



OpenStack Days Tokyo 2015

ホントのところどうなの？ OpenStack
～機は熟したのか？～

2015/2/4

ユニアデックス株式会社

戦略マーケティング部

田中 克弥/吉本 昌平

■ 会社概要



社名	ユニアデックス株式会社
代表者	代表取締役社長 入部 泰 (いりべ やすし)
住所/TEL	〒135 - 8560 東京都江東区豊洲1-1-1 03-5546-4900 (大代表)
設立	1997年3月4日
資本金	7億5,000万円
従業員数	3,174名(2015年12月1日現在)
売上高	1,278億円 (2015年3月期) *旧ネットマークス分含む

日本ユニシスグループの『インフラトータルサービス』企業

■ 自己紹介<田中 克弥>



Copyright©2015 UNIADEX, Ltd. All rights reserved.

● 業務

- ✓ マーケティング担当

● 主な経歴

- ✓ ネットワークエンジニア
- ✓ サーバーエンジニア
- ✓ Linuxアプライアンス開発
- ✓ Webアプリ開発(Vim派)
- ✓ サーバー仮想化エンジニア
- ✓ 2009~2011年 米国駐在
- ✓ プライベートクラウド企画

● 趣味

- ✓ フットサル
- ✓ 旅行

■ 自己紹介<吉本 昌平>

● どんな人？

- > MSX IBM PS/V Master 自作
NE (ASP) PG (Linux)
NE (企業コア)
企画 (仮想化 SDN)

> 自宅に山ほどある某社ネットワーク機器を処分中

● 日々の仕事

- > 今年からSDNエバンジェリスト / アーキテクト

● 趣味

- > 自作 卒業
- > コンピュータ全般 卒業？
- > 写真
- > 車 稟議中



OpenStackに関する Slerの悩み

興味の幅が広い

■ 本日のおはなし

1. 【入門編】 OpenStackってどうよ？
2. 【上級編】 Neutronって何がうれしい？



OpenStackってどうよ？



群雄割拠



18

■ いろいろなOpenStack

コミュニティ版



商用ディストリビューション

Cloudscaling, HP, Mirantis, metacloud, Nebula, StackOps, Red Hat, Suse, Oracle, Pistoncloud, Ubuntu, VMware

2015年2月現在商用ディストリビューション提供を発表あるいは計画している企業(アルファベット順)

