



INTEROP Tokyo 2014 ShowNetにおけるSDN/NFV

INTEROP Tokyo 2014
ShowNet NOC Team
中村 遼

INTEROP®

TOKYO | 11–13 JUNE, 2014

- **世界最大のネットワーク機器と技術の展示会**

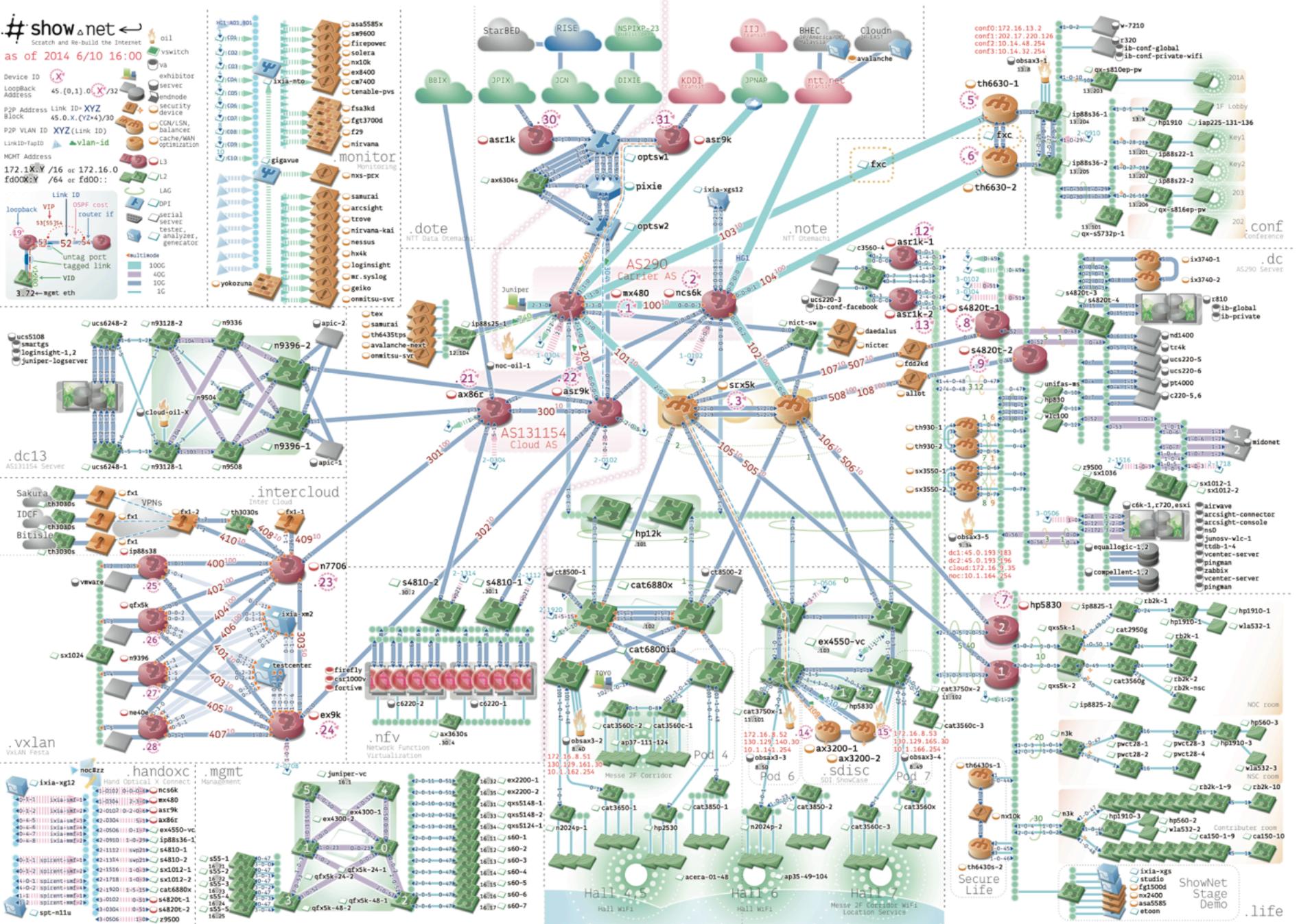
- 毎年6月に幕張メッセで開催
- 来場者数約13万人
- 参加企業、団体は526社




Scratch and Re-build the Internet

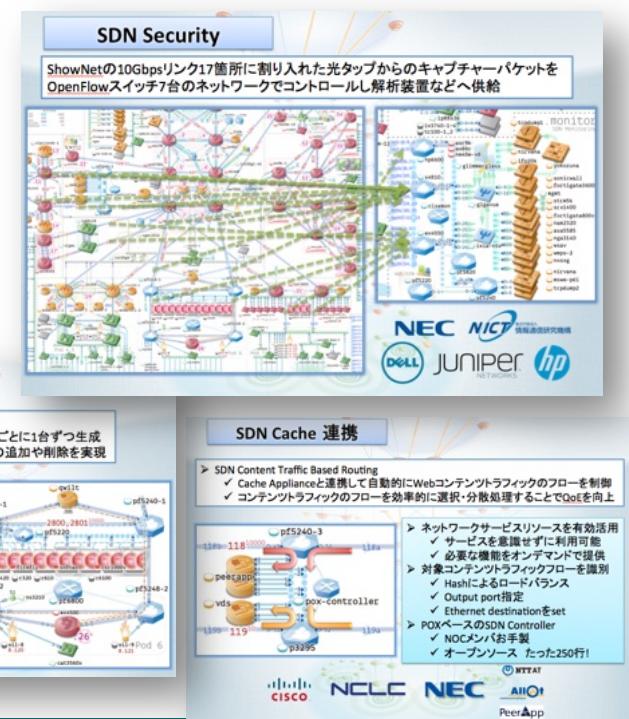
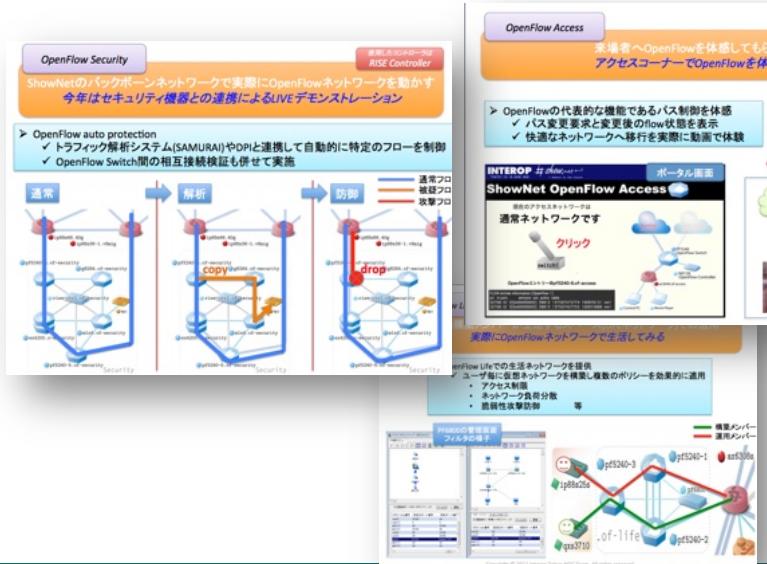
- **"I know it works because I saw it at INTEROP"**
 - INTEROPで構築される世界最大のデモンストレーションネットワーク
 - 最新の技術で10年先のインターネットを構築する
 - 様々な技術の相互接続性検証の場
 - 出展者や来場者へのネットワーク提供





ShowNetにおけるSDN

- ShowNetは「生きた」ネットワーク
 - 2012年からOpenFlowを始め様々な検証を実施
 - ShowNetでは動くSDNが求められる
 - そして「Interoperability」



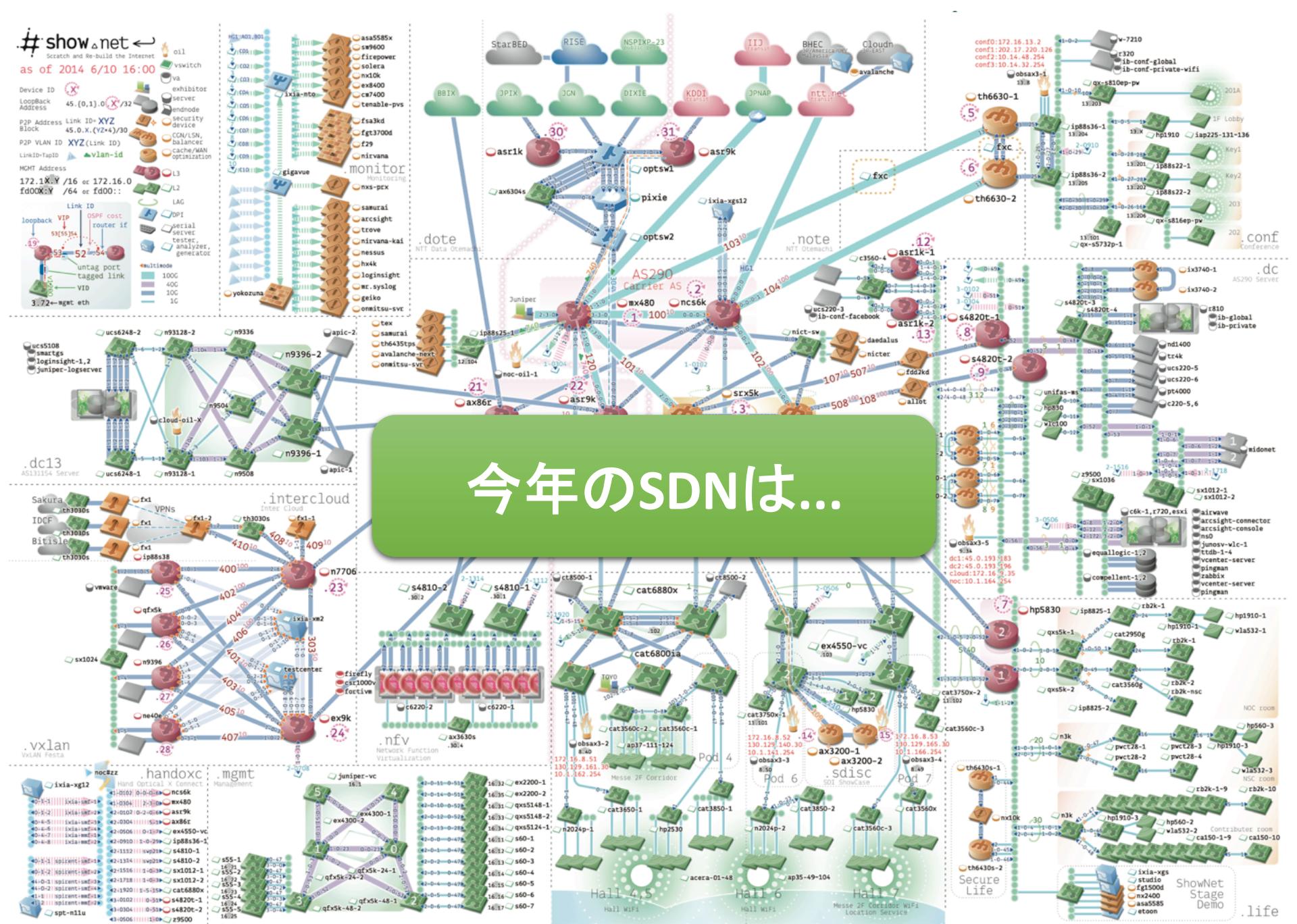
#show.net ←
Scratch and Re-build the Internet

