出てきた
- ネットワークの管理が複雑化し、**運用の自動化**が必要となってきた
- サーバ間トラフィックが増加し、帯域を太くするだけでなく、使用していない**帯域を有効活用**する必要が出てきた
- 仮想サーバの集積度が上がるにつれ、ハイパーバイザや**仮想スイッチのCPUオーバーヘッド**がネックになってきた

クラウド基盤を支えるネットワークに対する5つの要件

変える力を、ともに生み出す。
NTT DATAグループ

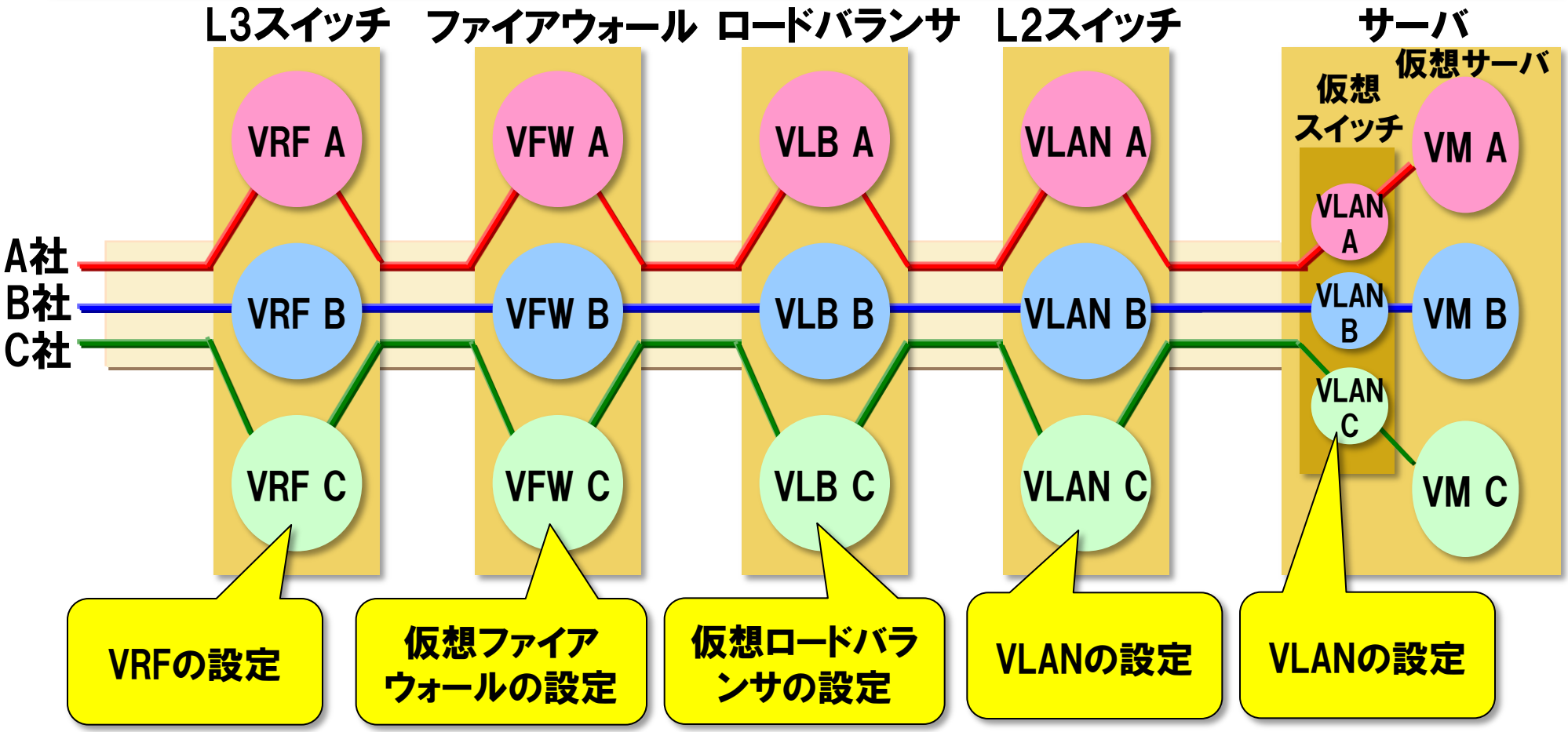
サーバ仮想化技術の普及によって、データセンタネットワークに求められる要件が急激に変化してきている



要件① マルチテナント対応

変える力を、ともに生み出す。
NTT DATAグループ

- クラウド環境では、複数のネットワークを仮想化する必要がある
- 従来のVLANなどの技術では、構成をテナント間で揃える必要がある



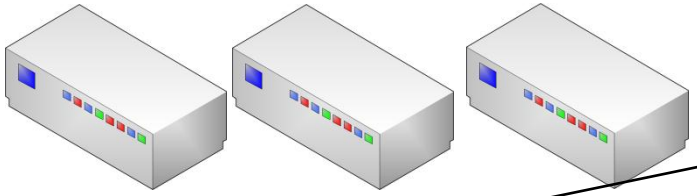
VRF(Virtual Routing and Forwarding)　VLAN(Virtual Local Area Network)
VFW(Virtual Firewall)　VLB(Virtual Load Balancer)　VM(Virtual Machine)