as of 2014 6/10 16:00

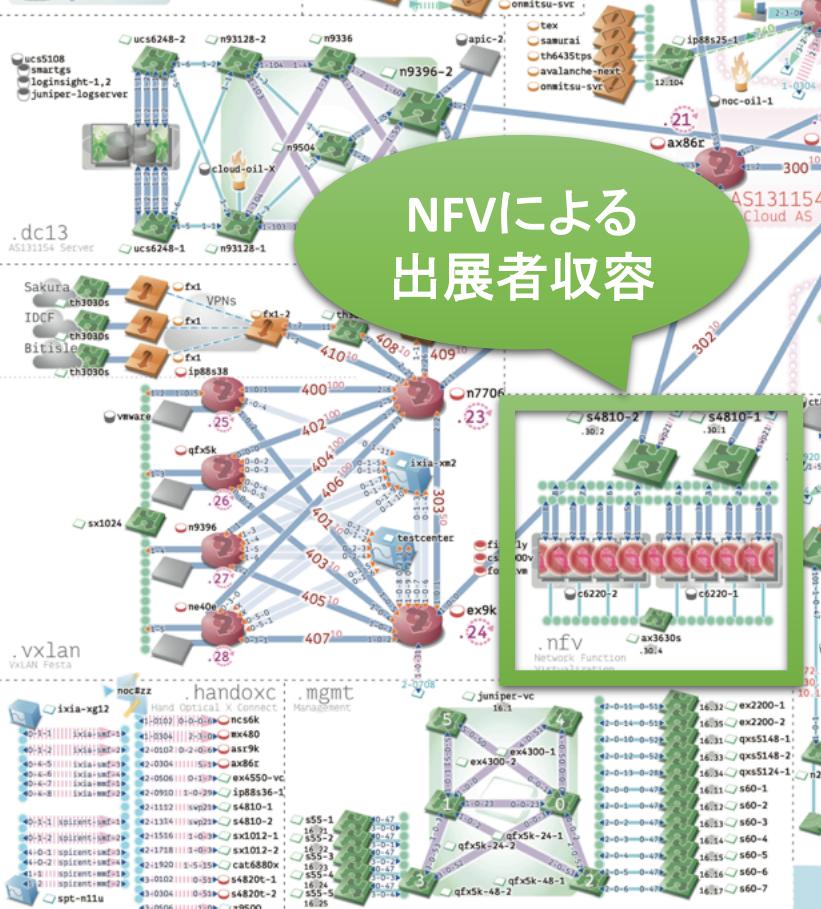
Device ID
LoopBack
Address 45.0.0.10/X/32
PnP Address Link ID: XYZ
45.0.X.(Y*2^4)/30
P2P VLAN ID XYZ (Link ID)
LinkID:vlan-id
MCHT Address
172.1.0/X/16 or 172.16.0
/64 or fd00:
fd00:X:0:0/128

Link ID OSPF cost router if
loopback VIP 53[53][54]
52 52 64
untag port tagged link
VID

oil
vswitch
exhibitor
server
endnode
security device
CM/LSN
balanced cache/WAN optimization
L3
L2
LAG
DPI
serial
server
tester
analyzer
generator
multimode
100G
40G



今年のSDNは...



NFVによる 出展者収容

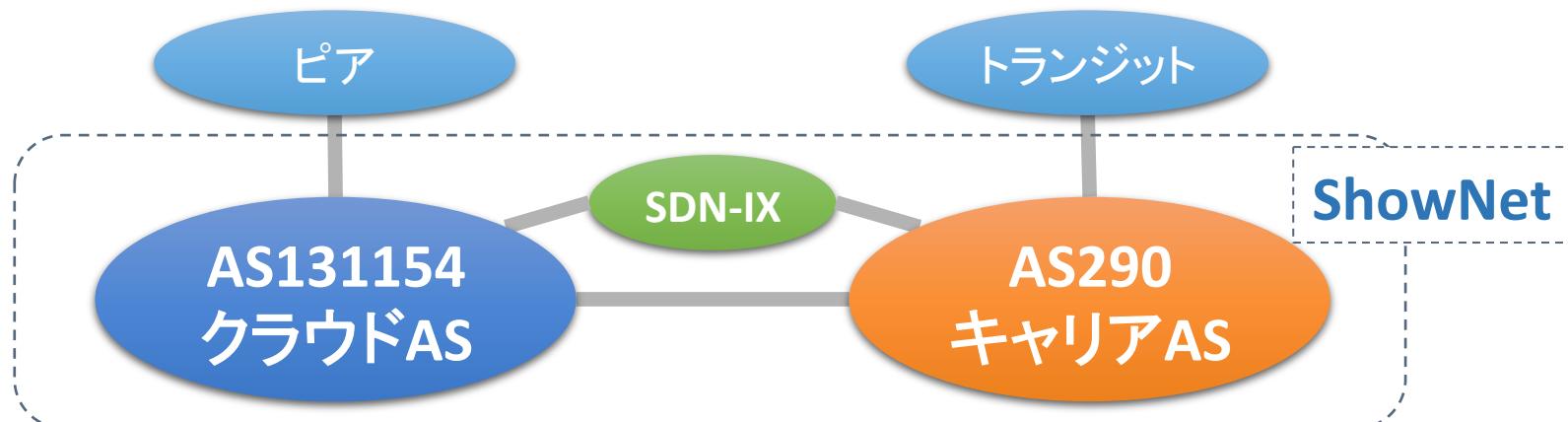
SDN技術 によるIX

そして全体のネットワークにまたがる設定の自動化

ShowNet 2014 バックボーン/SDNデザイン

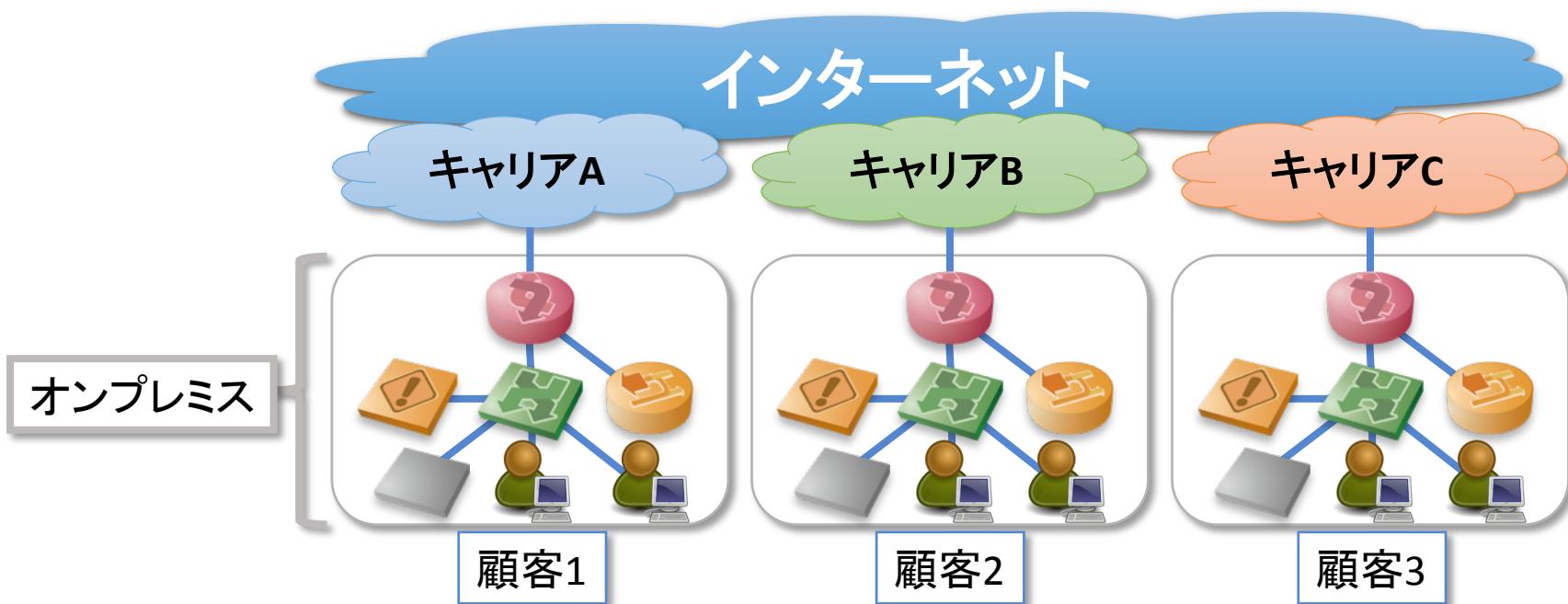
ShowNetにおける2つのAS

- ・ **さまざまサービス形態とネットワークデザイン**
 - ・ ISP、CSP、クラウド事業者など様々なサービス形態がある
 - ・ サービス応じてネットワークの構成は大きく異なる
- ・ **2014年のShowNetは2つのASから構築**
 - ・ 「AS290 キャリアAS」 バックボーン技術や出展者収容
 - ・ 「AS131154 クラウドAS」 最新のDCやクラウド技術の実験