仮想アプライアンスによるネットワーク機器の仮想化

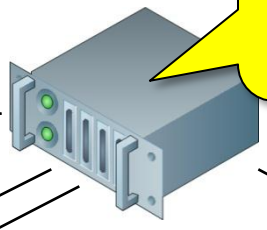
変える力を、ともに生み出す。
NTT DATAグループ

**ハイパーバイザの普及により、従来、専用ハードウェアで動作していた
ネットワーク機器がIAサーバの仮想化環境上で動作**

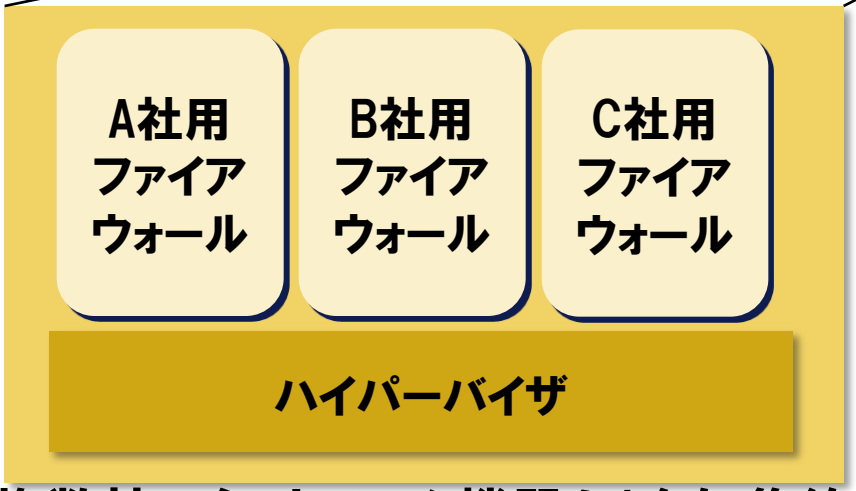
ファイアウォール、IPS、ロードバランサ、WAFなどの
ネットワーク機器



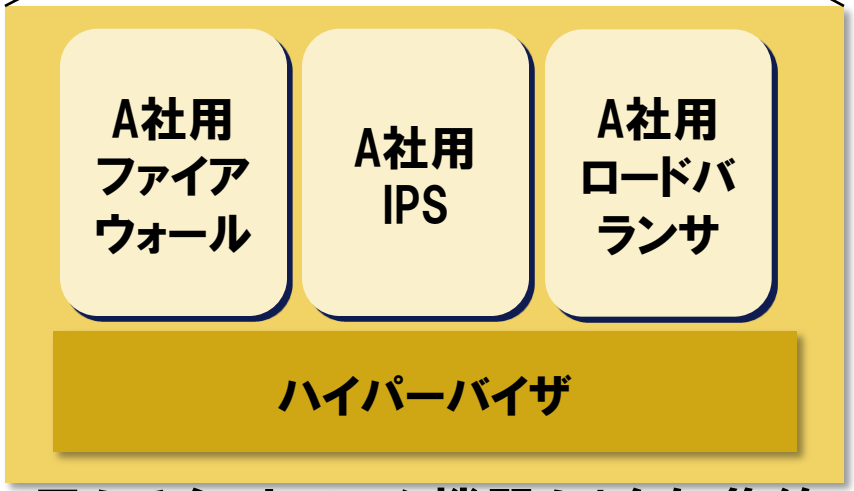
IAサーバ



ハードウェアの共有により、ハードウェアコスト/スペースを削減



複数社のネットワーク機器を1台に集約



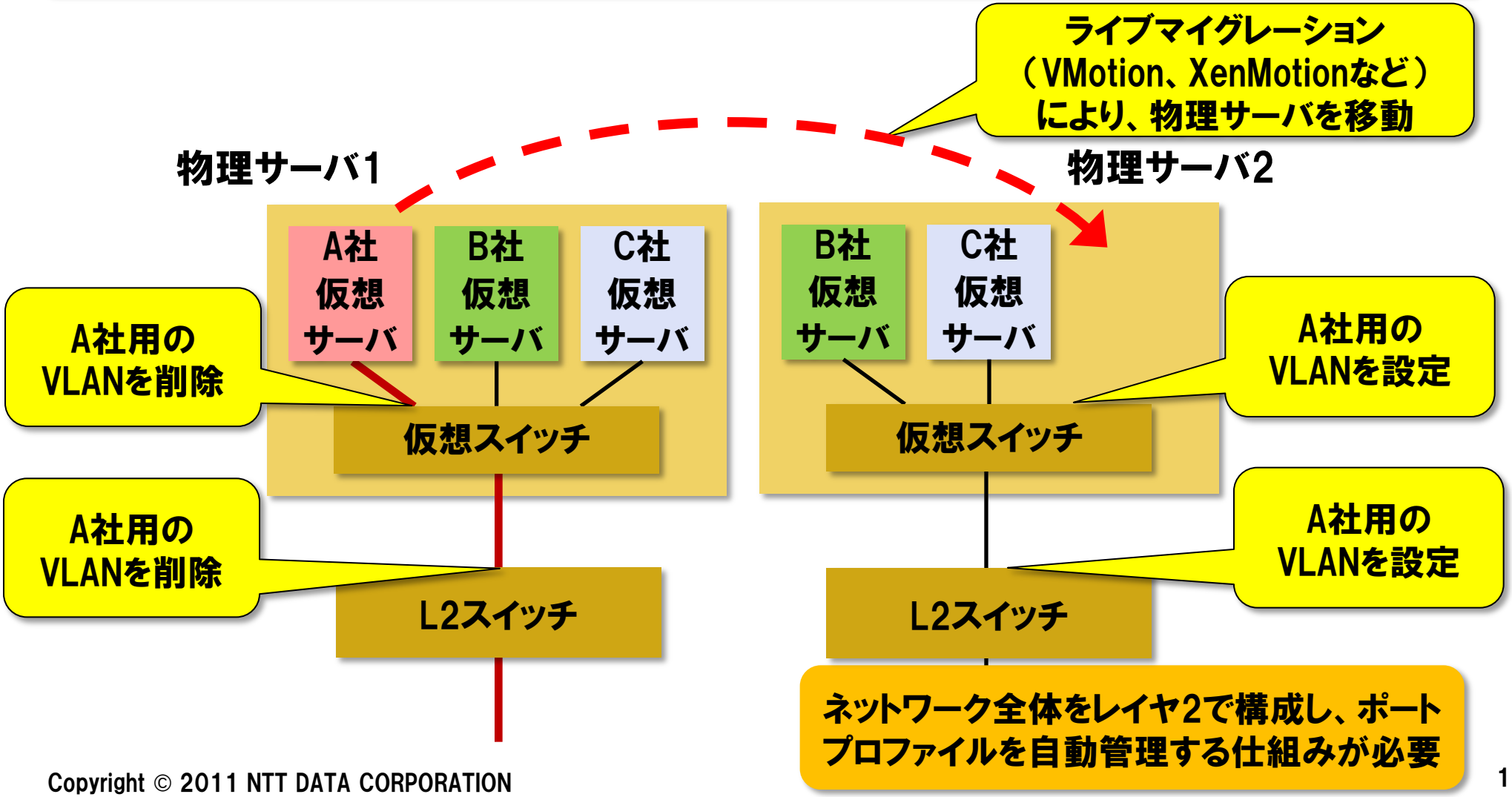
異なるネットワーク機器を1台に集約

IPS:Intrusion Prevention System　WAF:Web Application Firewall

要件② ライブマイグレーション対応

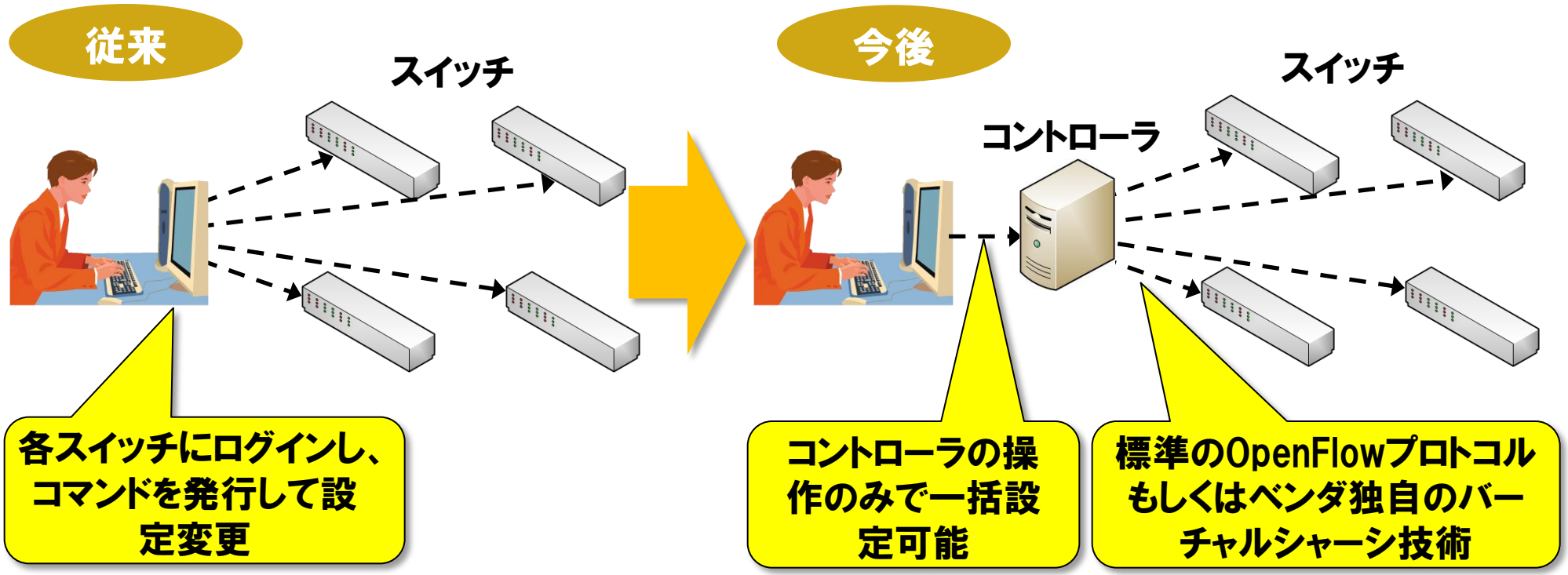
変える力を、ともに生み出す。
NTT DATAグループ

- 仮想サーバは、移動しても同じセグメントに所属させる必要がある
- ポートプロファイル(VLAN、QoS、ACLなど)を付け替える必要がある



要件③ 運用自動化

これまでの技術では、ネットワーク機器毎にベンダ固有のコマンドを使用して設定を行う必要があったため、自動化が難しい

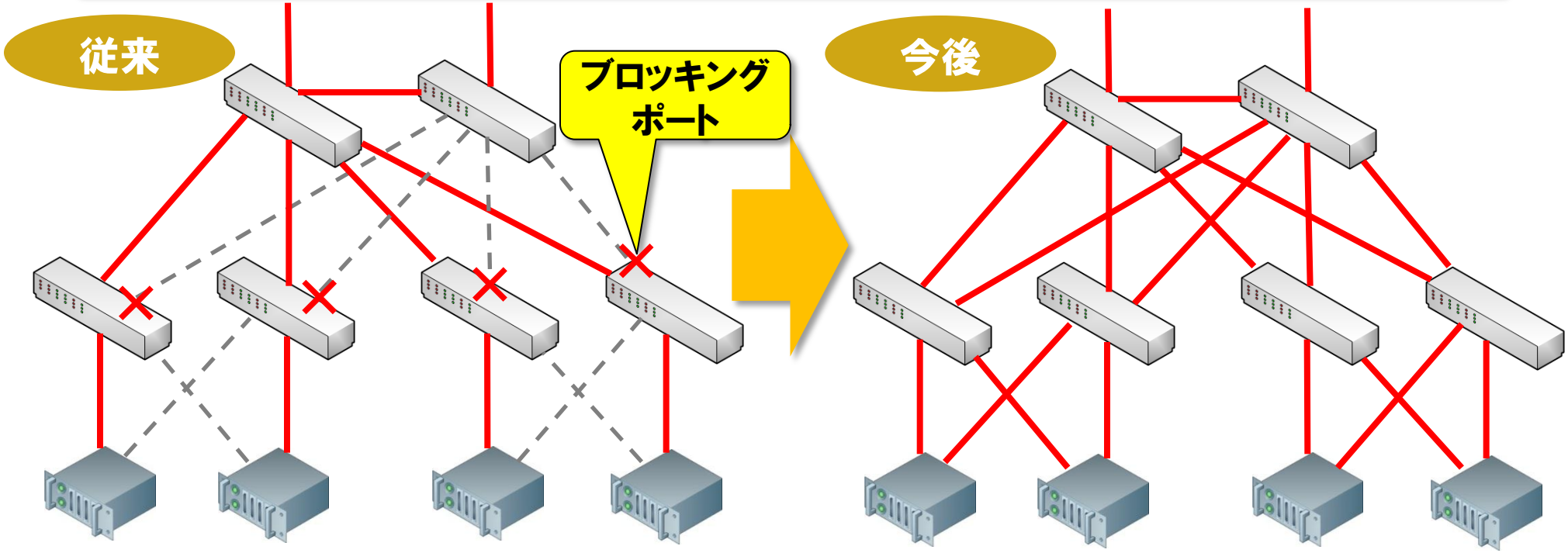


- ネットワーク機器毎に設定が必要
- 機種によって設定方法が異なる
  ⇒ 自動化が難しい

- 複数台のスイッチを1台のように管理
- OpenFlowはマルチベンダ対応可能
  ⇒ 自動化が容易に

要件④ 帯域の有効活用

クラウド環境では、サーバ集約が進むと同時に、サーバ間トラフィックが増大するため、より広帯域な環境が必要



従来のSTP(スパニングツリー)では、ブロッキングポートによってすべてのリンクを同時に利用できない

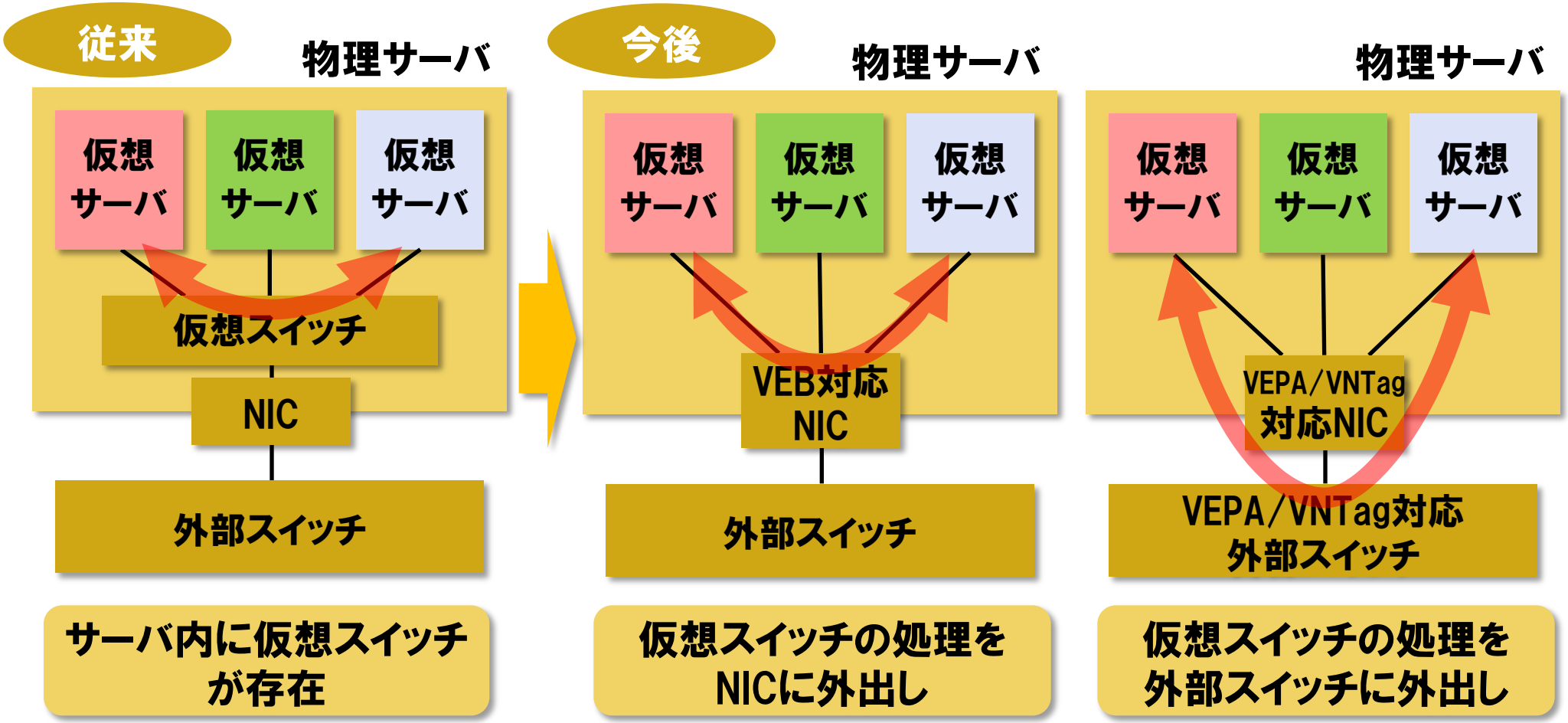
TRILL、SPB、MLAG、OpenFlowなどの技術により、すべてのリンクをアクティブ状態にして帯域を有効利用可能

STP:Spanning Tree Protocol　TRILL:TRansparent Interconnection of Lots of Links
SPB:Shortest Path Bridging　MLAG:Multi-chassis Link AGgregation

要件⑤ 仮想スイッチの負荷低減

変える力を、ともに生み出す。
NTT DATAグループ

- 仮想スイッチのCPUオーバーヘッドがサーバのリソースを圧迫
  - 仮想スイッチを誰が管理するのかという問題も存在



サーバ内に仮想スイッチが存在

仮想スイッチの処理をNICに外出し

仮想スイッチの処理を外部スイッチに外出し

VEB：Virtual Ethernet Bridge　VEPA：Virtual Ethernet Port Aggregator　VNTag：Virtual Network Tag