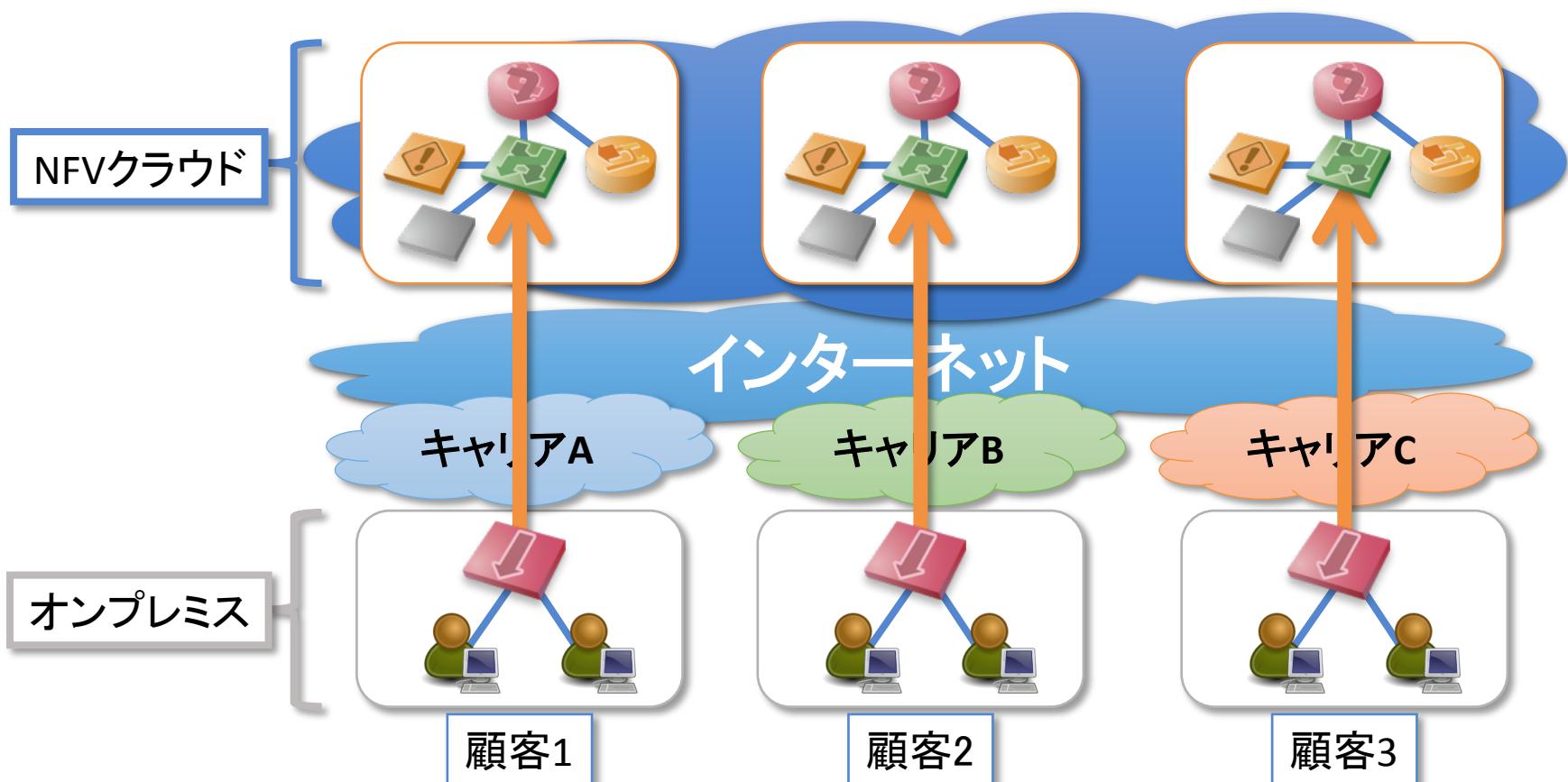
現在のネットワークの構成

- ・ オンプレミスでさまざまな機器を運用
 - ・ サーバ資源は仮想化技術によってクラウドへ
 - ・ ネットワーク機能は自分たちの手で用意
 - 上流接続用ルータ、Firewall、IPS/IDS、



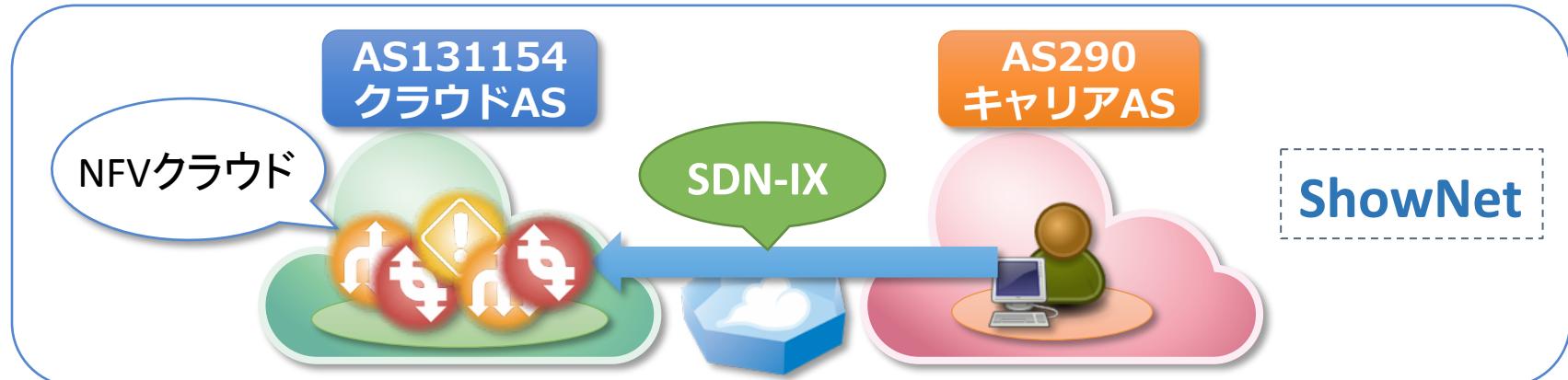
ネットワーク機能のクラウド化

- ネットワークの機能も仮想化してクラウドへ



ASを越えるSoftware Defined Network

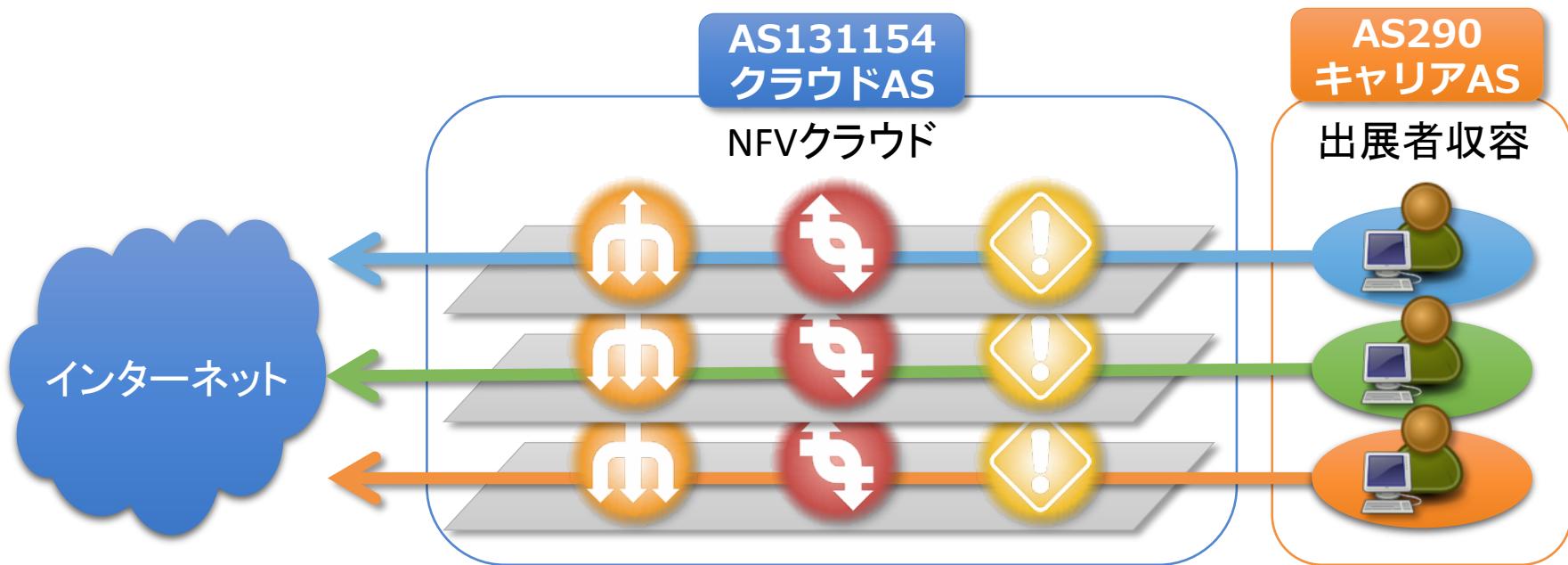
- 「必要な機能をクラウドから受け取る」
 - 出展者(顧客)は
 - キャリアASから接続性をうけとる
 - クラウドASから必要な"ネットワークの機能"をうけとる
 - **NFV**は"ネットワークの機能"を実現
 - **SDN**は"ユーザごとのネットワーク自動化"を実現



Network Function Virtualization

ShowNet 2014における Network Function Virtualizationの概要

- **AS131154 : クラウドASにNFVクラウドを構築**
 - 出展者ごとに仮想ネットワークを自動的に構築
 - 要望にあわせた柔軟なネットワークの変更
- **AS290からユーザのネットワークを接続**

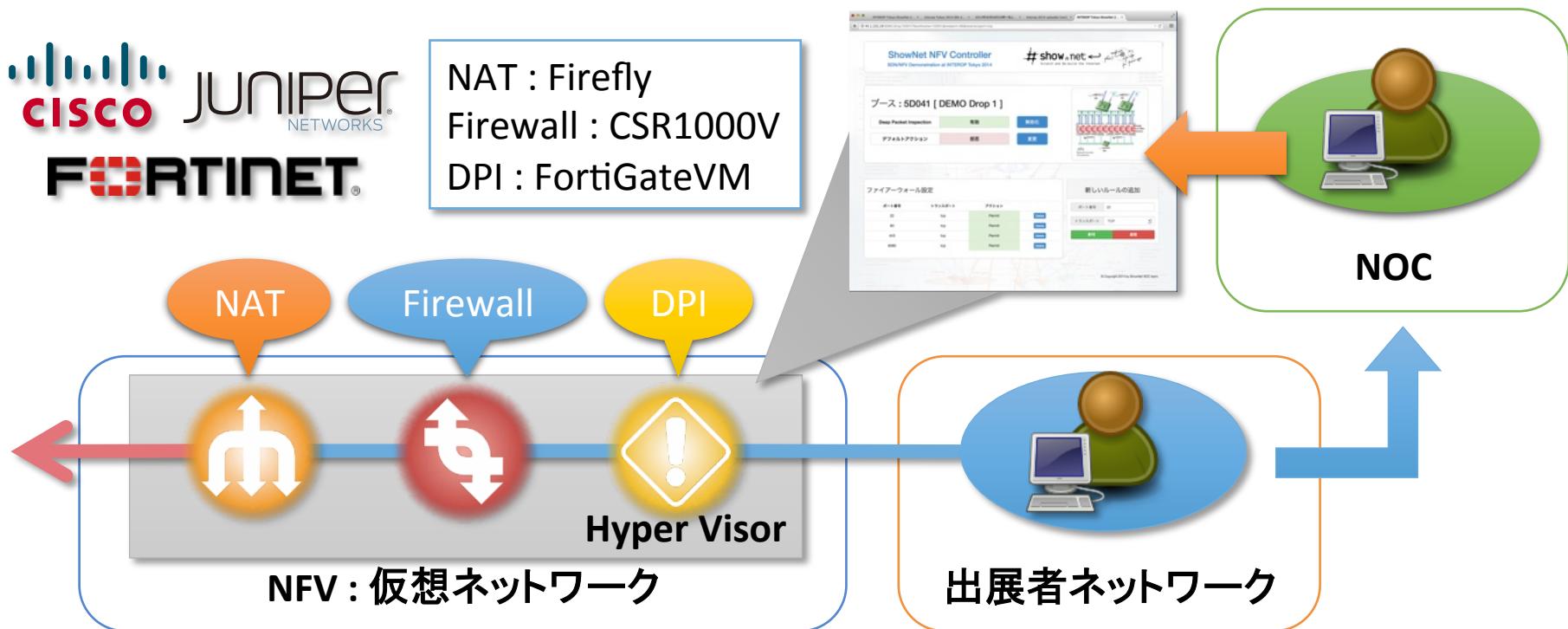


1出展者1仮想ネットワーク

- 1つのVirtual Network Function = “ネットワークの機能”は、1つのVirtual Appliance(VA)によって実現される
- 仮想ネットワークはNAT, Firewall, DPIの3種類のVAによって構築
- 各仮想ネットワークの設定はWeb画面からオンデマンドに可能



NAT : Firefly
 Firewall : CSR1000V
 DPI : FortiGateVM



ShowNet NFV Control Panel

INTEROP Tokyo ShowNet 2... × Interop Tokyo 2014 [RS: 4... × 2014年06月08日20時~地上... × Interop 2014 uploader [noc] × INTEROP Tokyo ShowNet 2... ×

← 45.1.131.19:8080/drop/5D041?boothname=5D041&newport=80&newtransport=tcp

ShowNet NFV Controller
SDN/NFV Demonstration at INTEROP Tokyo 2014

ブース : 5D041 [DEMO Drop 1]

Deep Packet Inspection: 有効 (Enabled) / 無効化 (Disable)

デフォルトアクション: 拒否 (Deny) / 変更 (Change)

ファイアーウォール設定:

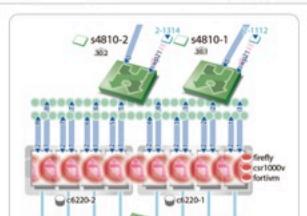
ポート番号	トランSPORT	アクション
22	tcp	Permit
80	tcp	Permit
443	tcp	Permit
8080	tcp	Permit

新しいルールの追加:

ポート番号: 22 / トランSPORT: TCP

許可 (Allow) / 拒否 (Deny)

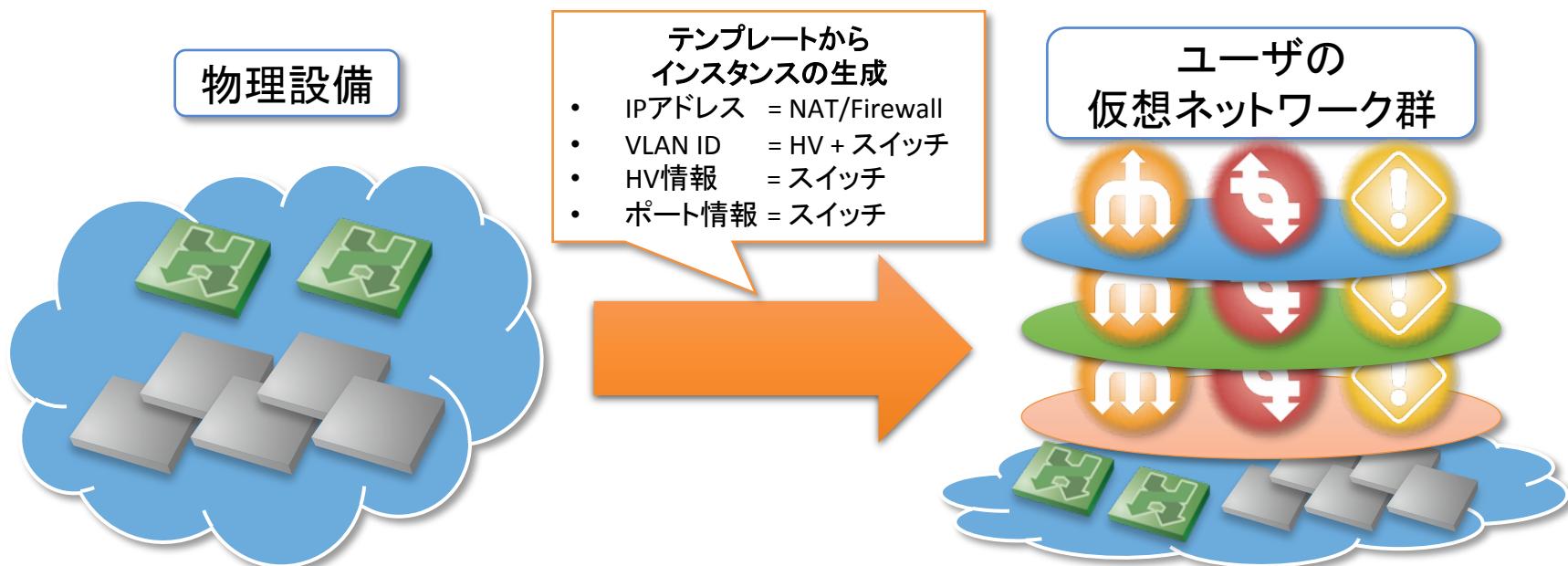
Network Function Virtualization (NFV) Diagram:



Copyright 2014 by ShowNet NOC team.