これからのクラウド基盤を支える
新ネットワークアーキテクチャ

「OpenFlowベース」vs.「VLANベース」

今後のデータセンタネットワークのアーキテクチャは、
「OpenFlowベース」か「VLANベース」かの選択になる

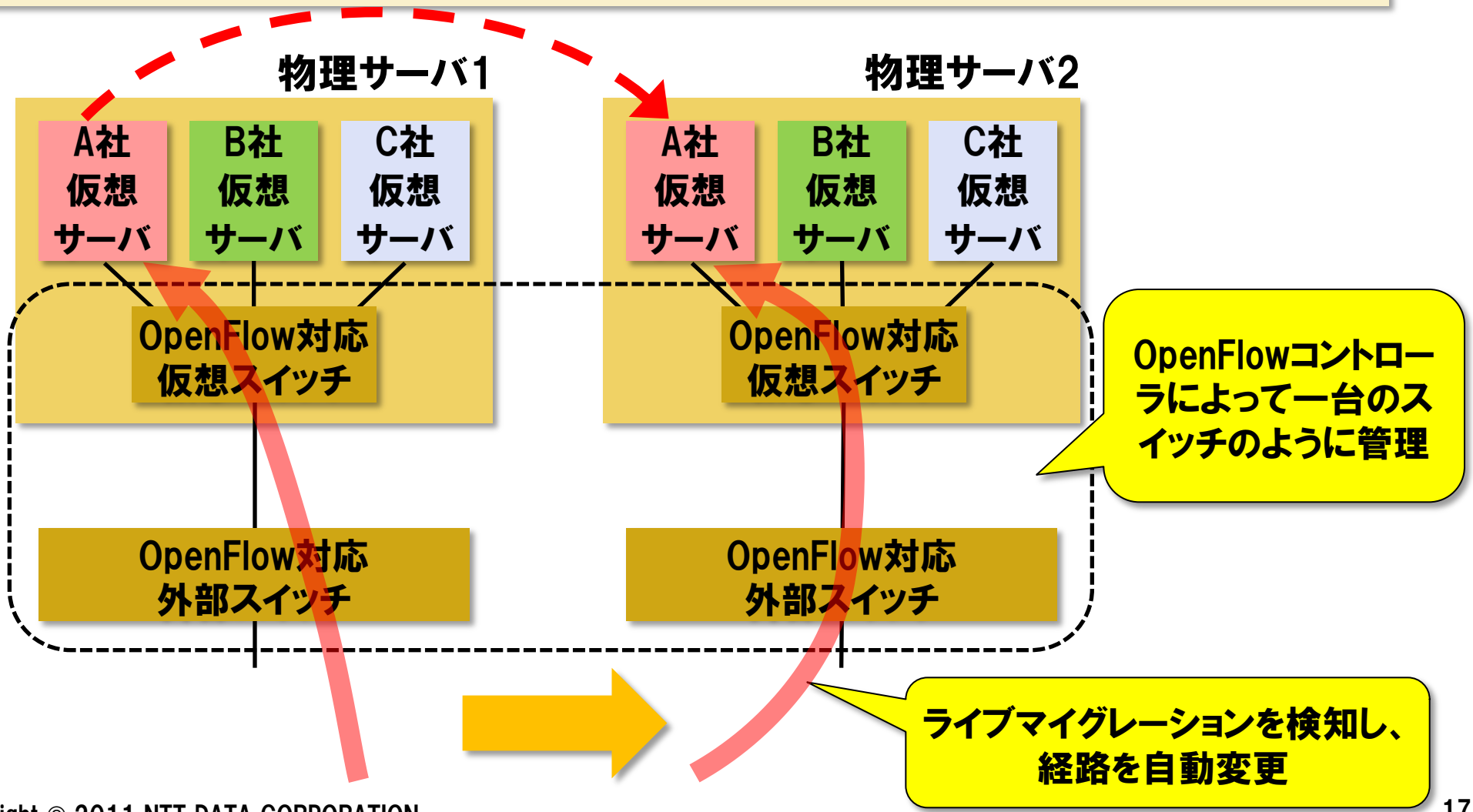
ネットワークに対する要件	OpenFlowベース	VLANベース
マルチテナント対応	OpenFlow ＋ 仮想アプライアンス	VLAN ／ VXLAN ／ NVGRE ＋ 仮想アプライアンス
ライブマイグレーション対応		VEPA ／ VNTag ＋バーチャルシャーシ ＋ポートプロファイル自動管理
運用自動化		バーチャルシャーシ ＋ 仮想アプライアンス
帯域の有効活用		TRILL ／ SPB ／ MLAG
仮想スイッチの負荷低減	VEPA	VEPA ／ VNTag

VXLAN：Virtual Extensible Local Area Network
NVGRE: Network Virtualization using Generic Routing Encapsulation

ライブマイグレーション対応の例（OpenFlowベース）

変える力を、ともに生み出す。
NTT DATAグループ

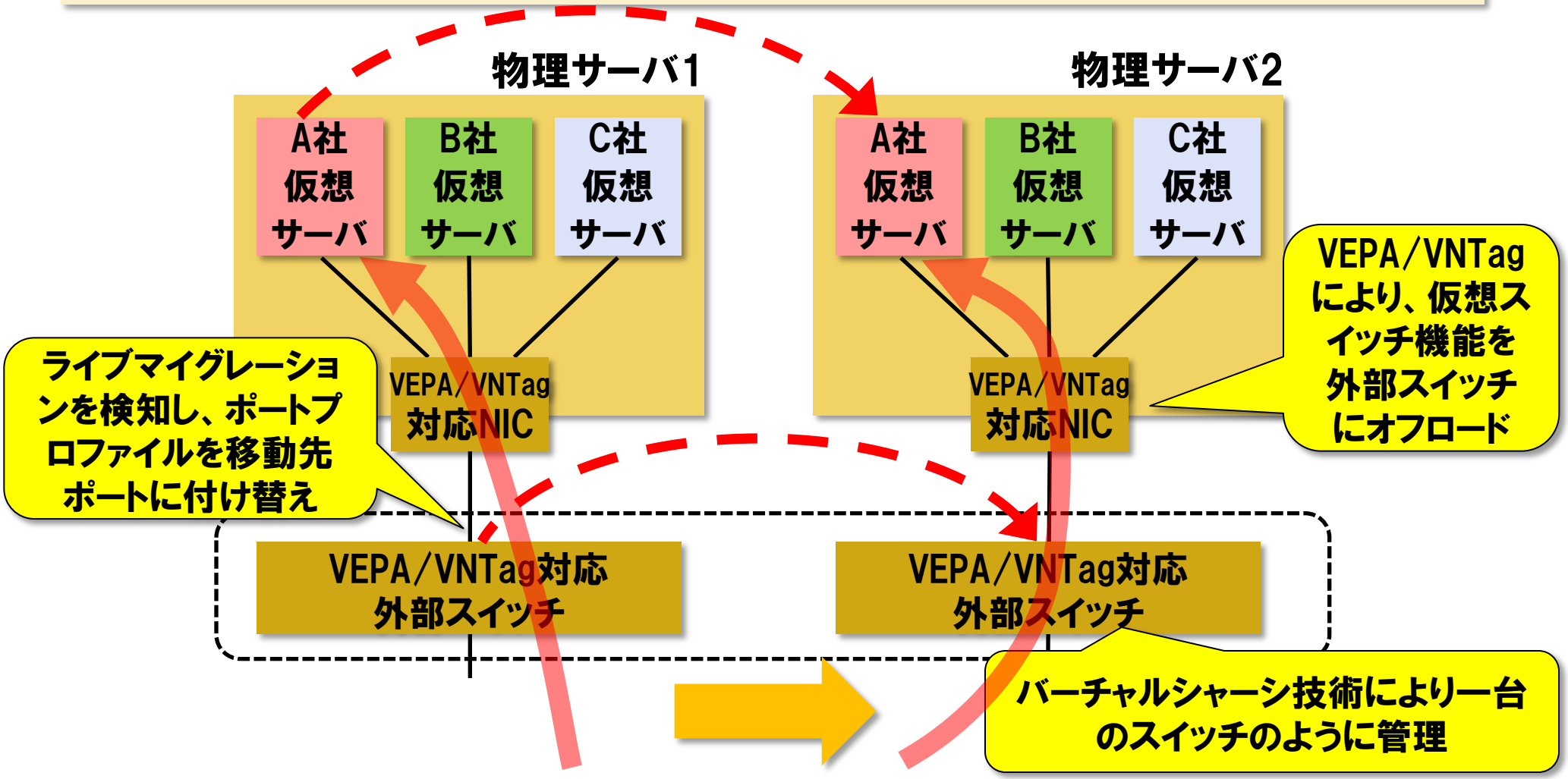
OpenFlowでは、ライブマイグレーションを検知すると、OpenFlowコントローラが自動的に「フロー」（経路）を変更する



ライブマイグレーション対応の例（VLANベース）

変える力を、ともに生み出す。
NTT DATAグループ

VEPA/VNTag、バーチャルシャーシ、ポートプロファイル自動管理などの技術を組み合わせることによりライブマイグレーションに対応



標準化ステータス

- 標準化作業中の技術が多いが先行して実装している製品もある
  - 2012年ぐらいから本格的に対応製品がリリースされると予想

技術	標準化ステータス
VLAN	IEEE 802.1Q - Virtual LANs として標準化済
VXLAN / NVGRE	IETFにて議論中
VEB / VEPA（EVB）	IEEE 802.1Qbg - Edge Virtual Bridging として標準化作業中
VNTag	IEEE 802.1BR - Bridge Port Extension として標準化作業中
ポートプロファイル自動管理	DMTF SVPC WGにて標準化作業中
TRILL	RFC 6325～6327として標準化済
SPB	IEEE 802.1aq - Shortest Path Bridging として標準化作業中
OpenFlow	ONF(Open Networking Foundation)にて標準化

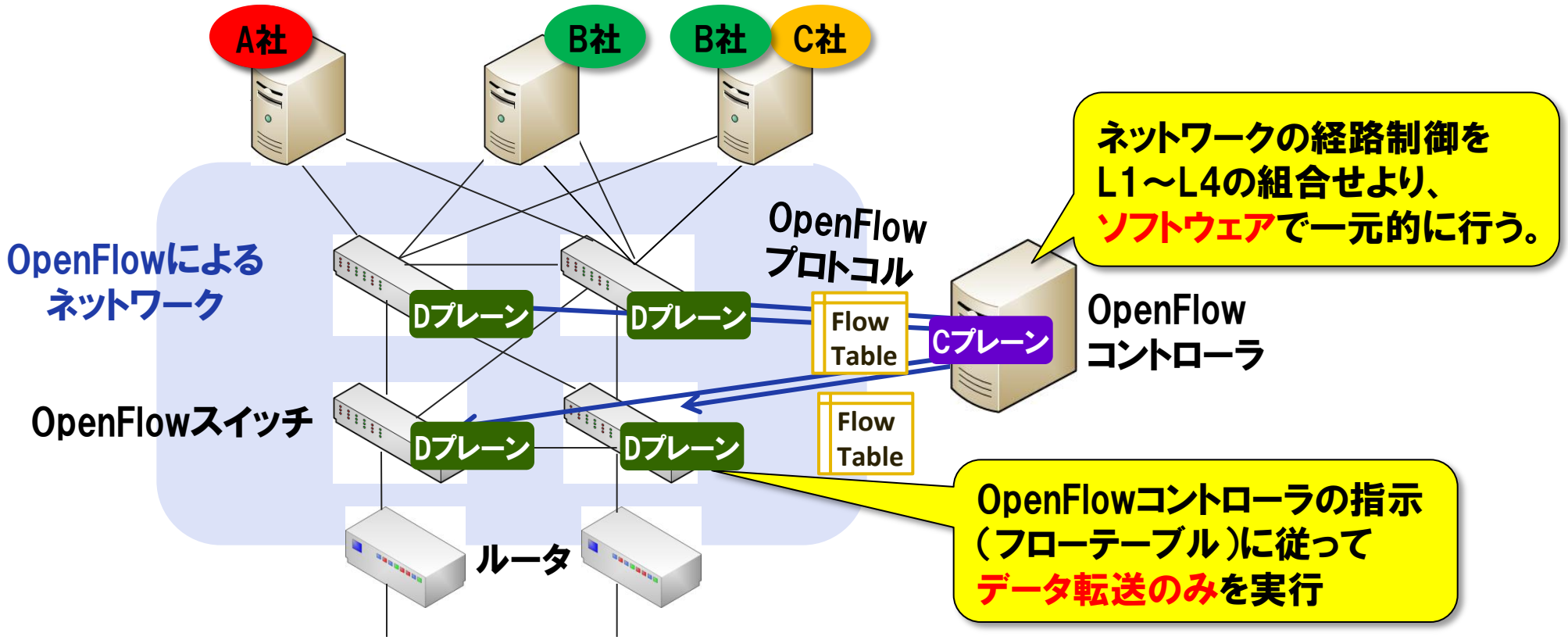
DMTF:Distributed Management Task Force

OpenFlowの概要

OpenFlowの概要と特徴

変える力を、ともに生み出す。
NTT DATAグループ

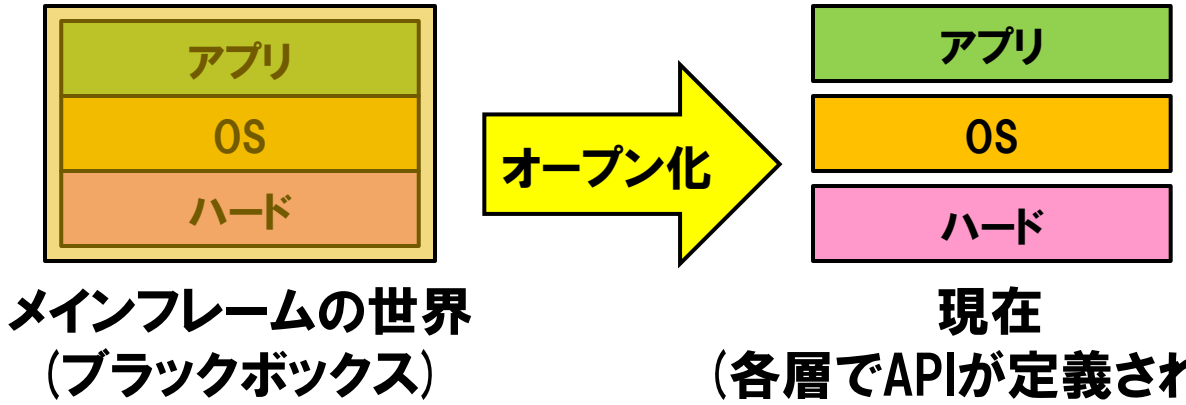
3つの構成要素　・・・　①OpenFlowスイッチ、②OpenFlowコントローラ、③OpenFlowプロトコル



3つの特徴　　・・・　①Software Defined Networking　②CD分離・集中制御　③オープン

OpenFlowの特長　③オープン化について

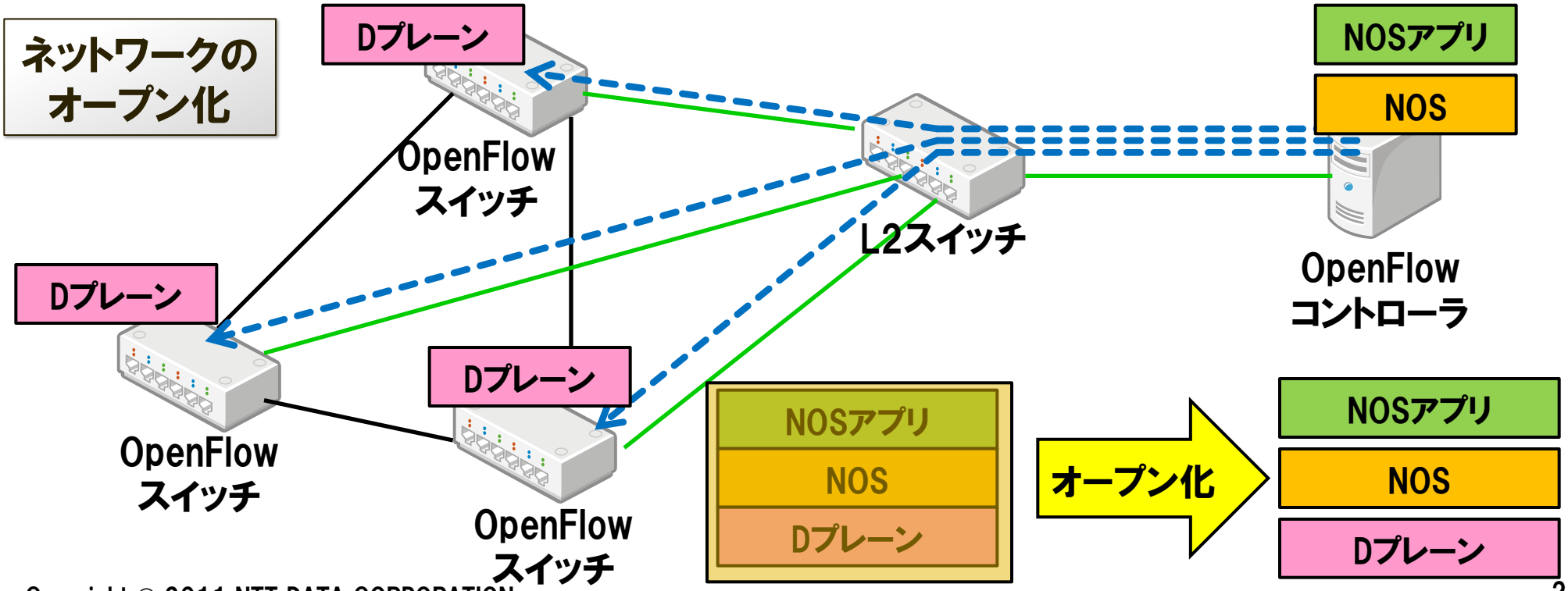
サーバのオープン化



メインフレームの世界
（ブラックボックス）

現在
（各層でAPIが定義される）

ネットワークのオープン化



OpenFlowの誕生と標準化動向

- **2008年～**
  米Clean Slate Programの中で、スタンフォード大学を中心に提唱され、OpenFlowスイッチングコンソーシアムとして研究開発が進む
- **2009年12月**
  OpenFlowプロトコル1.0（標準化）
  オープンソース公開
  ・OpenFlowコントローラ
  ・OpenFlowスイッチ
- **2011年2月**
  OpenFlowプロトコル1.1（標準化）
- **2011年3月**
  ONF(Open Networking Foundation)設立

スタンフォード大、カリフォルニア大バークレー校等、学内NWにおいて2年間運用

DC向け・LAN仕様の基本部分はおよそ完成

ボードメンバ：Google、Facebook、Microsoft、ベライゾン、Yahoo!、ドイツテレコム

メンバ：　Cisco、HP、IBM、NEC、VMware、NTT等17社

・産業界への導入へ向けた、仕様詳細化
　実装を考慮したVer1.1のブラッシュアップ
・広域ネットワークへの拡張
　を図り、Ver1.2以降の仕様を確立していく予定

標準化組織ONFへの参加企業

変える力を、ともに生み出す。
NTT DATAグループ

クラウドサービス事業者（5社）
Google (*)，Facebook (*)，Yahoo! (*)，Microsoft (*)，Tencent

通信事業者（4社）
Deutsche Telekom (*)，Verizon (*)，NTT，Comcast

ネットワーク機器チップメーカー（4社）
Broadcom，Marvell，Intel，Netronome

ネットワーク機器／ソフトウェアベンダ（30社）
Cisco, Juniper Networks, Brocade, Extreme Networks, HP, IBM, Dell, NEC, Force10 Networks, NETGEAR, Ciena, Vello Systems, Nokia Siemens Networks, Ericsson, Huawei Technologies, SUMSUNG, Mellanox Technologies, Riverbed Technology, Ixia, Fujitsu, Pronto Systems, Infoblox, IP Infusion, Big Switch Networks, Nicira Networks, Plexxi, Metaswitch Networks, Midokura, LineRate Systems, ZTE