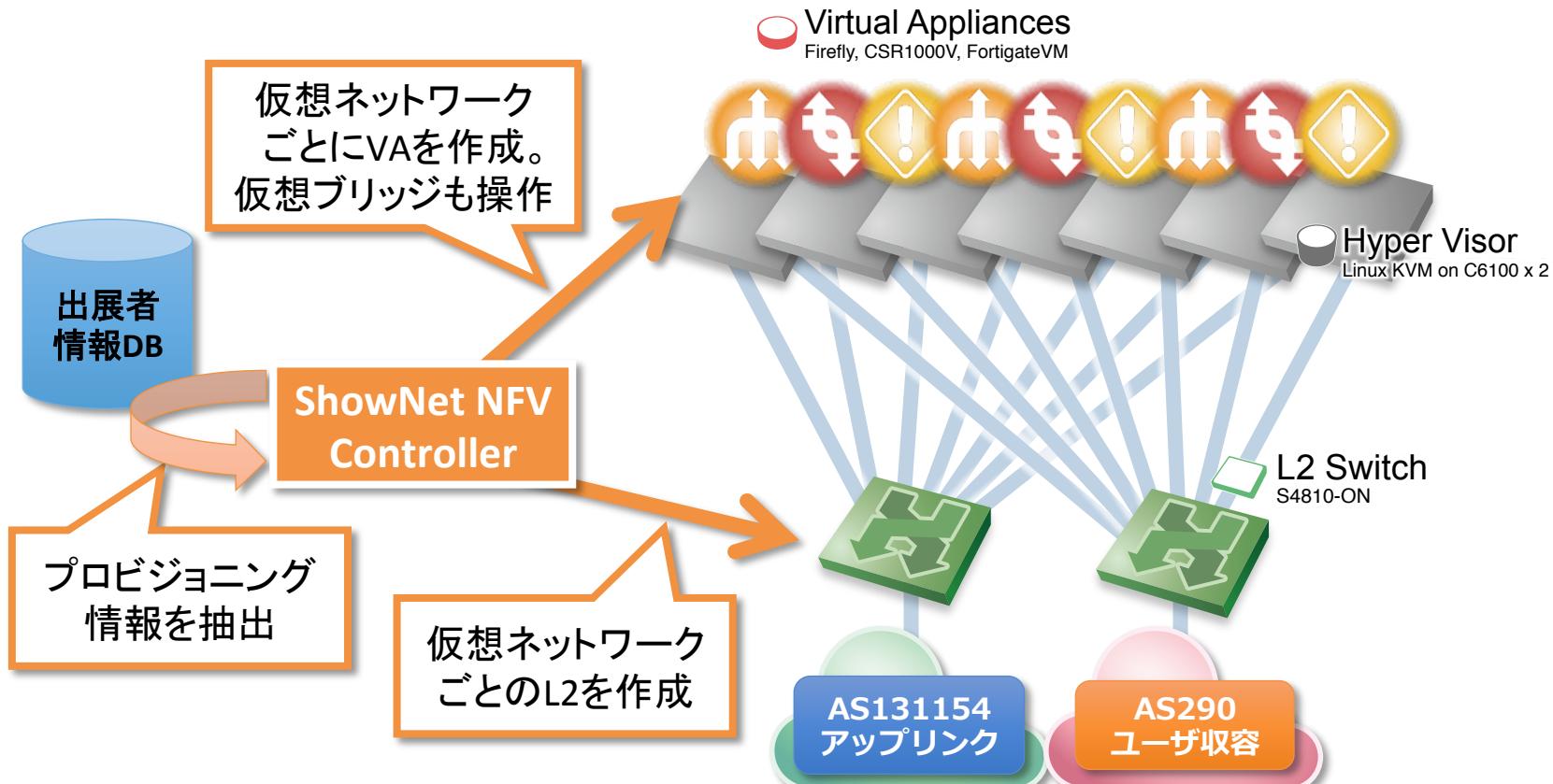
仮想ネットワークの構築

- ネットワークのテンプレート化と生成
 - 仮想ネットワークのテンプレートを用意
 - 変数化されたユーザごとの情報を埋め込んで仮想ネットワークを生成

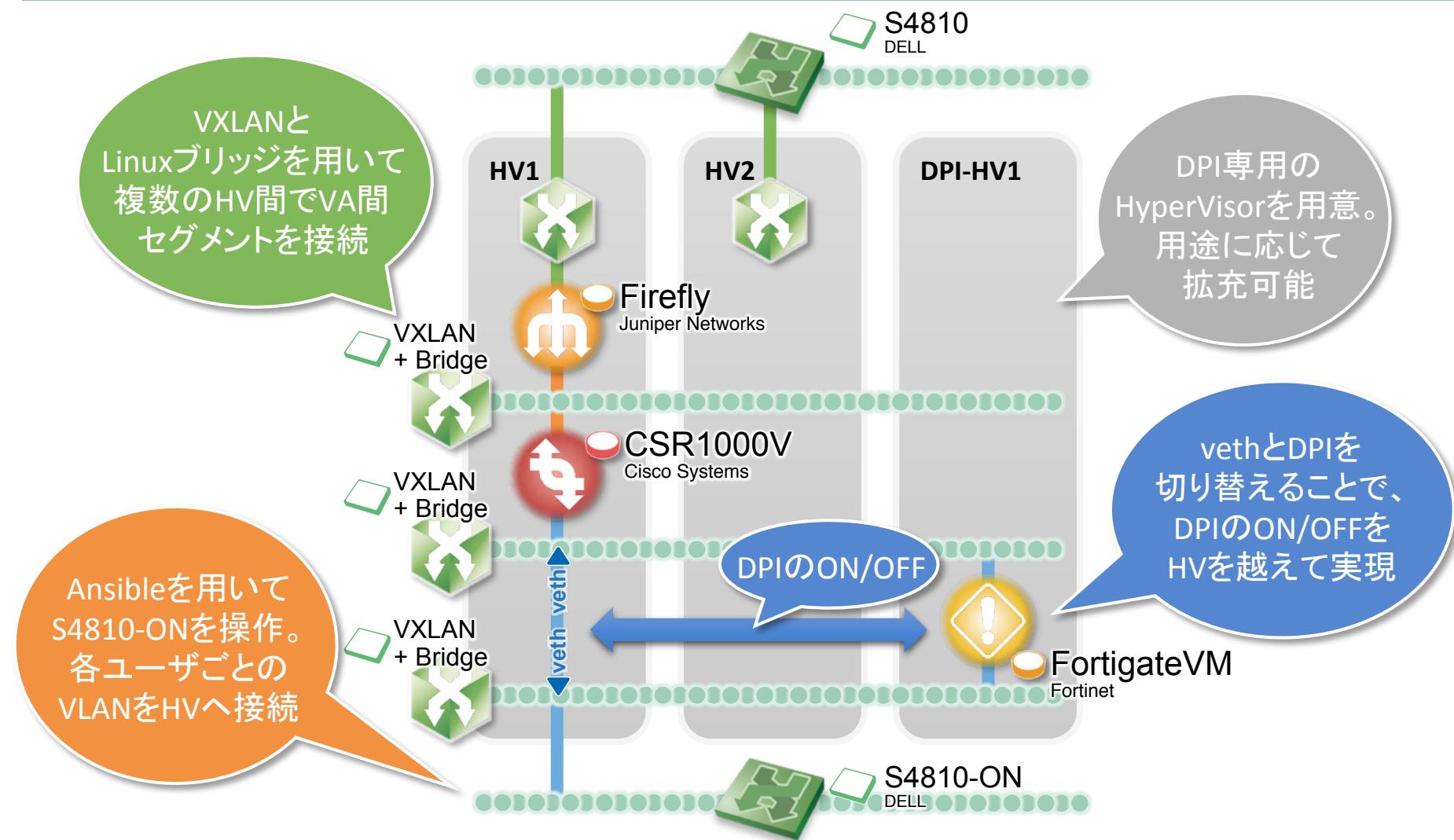


動作概要

- ・ コントローラから仮想ネットワークをデプロイ
 - ・ 2013年のSDN@ShowNetと同様の手法



詳解:1出展者のための1仮想ネットワーク



やってみて解ったこと

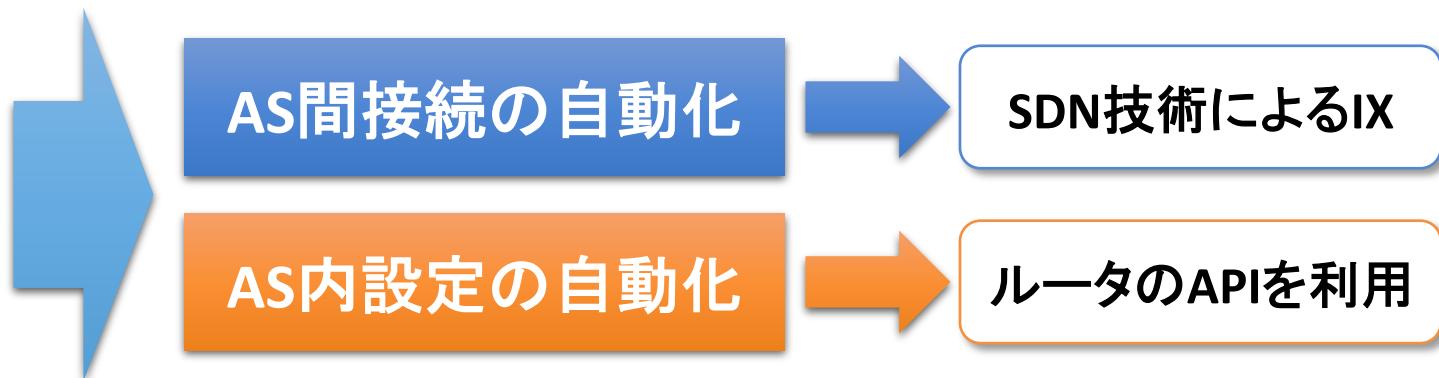
- **仮想ネットワークとプロビジョニングは◎**
 - 2013年のShowNetで得たノウハウもありました
 - 今年はKVMとLinux Bridge、昨年はVMwareとOpenFlow
 - 実質30出展者の構築に4,50分程度
- **サーバ運用の知識と経験をネットワーク運用に**
 - 仮想化は、汎用サーバと切っても切り離せない
 - サーバ運用で溜めた知識や経験を、仮想ネットワークの構築と運用に大きく役立てることができる
 - プログラミング/スクリプティングしよう！
- **性能面にはまだ課題も**
 - IXIAさんの協力を得て仮想ネットワークの性能を計測
 - Linuxのソフトウェアパケット転送のボトルネック
 - Intel DPDKなど、今後の高速化技術に期待

SDNによる ASを越えた接続の自動化

ASを越えてネットワークをつなぐには

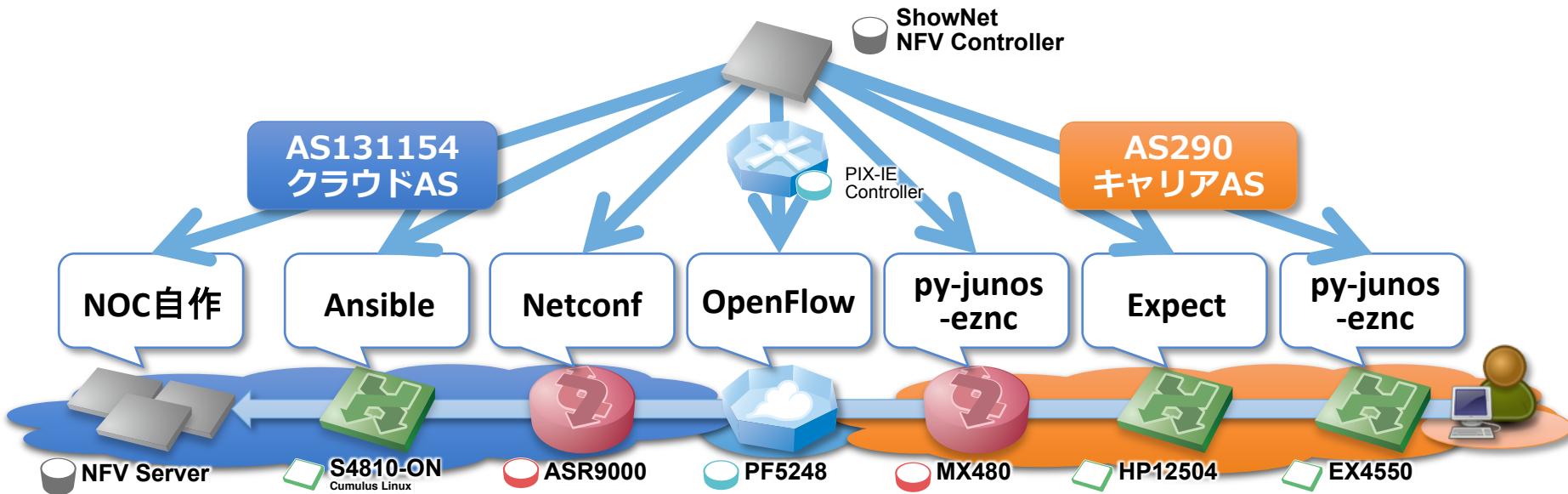
- **クラウドAS上のNFV、キャリアAS上のユーザ**
 - “ネットワークの機能”はクラウド上に実現
 - Firewall、DPIなどの機能を選択的に利用可能

キャリアASからクラウドASにあるNFVまで、
どうやってユーザのネットワークを接続する。。。？



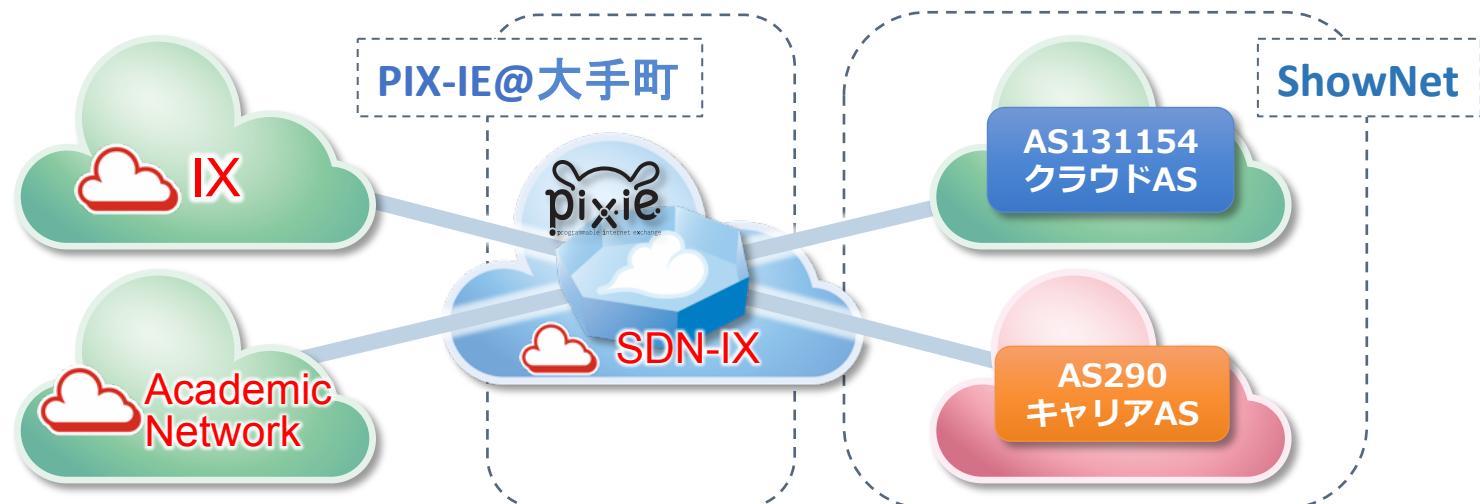
ASを越えたネットワーク接続の自動化

- **AS間ネットワークの自動化**
 - **PIX-IE** : VLAN接続のための APIを持つInternet eXchange
- **AS内ネットワークの自動化**
 - 各機器の持つ様々なAPIを利用
- 様々なSDN技術を活用し、ネットワークをデプロイ
ゼロオペレーションでクラウドASのNFVへ接続



AS間接続の自動化 : SDN-IX

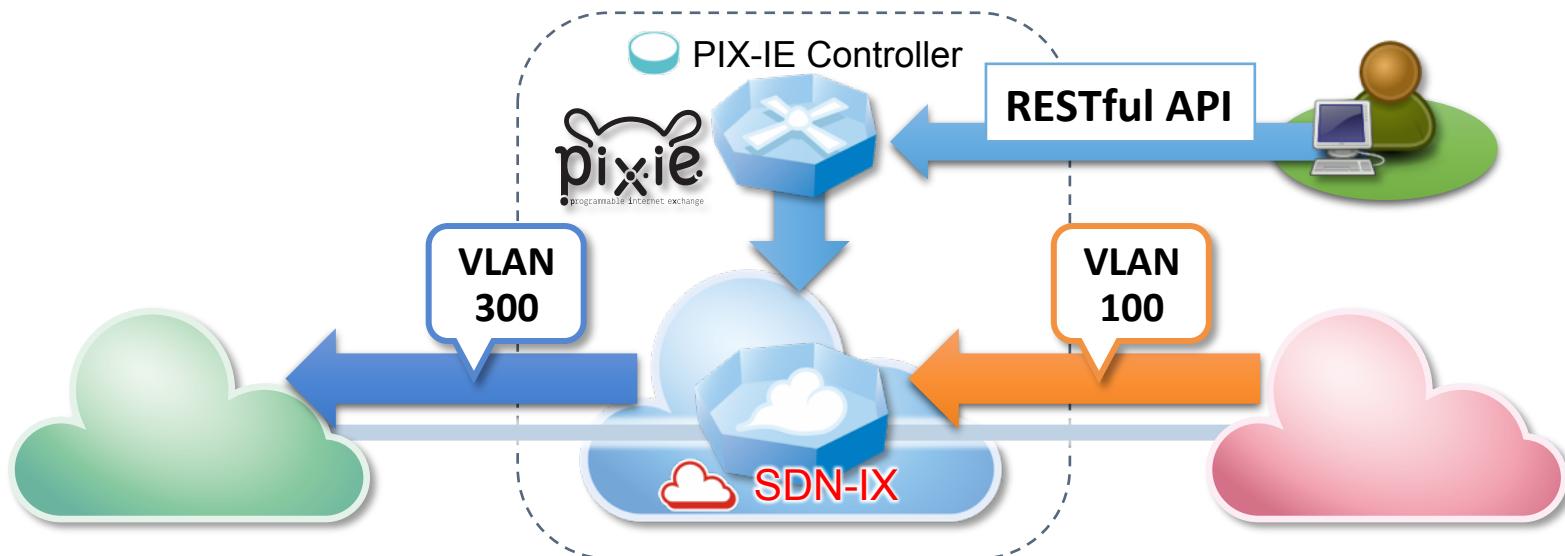
- **PIX-IE: Programmable IX in EDO**
 - 学術組織(WIDE, NECOMA project)からのコントリビューション
 - OpenFlowによって構成されたInternet eXchange
 - 複数AS間でのVLAN接続機能を提供



ShowNetにおけるPIX-IEの構成

- **PIX-IE Controller**

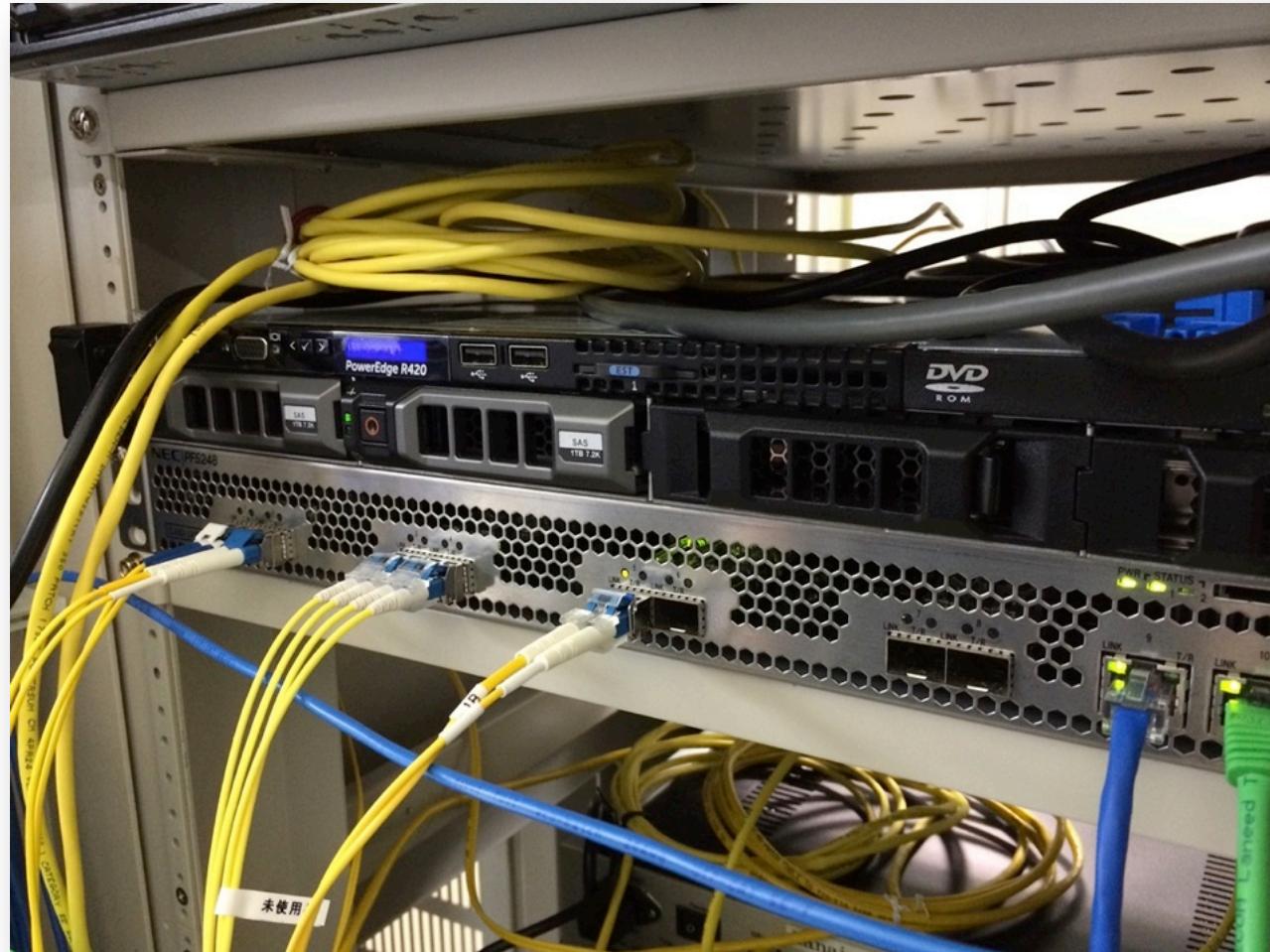
- PIX-IEに接続するAS間でVLAN IDを変換して接続
 - ASごとにVLAN ID空間を分離
- RESTful APIによるVLAN接続作成の自動化
 - 接続する各ASが接続リクエストをコントローラに送信