仮想化ソフトウェアベンダ（2社）
Citrix, VMware

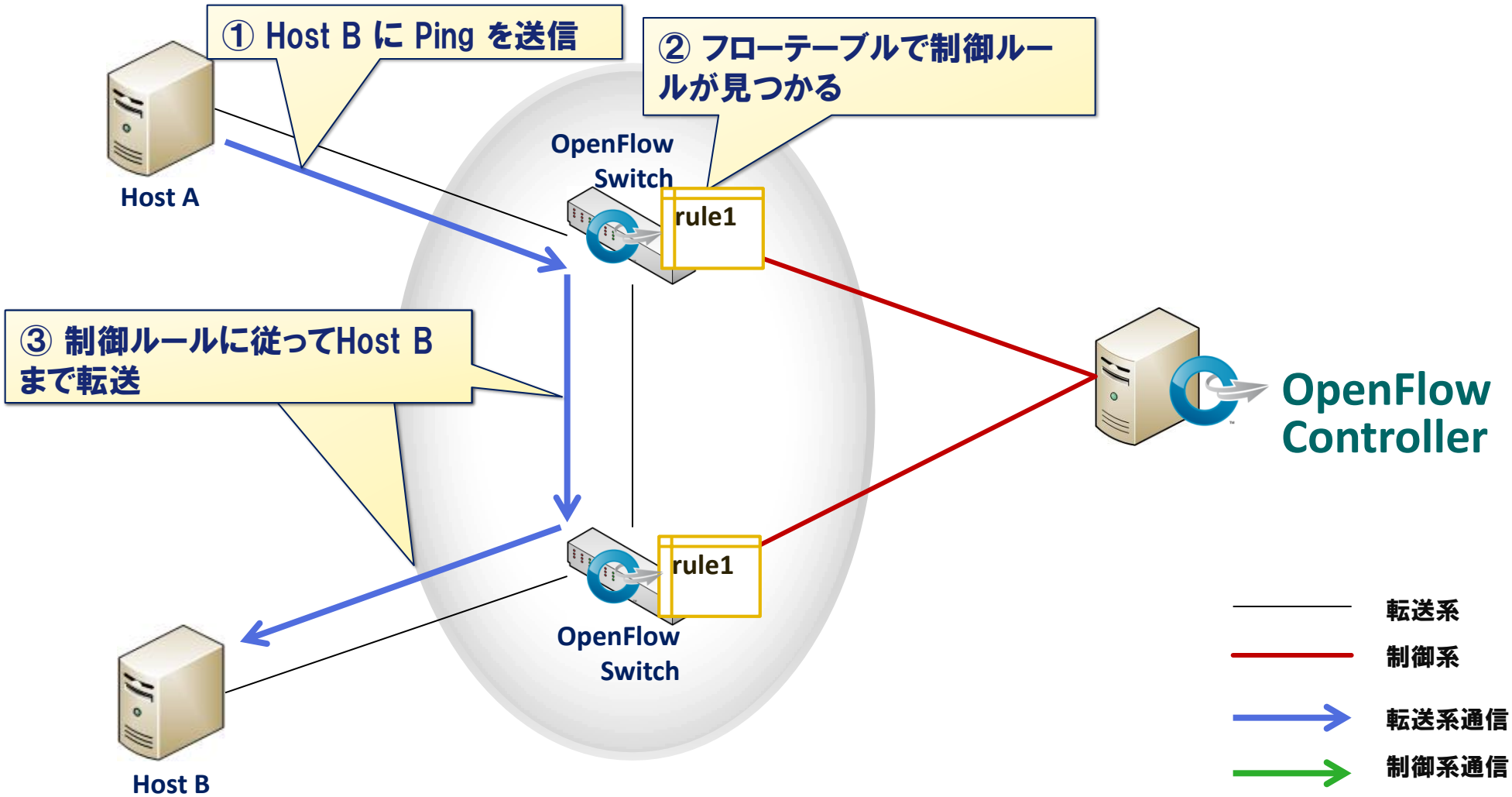
その他（2社）
CompTIA, ETRI

2011年10月1日現在　47社　(*) はボードメンバ

OpenFlowの基本動作①

変える力を、ともに生み出す。
NTT DATAグループ

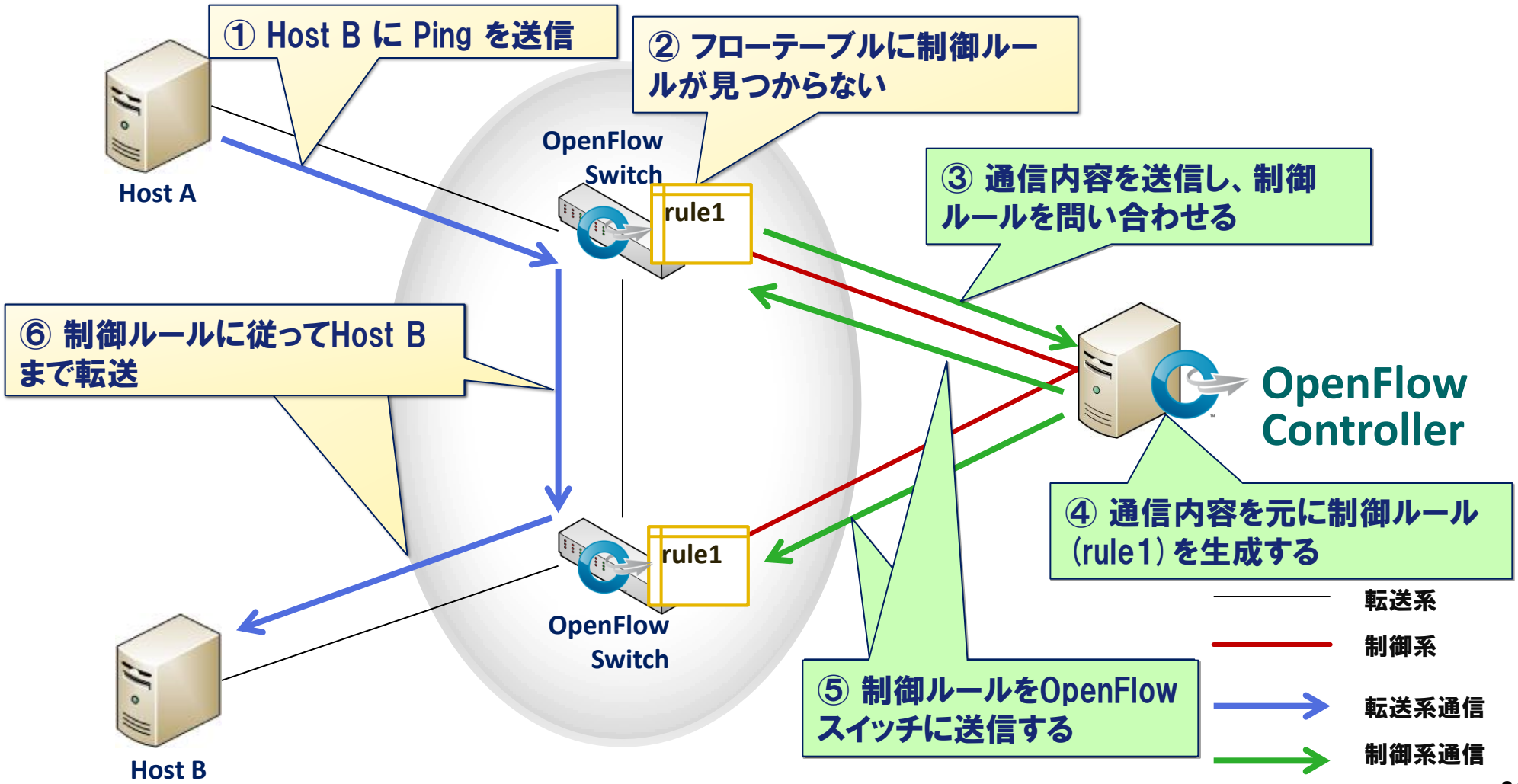
フローテーブルで保持している制御ルールに従って通信を制御する



OpenFlowの基本動作②

変える力を、ともに生み出す。
NTT DATAグループ

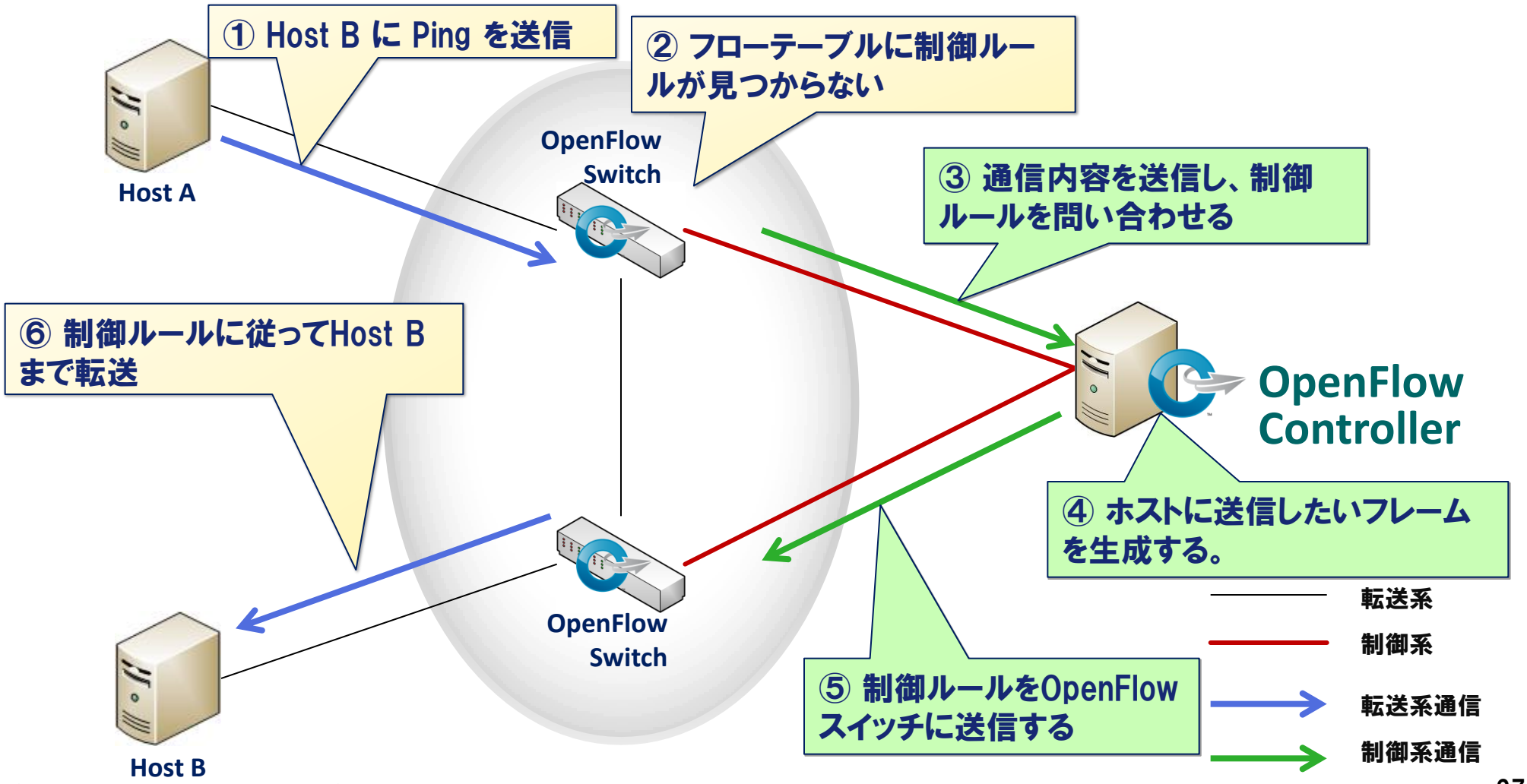
経路制御ルールがフローテーブルに見つからない場合は、OpenFlowコントローラに問い合わせる



OpenFlowの基本動作③

変える力を、ともに生み出す。
NTT DATAグループ

コントローラから任意のパケットをホストに送信することも可能



OpenFlowスイッチのフローテーブルの内容

変える力を、ともに生み出す。
NTT DATAグループ

フロー識別に利用可能な情報（OpenFlow1.0の場合）

レイヤ	ヘッダフィールド
レイヤ1	イングレスポート
レイヤ2	送信元MACアドレス
	宛先MACアドレス
	イーサタイプ
	VLAN ID
	VLANプライオリティ
レイヤ3	送信元IPアドレス
	宛先IPアドレス
	IPプロトコル
	ToS
レイヤ4	送信元ポート/ICMPタイプ
	宛先ポート/ICMPコード

フローに対するアクション

アクション	説明
Forward	パケットを指定したポートに転送（カプセル化してOpenFlowコントローラに転送することも可能）
Drop	パケットを破棄する
Enqueue	パケットを指定したキューに入れる(オプション)
Modify-Field	パケットのフィールドを書き換える（オプション）