大手町に設置した機材

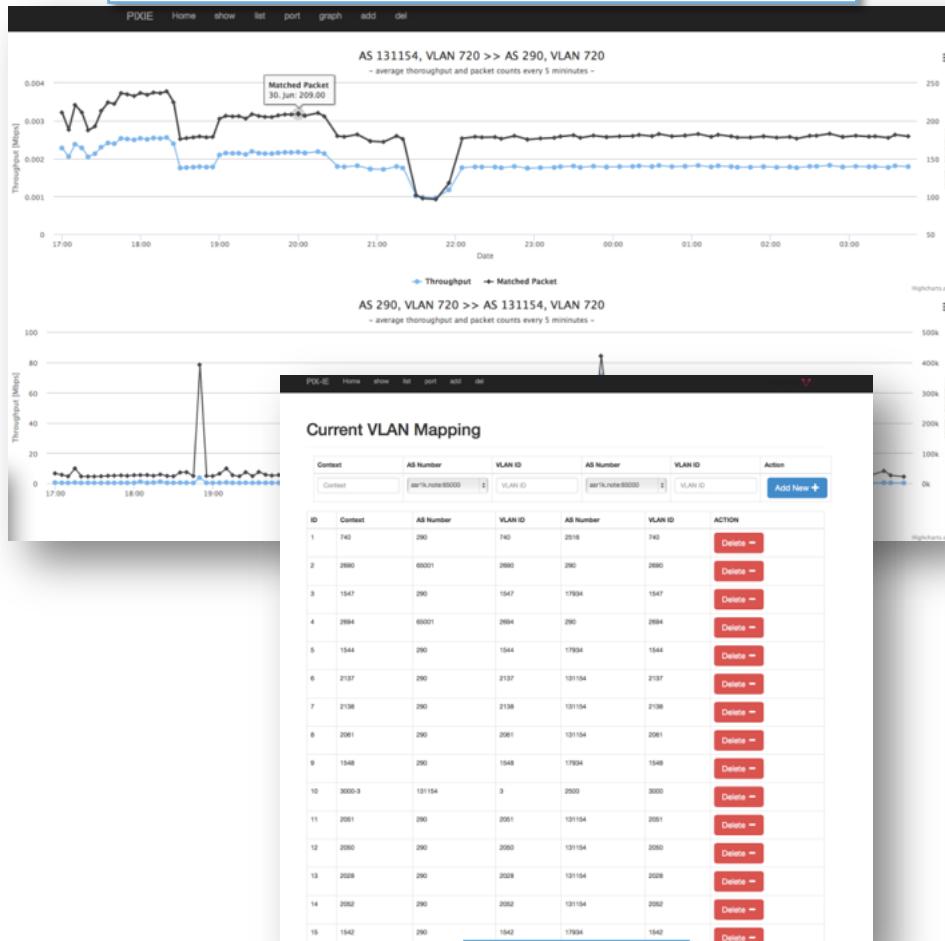


NEC



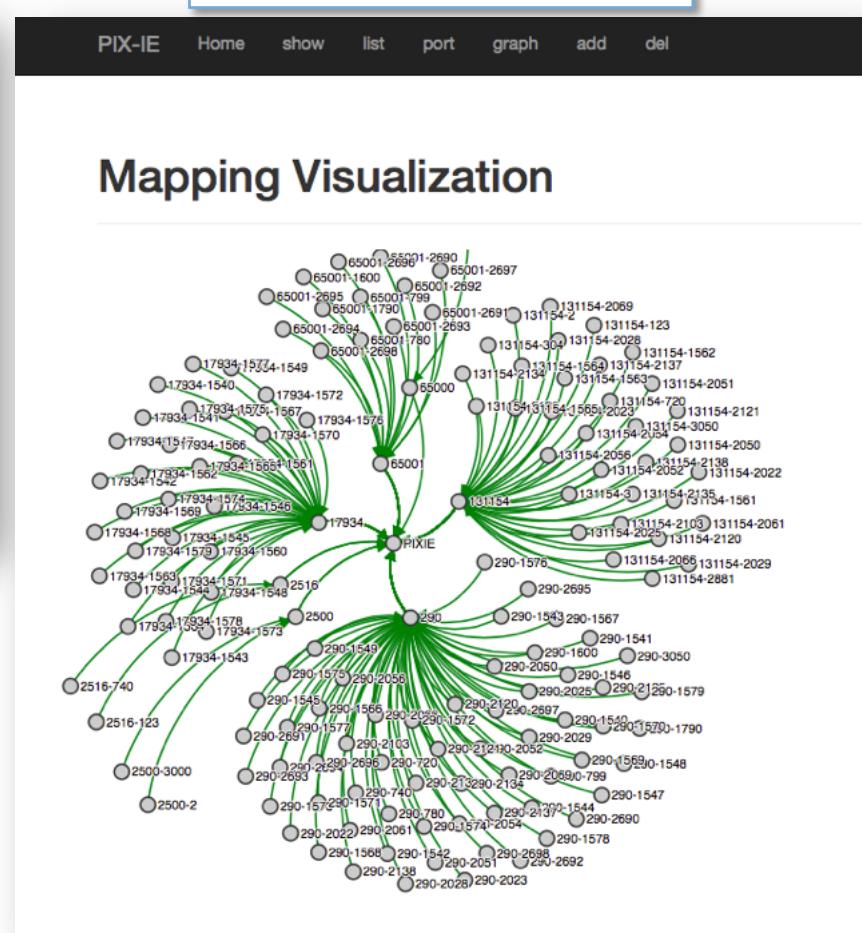
SDN-IX WebUI

各変換フローのスループット/パケット量



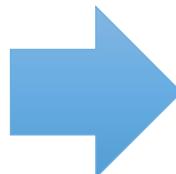
変換リスト

AS間のVLAN変換トポロジ

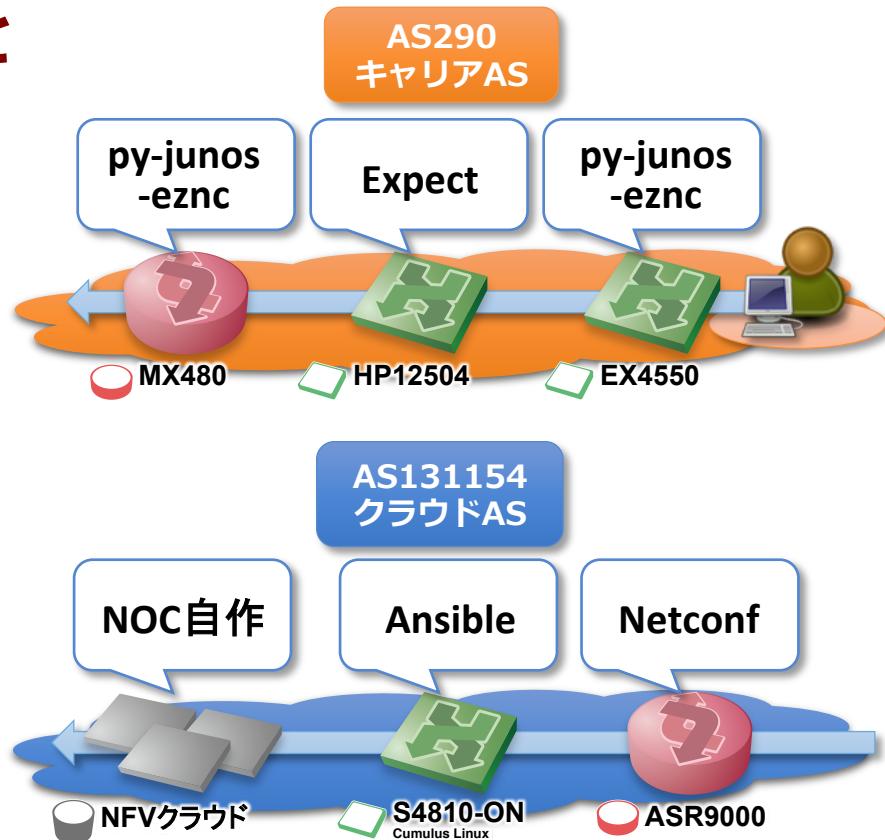


AS内ネットワーク設定の自動化

- AS間接続はSDN-IXを用いて自動化を実現
- AS内はSDNで自動化
 - ユーザごとのVLANを1つ1つ設定するのは現実的でない(OPEX)
 - しかし、全ての機器を突然OpenFlow機器に置き換えるのは難しい

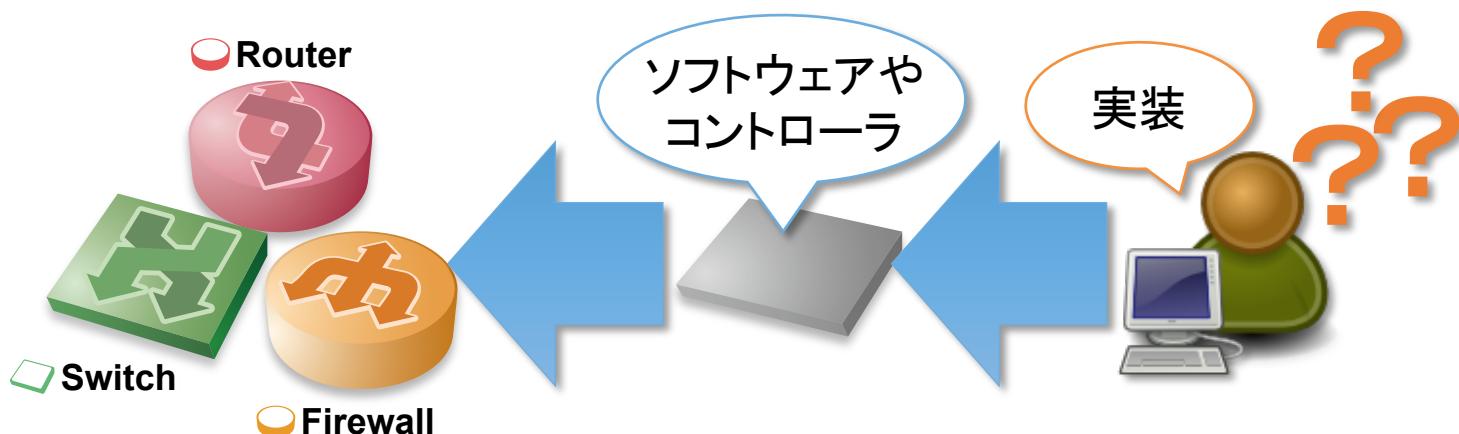


機器に搭載されている
さまざまなAPIを利用



ネットワーク運用自動化の難しさ

- ・ ソフトウェア制御で設定の変更を自動化
- ・ ベンダーや製品、バージョンごとに異なるAPI
 - ・ 実際の現場ではさまざま機器を利用している
 - ・ 全ての機器を網羅するAPIは現状では存在しない
- ・ エラーハンドリングの難しさ
 - ・ Debuggabilityの欠如



ネットワーク機器制御のためのAPI

- **SouthBoundはOpenFlowだけじゃない！**
 - 古今東西、さまざまな機器制御技術がある
 - 長年ネットワークオペレータに愛されてきた技術から、最新の自動化ツールまで幅広く検証

機器名	API/ソフトウェア
Juniper EX4550	py-junos-eznc
HP HP12504	Expect
Juniper MX480	py-junos-eznc
PIX-IE : NEC PF5248	OpenFlow
Cisco ASR9000	Netconf
DELL S4810-ON	Ansible



Expect

- 古くからあるUNIXコマンド
 - Configurationを知っていれば容易に実装可能
- Programmabilityの欠如
 - 結局は簡易な文字列処理の連続
 - 条件分岐は可能だが柔軟性不足
 - エラーハンドリング
 - ほぼ不可能
 - Timeoutに頼るしかない

```
#!/bin/sh
#
#
host=$1
conf=$2
user="username"
pass="password"

web=10.11.194.248

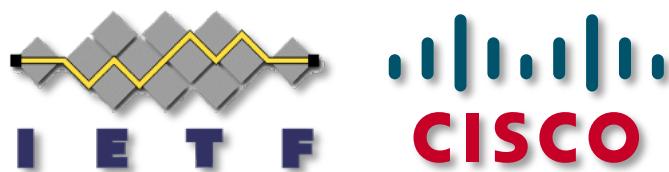
if [ ! "$conf" ]; then
    echo "update-vsrx.sh [HOST] [CONFIGNAME]"
    exit 1
fi

expect -c "
set timeout 5
spawn telnet $host

expect login: ; send \"$user\n\"
expect Password: ; send \"$pass\n\"
expect \"*\r\" ; send \"configure\n\"
expect \"*#\r\" ; send \"load override http://$web/$conf\n\"
expect \"*#\r\" ; send \"commit\n\"
expect \"commit complete\" ; send \"\n\"
expect \"*#\r\" ; send \"exit\n\"
expect \"*\r\" ; send \"exit\n\"
"
```

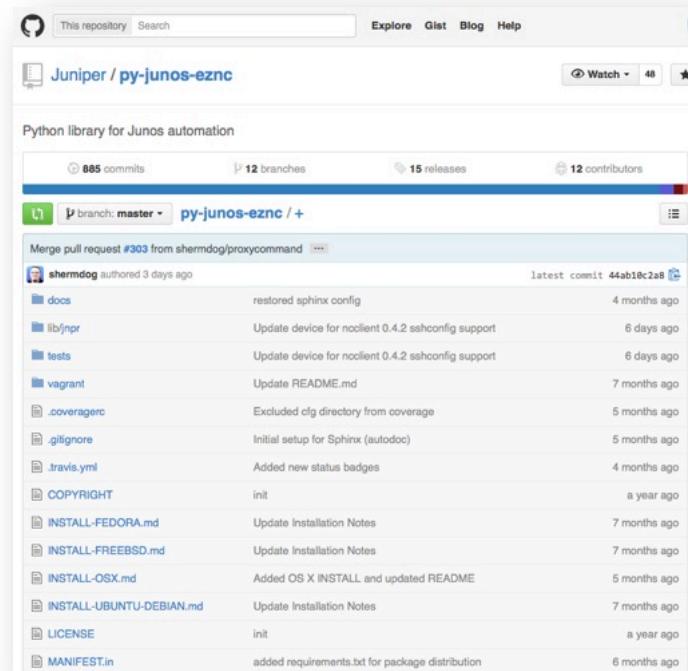
NETCONF

- **標準化された技術 : RFC 6241**
 - XMLによるConfigの投入や状態の取得
 - トランSPORTと、CommitやValidateなど、汎用的な”操作”が標準で規定されている
 - エラーハンドリングが可能
- **ベンダーごとの差異**
 - 投入するXML自体は、ベンダーや機器ごとに大きく異なる(YANGデータモデル)
 - トランSPORTにもベンダーごとにクセがある
 - 機器によってサポートされた処理のみ



py-junos-eznc

- **JuniperのNETCONFラッパライブラリ**
 - JUNOSを外部から制御するためのPythonライブラリ
 - 実際の機器との通信はNETCONFで行う
 - しかし、ユーザはNETCONFを意識する必要がない
 - エラーハンドリングも容易
- **専用ライブラリ**
 - JUNOSのためのライブラリ
 - モジュール化
 - ネットワーク機器の制御に特化したさまざまな機能



実例：py-junos-eznc

- テンプレートからVLAN設定を生成、投入

```
from jnpr.junos import Device
from jnpr.junos.utils.config import Config

dev = Device (host = hostname, user = username, password = password)

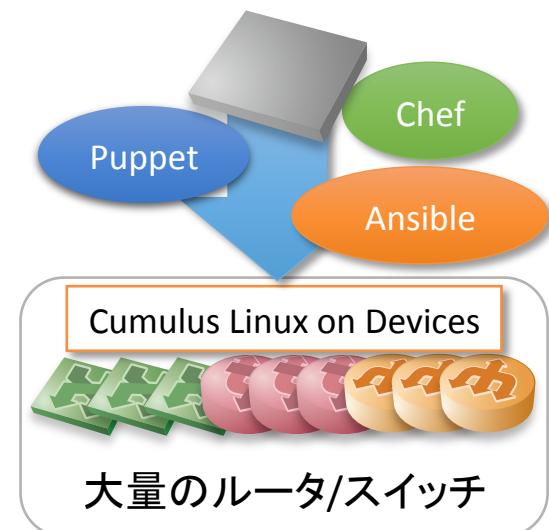
dev.open ()
cu = Config (dev)
template_vars = { 'intf1' : intf1, 'intf2' : intf2, 'vlan_id' : vlan }
cu.load (template_path = template, template_vars = template_vars)

res = cu.commit ()
if res :
    print res
    print "commit sucess"
else :
    print "commit failed"

dev.close ()
```