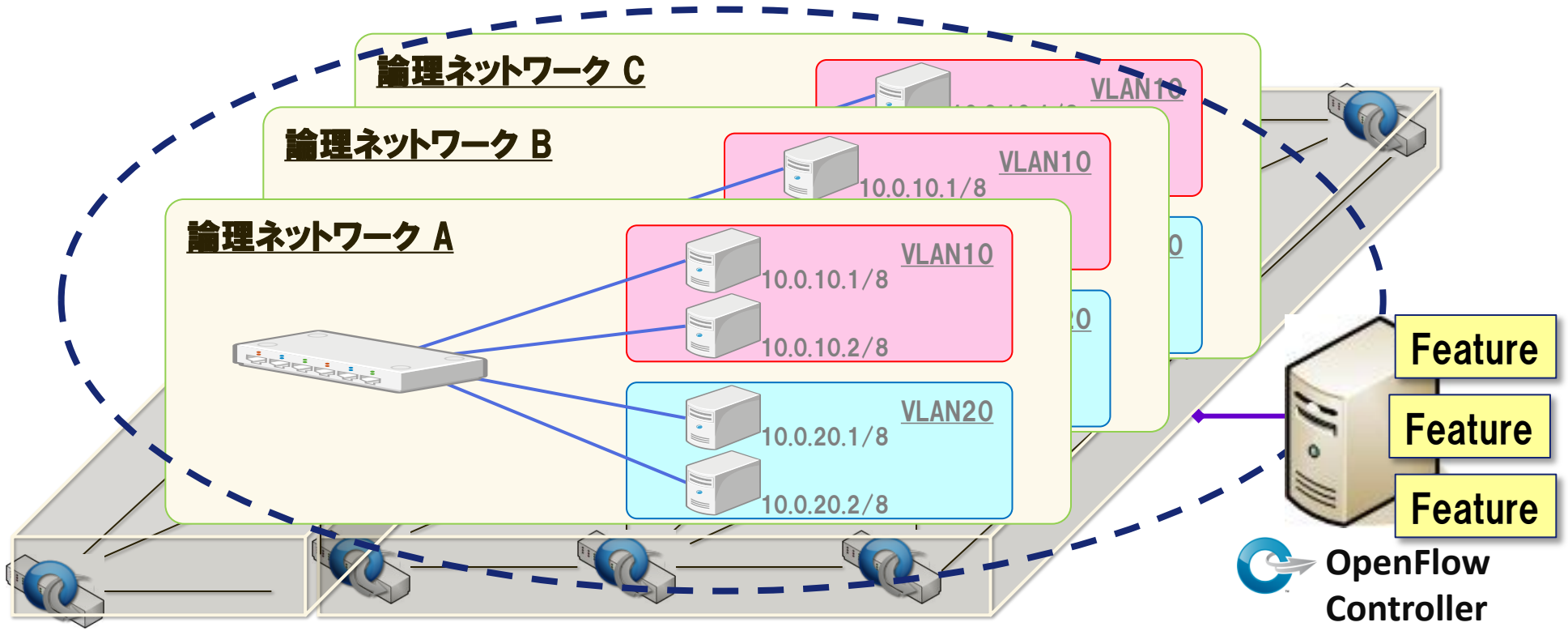
OpenFlowで実現できるネットワークの世界

変える力を、ともに生み出す。
NTT DATAグループ

① 集中制御と容易なスケールアウト →運用自動化
個別の機器設定、リンク・アグリケーションの設定、スパニングツリーの考慮の必要なし

② 多様且つ動的なスライシング →マルチテナント対応、ライブマイグレーション対応
様々なFeatureに基づく、多様な論理ネットワークへのスライシング

③ ロードバランシング →帯域の有効活用
ネットワーク全体を最適化するロードバランシング

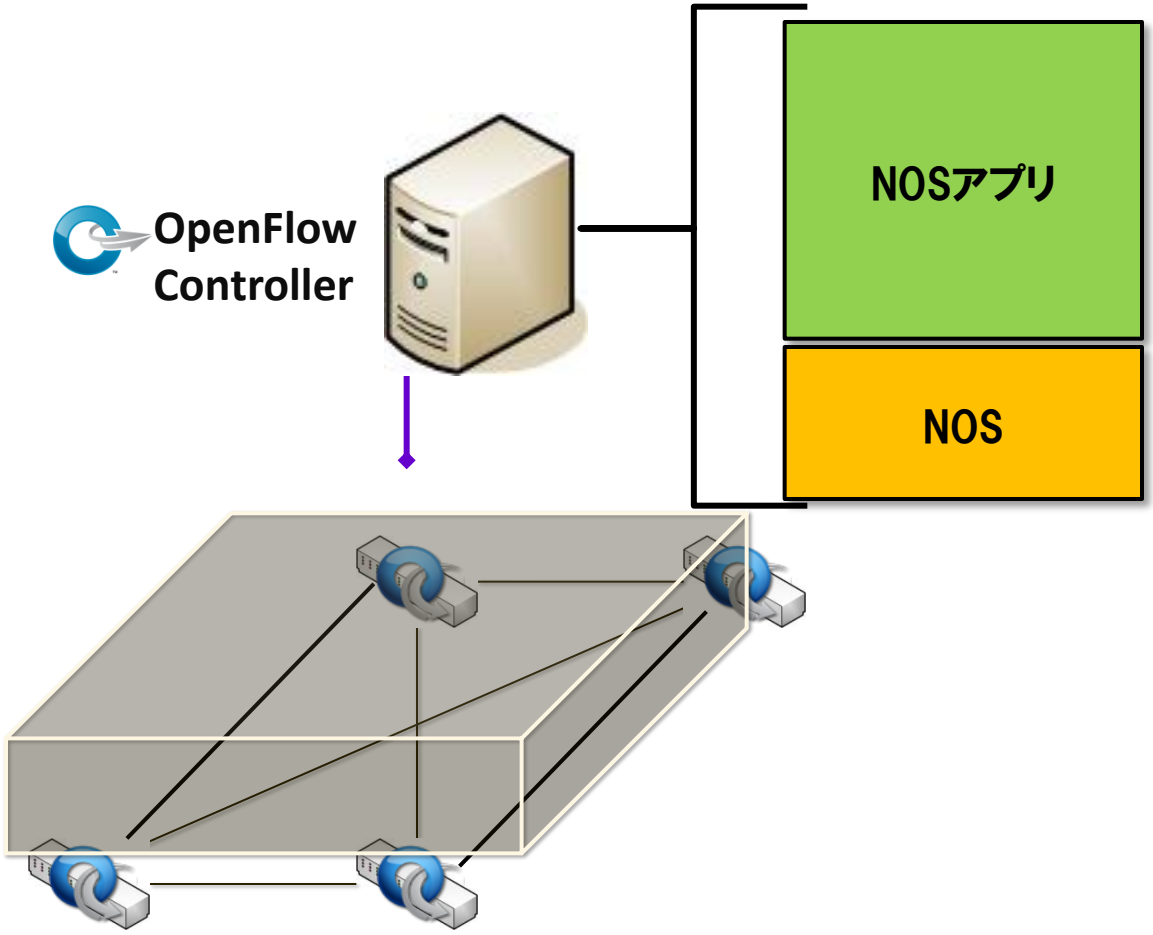


NTTデータの取り組み
～OpenFlowコントローラの開発とネットワーク仮想化～

OpenFlowコントローラの開発

変える力を、ともに生み出す。
NTT DATAグループ

- マルチベンダに対応するコントローラを開発
- 豊富なNOSアプリ(Features)によりデータセンタのネットワーク課題に対応
- Hinemosとの連携により、サーバ・ネットワークの統合管理の実現



NOSアプリ(Features)
- 物理ネットワーク管理
- 論理ネットワーク管理
- 論理L2ネットワークエミュレート
- 論理L3ネットワークエミュレート
- 自動経路計算
- 故障スイッチ迂回
- ライブマイフレーション追随

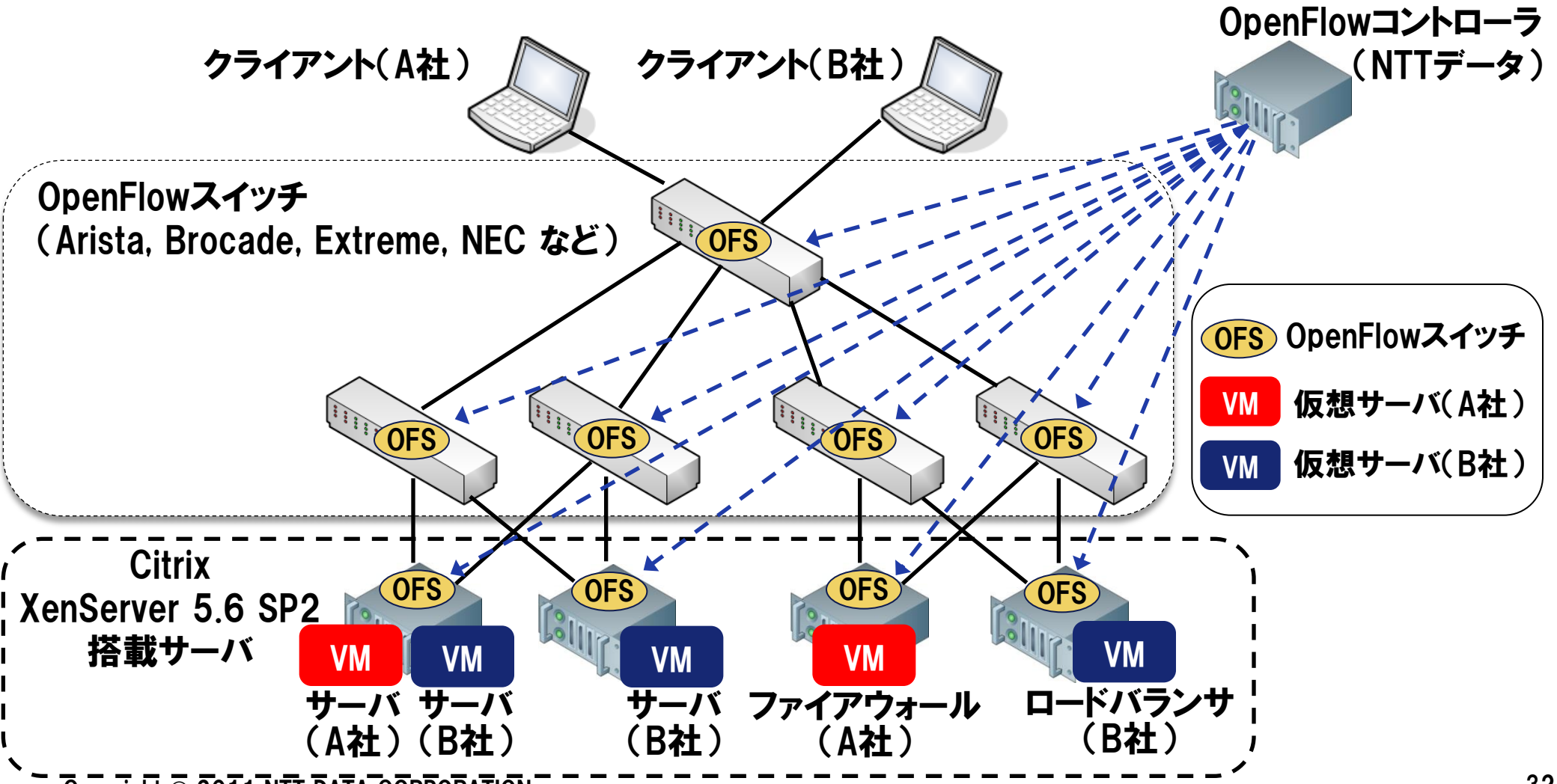
NOS(OpenFlow1.0対応)
- マルチベンダスイッチ対応
- 仮想スイッチ(Open vSwitch)対応

その他
- 運用管理(Hinemos)連携
- 仮想アプライアンス連携

様々なOpenFlowスイッチとの相互接続

変える力を、ともに生み出す。
NTT DATAグループ

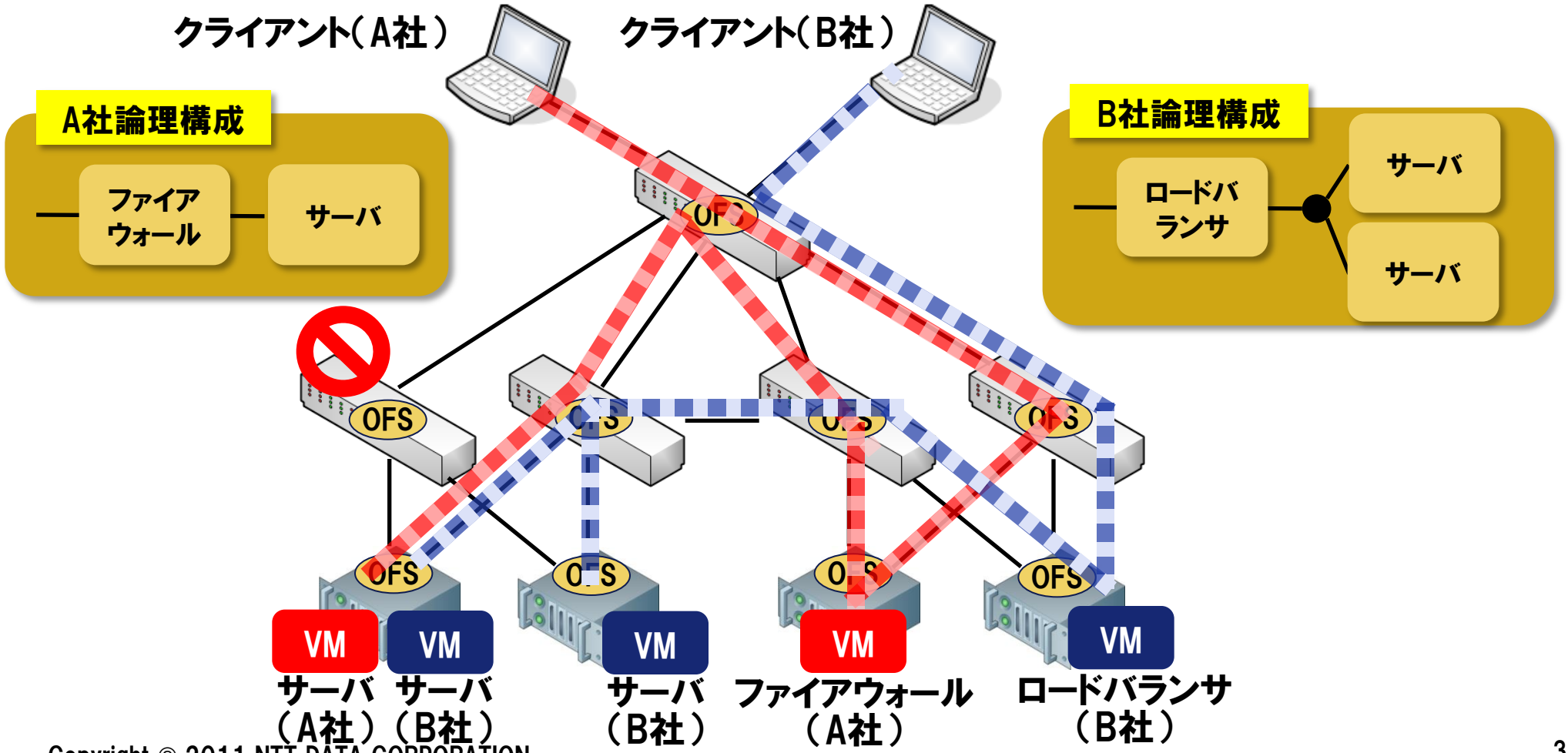
各ベンダスイッチを経由した、テナント企業向け論理ネットワークの生成、削除、経路制御、ライブマイグレーション追随を実現



マルチベンダ環境でのOpenFlow動作検証

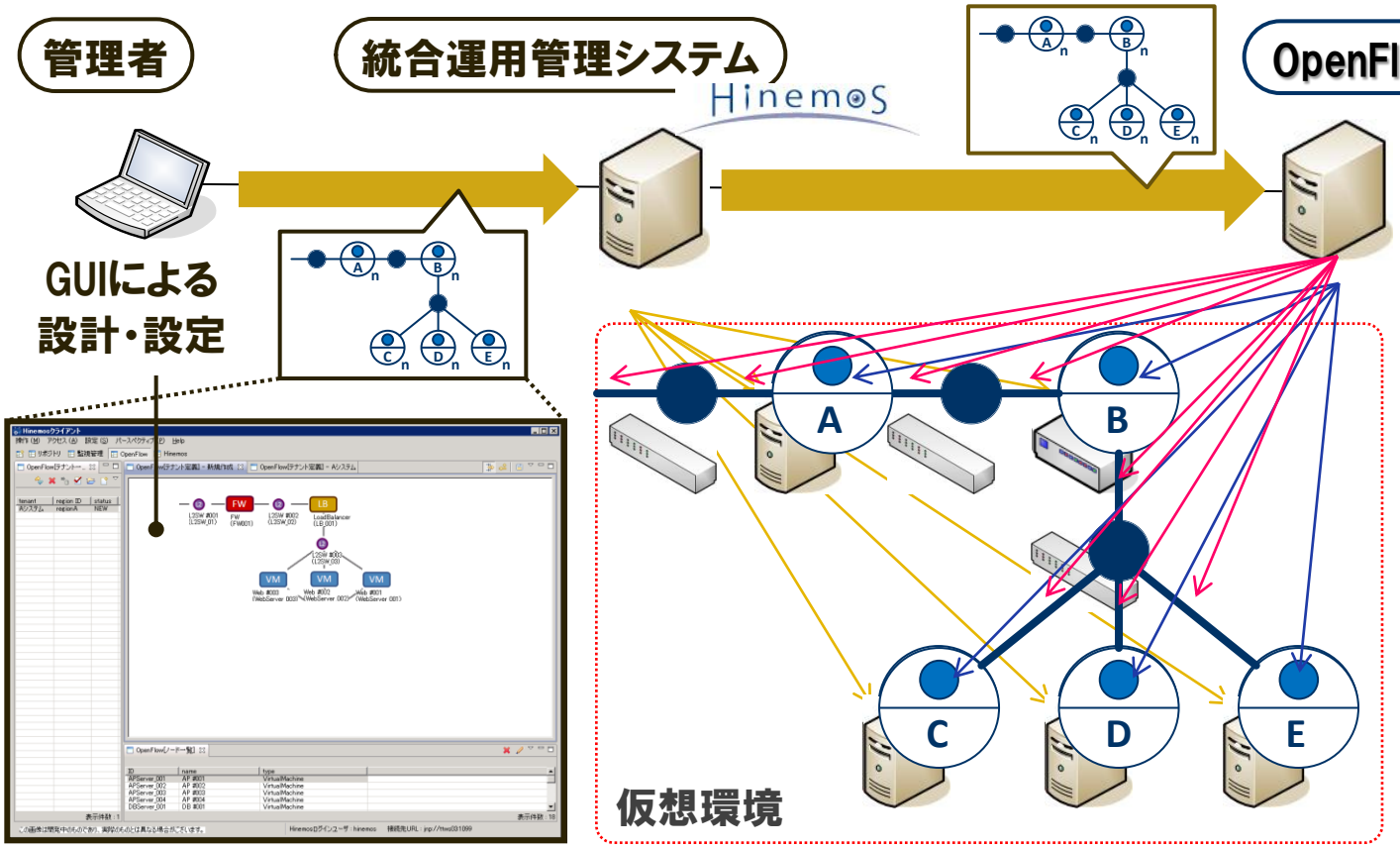
変える力を、ともに生み出す。
NTT DATAグループ

①テナント企業向け論理ネットワークの生成
②経路制御（保守対象スイッチ自動迂回）
③ライブマイグレーション自動追随



データセンタにおけるサーバ・ネットワークの統合管理 ～テナント企業向けネットワークの自動作成の例～

- GUIで描かれた論理構成図から仮想環境上に自動で仮想的なシステム（サーバ、ネットワーク）を実現



動作

1. 論理ネットワーク構成をGUIで描画
   - 各ノードのIPアドレス、ネットマスク、デフォルトゲートウェイ
   - NTPサーバ、DNSサーバのアドレス
   - ロードバランサの設定、ファイアウォールの設定
2. HinemosのVM管理機能により必要な仮想サーバを起動
3. OpenFlowコントローラが各ノードのネットワーク設定を実施
   - IPアドレス、ネットマスク、デフォルトゲートウェイ
   - NTPサーバ、DNSサーバのアドレス
4. OpenFlowコントローラによりOpenFlowスイッチの経路とFWポリシーを設定

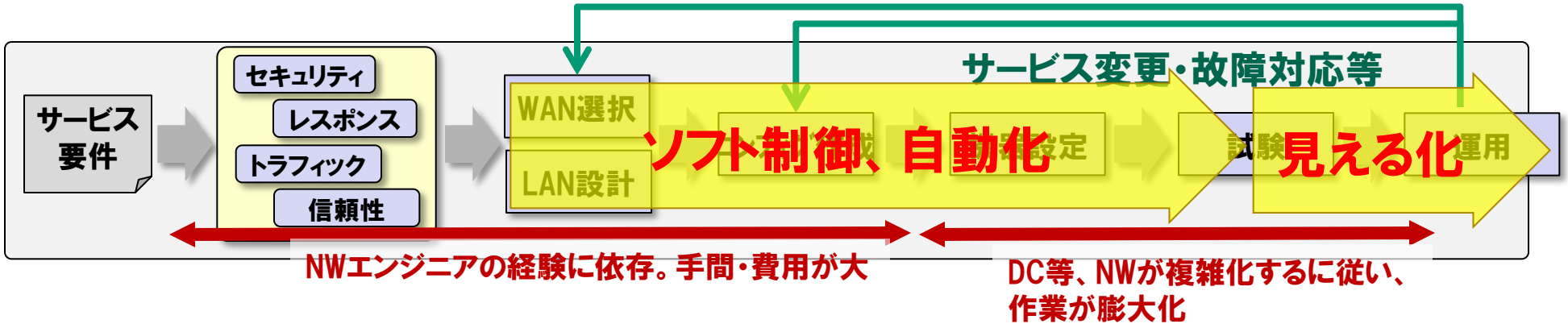
ノード： 仮想サーバ，ロードバランサ，ファイアウォール等のインスタンス．
リンク： ノード同士を接続する論理結線，およびSW等の中継機器．

凡例 リンク（論理結線） リンク（中継機器） ノード（VM） IPアドレス MACアドレス

データセンタネットワーク効率化の期待

変える力を、ともに生み出す。
NTT DATAグループ

① NWインテグレーション、オペレーションコストの大幅な削減



② NW設備の大幅なコスト低減

従来、垂直統合であったネットワーク機器が、**オープン化**
※データ転送レイヤ、制御レイヤが分離し、転送系はコモディティ化し
制御系は**ソフトウェアの領域**に
サーバ世界と同等の価格破壊、Bizモデルの変化が起こる可能性が大