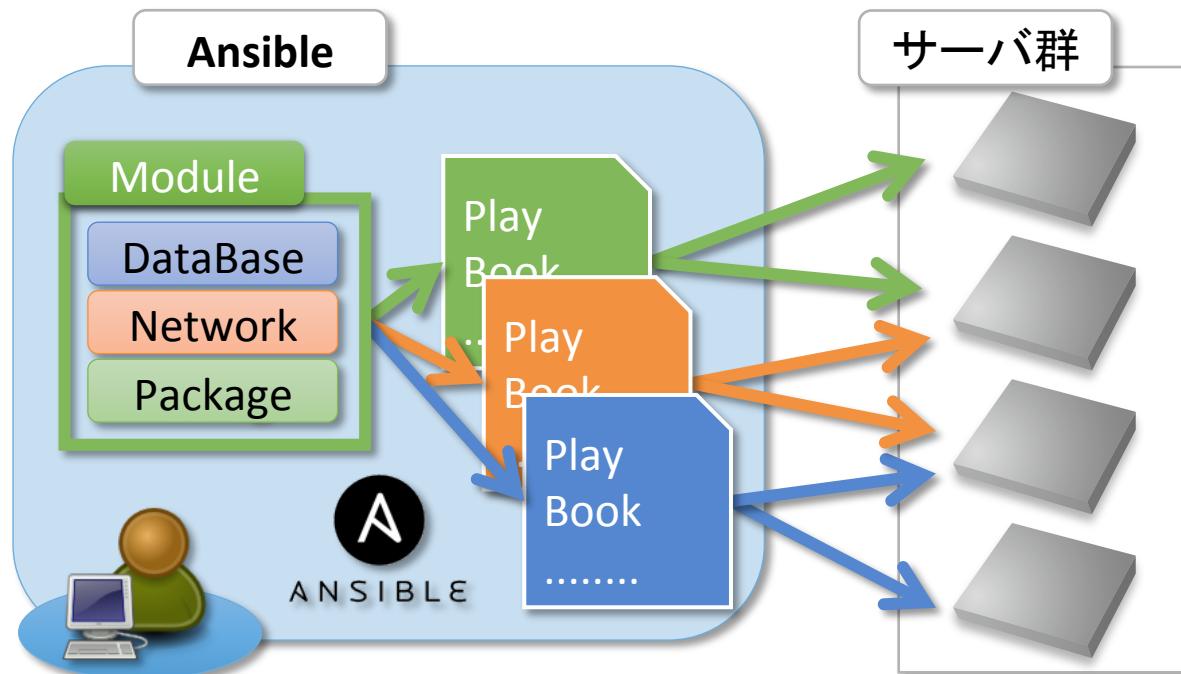
Cumulus Linux + Ansible

- サーバ運用のノウハウをネットワーク機器へ
 - Cumulus Linuxが動作するDELL S4810-ONを、サーバ構築自動化ツールであるAnsibleを用いて設定
 - Programmability、Debuggabilityはとても柔軟
- 新しい考え方でのソフトウェアによる機器制御
 - write memoryのようにstateを保存することはできない
 - 今までとは全く違う考え方でネットワークを構築する必要がある



Ansibleによる設定の自動化

- オープンソースなサーバ設定自動化ツール
 - 様々な操作がモジュールとして用意されている
 - 実行したいタスクをPlaybookに記述



Ansible Playbook

- NFVを収容するDELL S4810-ONを操作

```
---
- hosts: cumulus
  sudo: yes
  tasks:
    - name: add vlan interface from asr9k
      vlan: vlan={{vlan}} port=swp1 name=swp1.{{vlan}} state={{state}}

    - name: add vlan to vxlan-node
      vlan: vlan={{vlan}} port=swp8 name=swp8.{{vlan}} state={{state}}

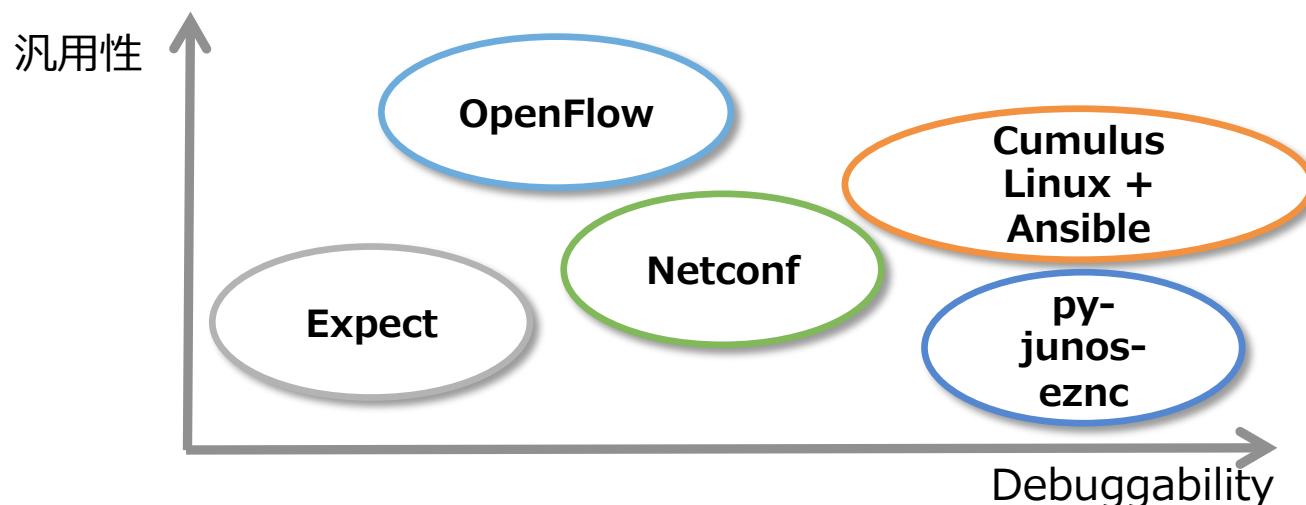
    - name: add bridge for vlan
      linux_bridge: bridge=vbr{{vlan}} state={{state}}

    - name: add vlan interface of uplink to bridge
      linux_bridge_port: bridge=vbr{{vlan}} port=swp1.{{vlan}} state={{state}}

    - name: add vlan interface of vxlan-node to bridge
      linux_bridge_port: bridge=vbr{{vlan}} port=swp8.{{vlan}} state={{state}}
```

様々なAPIを使ってみて

- ソフトウェアによるネットワーク機器の制御
 - ソフトウェアによる自動化はネットワークでも強力
 - 以前からノウハウがあり、現在は様々なAPIが誕生
 - それぞれに長所と短所があり使いどころがある
 - 目的や環境、機器、スキルに合わせて最適なAPI、ソフトウェアを利用しよう

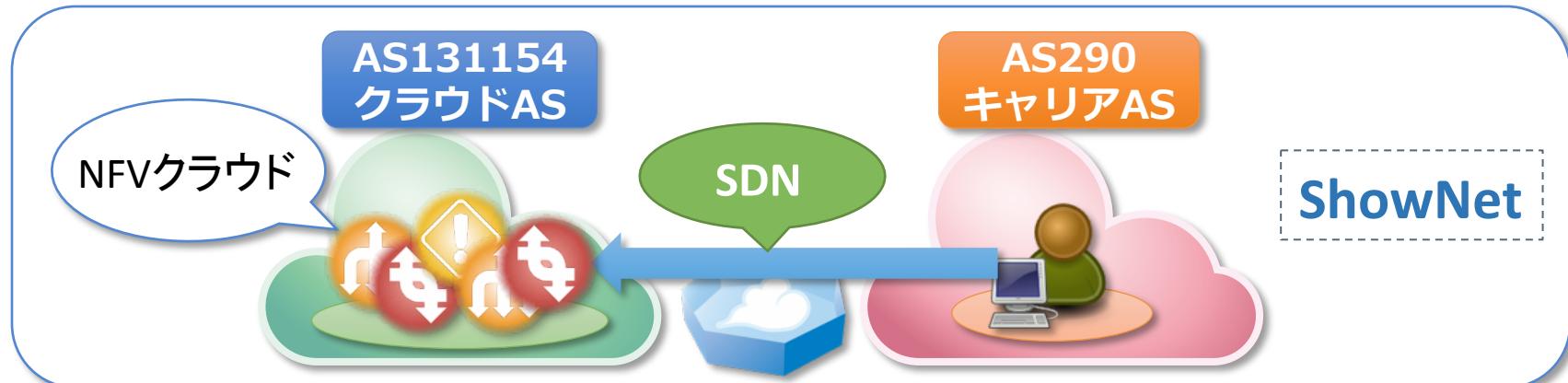




まとめ

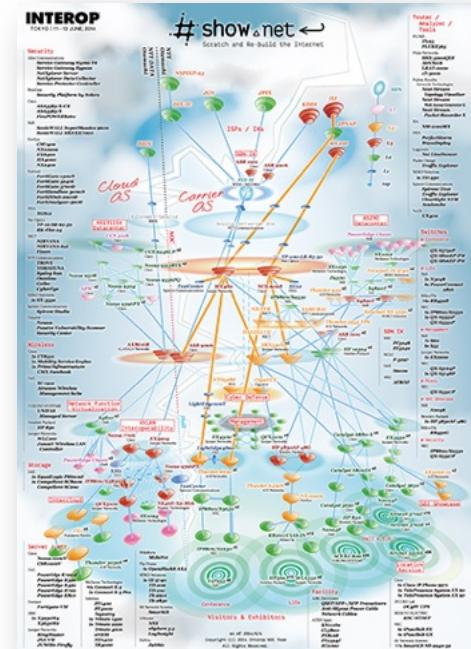
ShowNet 2014におけるSDN/NFV

- ・ ネットワークの機能もクラウドへ
- ・ クラウドASにNFVによる仮想ネットワークを構築
 - ・ ネットワークのテンプレート化と生成による自動化
 - ・ 複数のVAによる柔軟なネットワーク
- ・ キャリアASからクラウドASへの接続をSDNで自動化
 - ・ SDN-IXによるAS間接続の自動化
 - ・ さまざまなAPIやソフトウェアを利用したAS内接続の自動化



INTEROP Tokyo ShowNet

- **未来のネットワークの1つのカタチ**
 - 10年先のインターネットをつくる
 - その1つのモデルとしての、SDNとNFVの利用
- **Live Network**
 - ShowNetは生きたネットワーク
 - 実際に動くSDNとNFV
- **相互接続性**
 - 同じ目的でも様々な技術がある
 - それぞれの特徴と活用方法
 - そしてフィードバック



!show \triangle net ←

Scratch and Re-build the Internet



INTEROP®
TOKYO | 11 - 13 JUNE, 2014