③ NW設備の小電力化

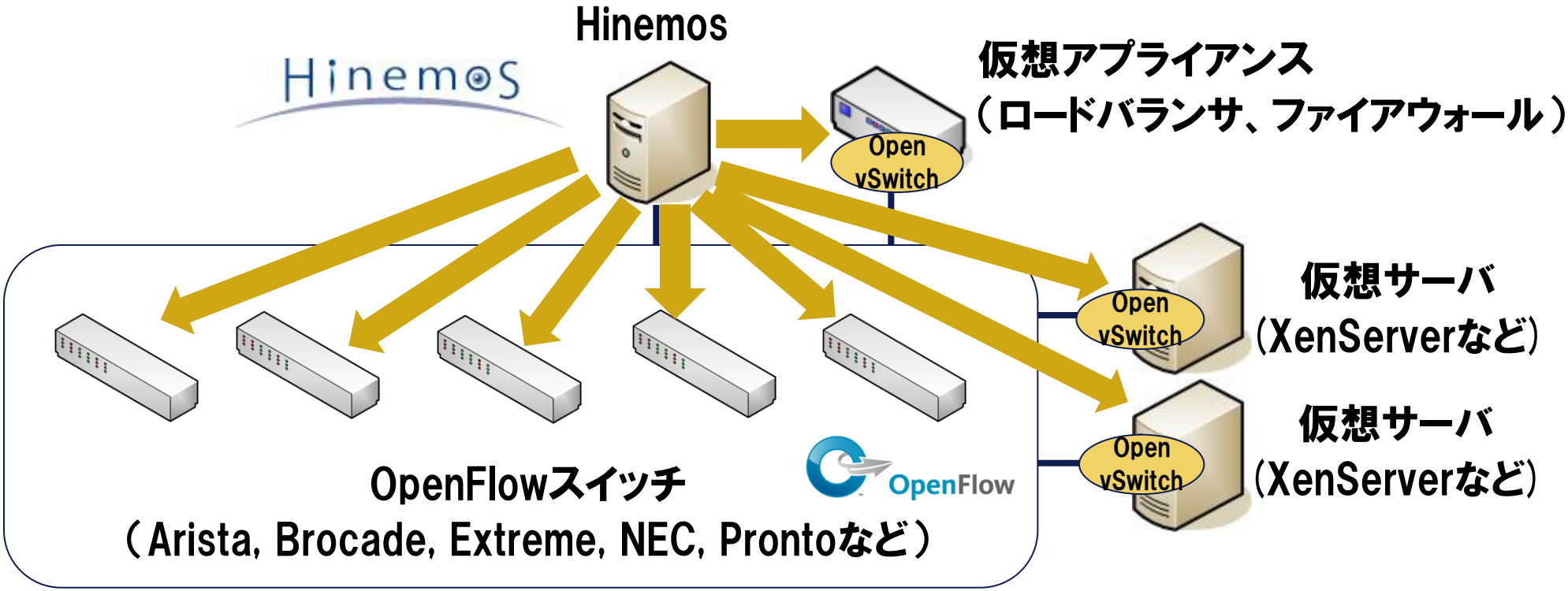
オフピーク時に、**計画的なトラヒックの片寄せ**と、機器の電源オフが可能

NTTデータの仮想プライベートクラウドの実現に向けた取り組み

仮想プライベートクラウドコントローラの開発

変える力を、ともに生み出す。
NTT DATAグループ

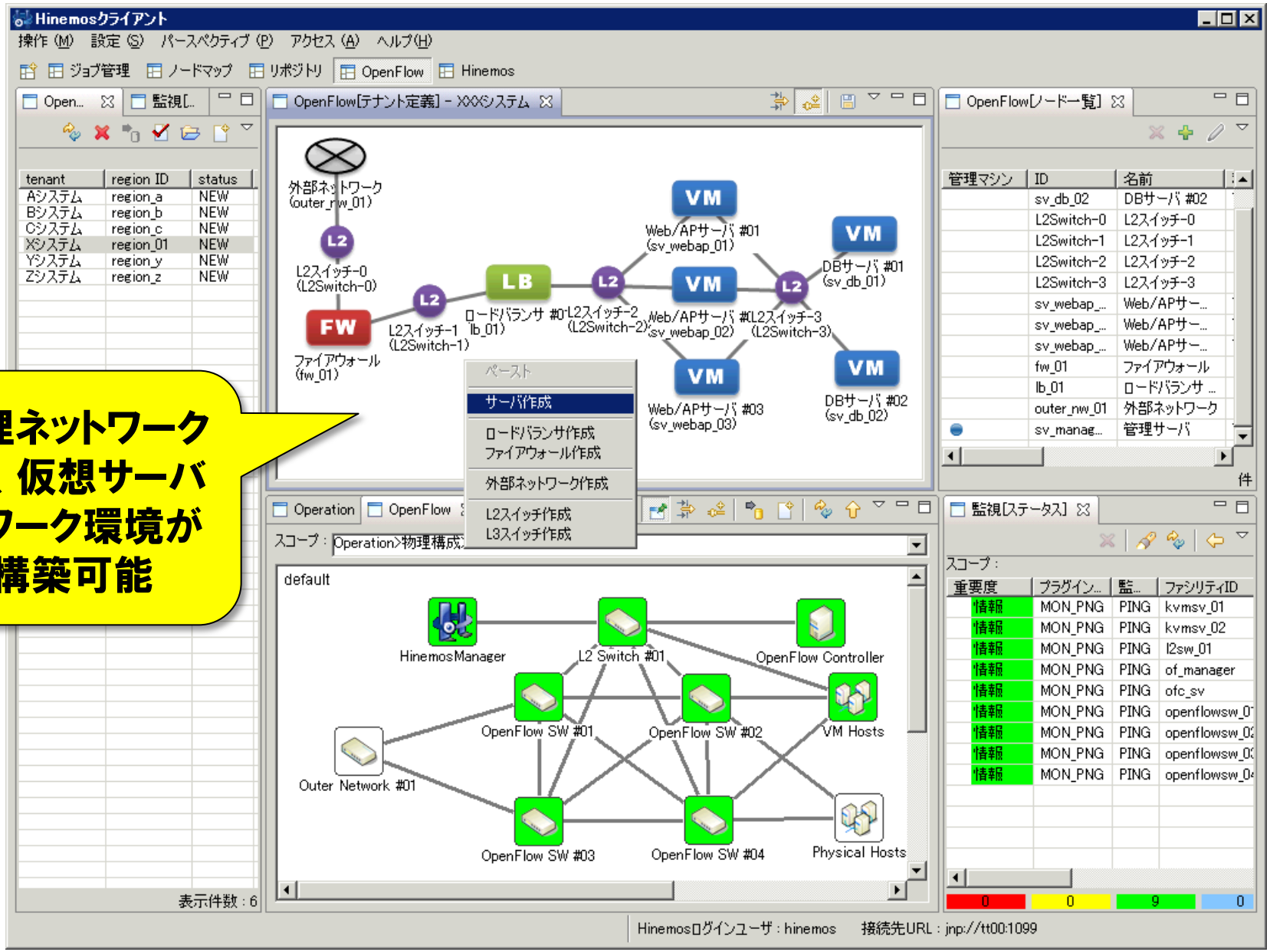
NTTデータのオープンソース統合管理ソフトウェア「Hinemos」から、仮想サーバ、仮想アプライアンス、OpenFlowスイッチを自動制御



「Hinemos OpenFlowオプション」（仮称）として2012年4月にリリース予定
NTTデータ展示ブースにてデモンストレーション実施中！
ITpro EXPO AWARD 優秀賞受賞！

「Hinemos OpenFlowオプション」(仮称)のイメージ

変える力を、ともに生み出す。
NTT DATAグループ

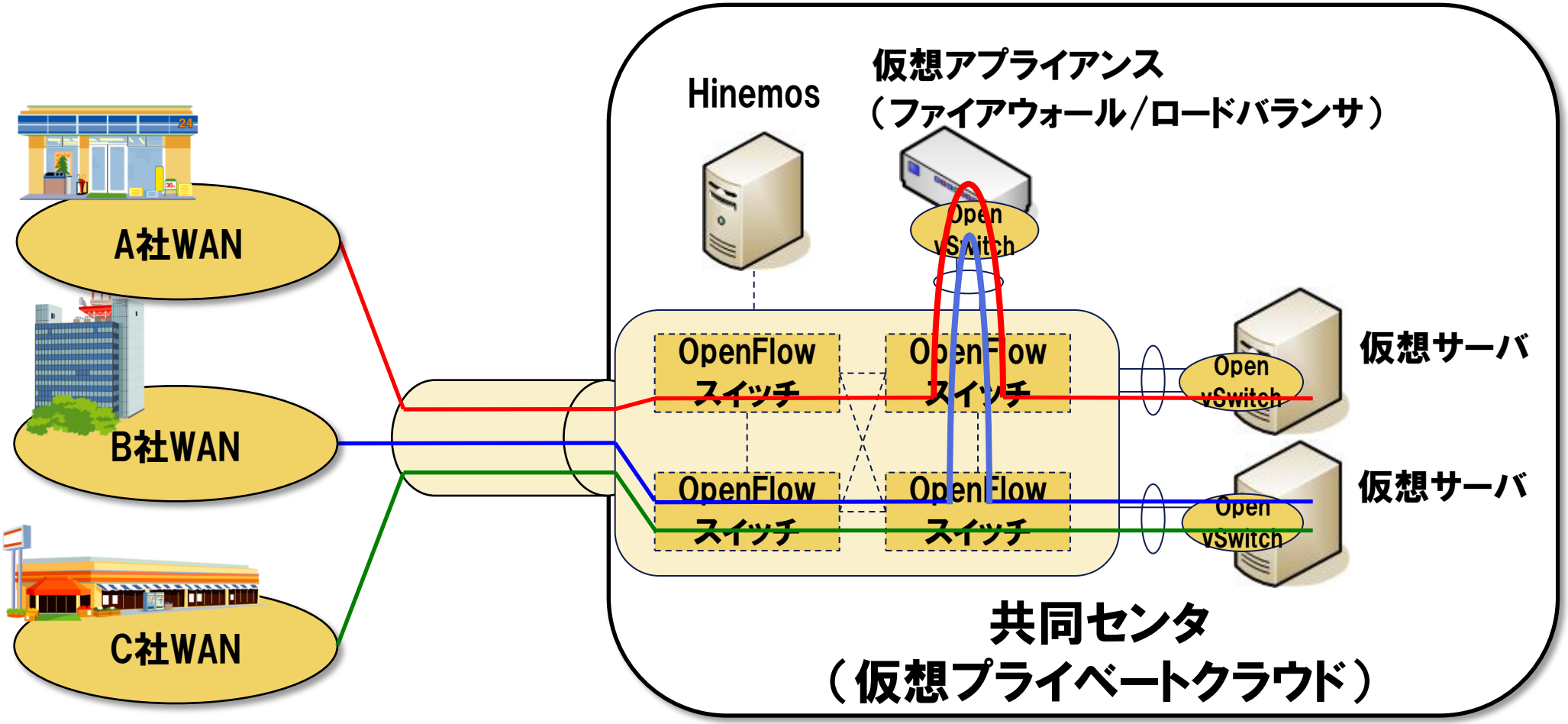


画面上に論理ネットワークを描くだけで、仮想サーバ/仮想ネットワーク環境が自動的に構築可能

仮想プライベートクラウド構築・運用サービスの提供

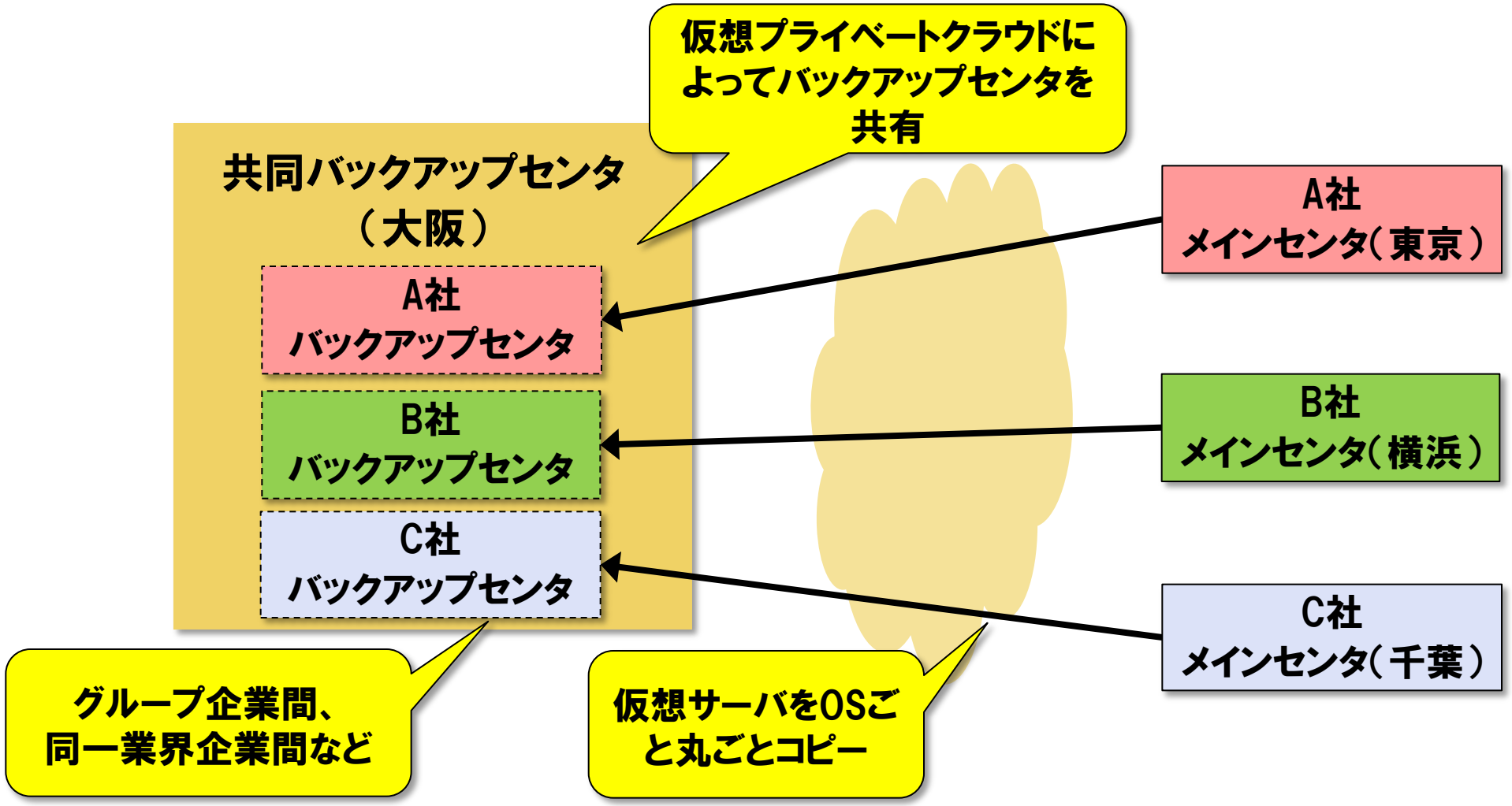
変える力を、ともに生み出す。
NTT DATAグループ

仮想アプライアンス、OpenFlowを活用した、仮想プライベートクラウド構築・運用サービスを提供予定



仮想プライベートクラウドの活用例

バックアップセンタはコストがかかるが、仮想プライベートクラウドによって他社と共有することによって、低いコストで事業継続が可能



まとめ

- 今後のクラウドコンピューティング基盤には、ネットワークの仮想化と運用自動化の技術が重要となります。
- 現在、様々な技術が出てきていますが、大きく、「VLANベース」と「OpenFlowベース」の2つのアーキテクチャが主流になっていくと考えられます。
- NTTデータでは、仮想アプライアンスとOpenFlowを活用した仮想プライベートクラウドコントローラを開発し、サーバとネットワークを含んだデータセンタ全体の運用管理の自動化を実現します。また、仮想プライベートクラウドの構築・運用をご支援いたします。

変える力を、ともに生み出す。

NTT DATAグループ