<http://www.openstack.org/marketplace/distros/>

■ OpenStack周辺機材の注意点



ネットワークメーカーA

対応

OpenStack A

非対応

OpenStack B



ストレージメーカーB

対応

OpenStack C

非対応

OpenStackの 落とし穴

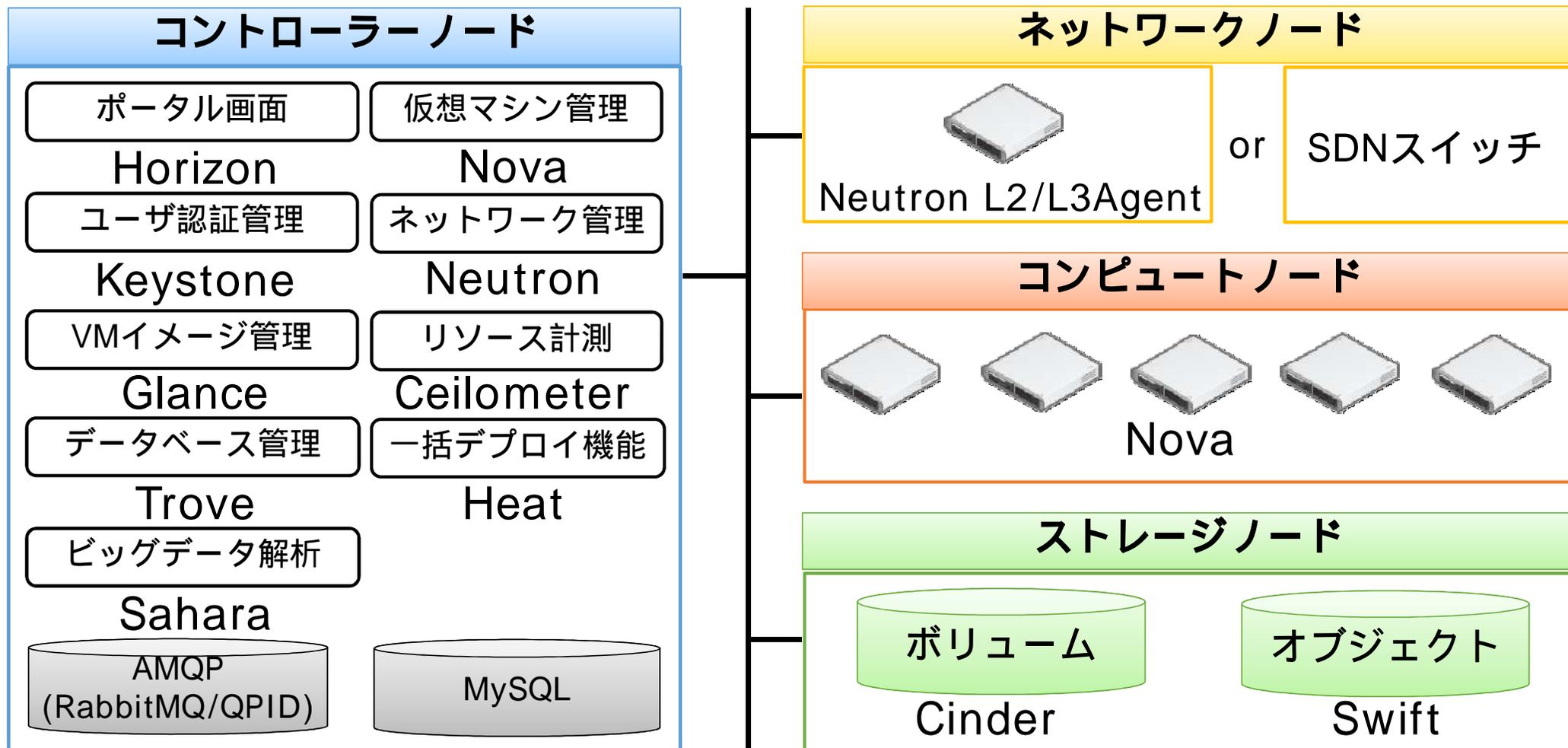
<https://flic.kr/p/8z11Xd>



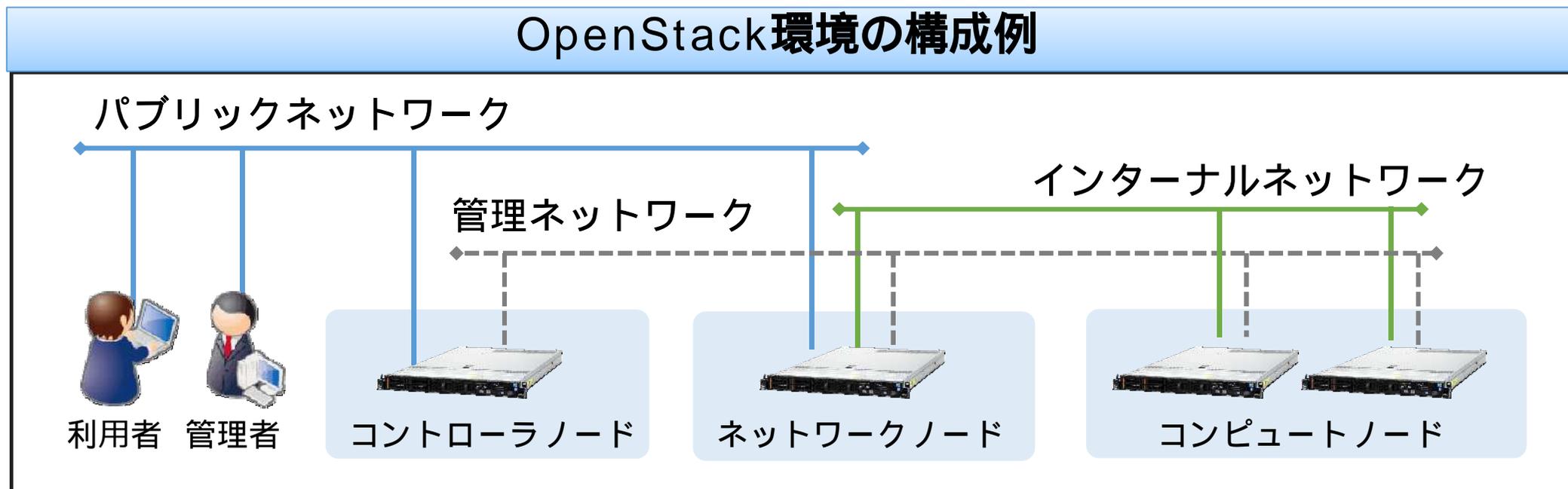
落とし穴その1

既存環境からの移行

■ おさらい) OpenStackの主要コンポーネント



■ 落とし穴その1) 既存環境からの移行



レノボエンタープライズソリューションズ共同検証済み構成

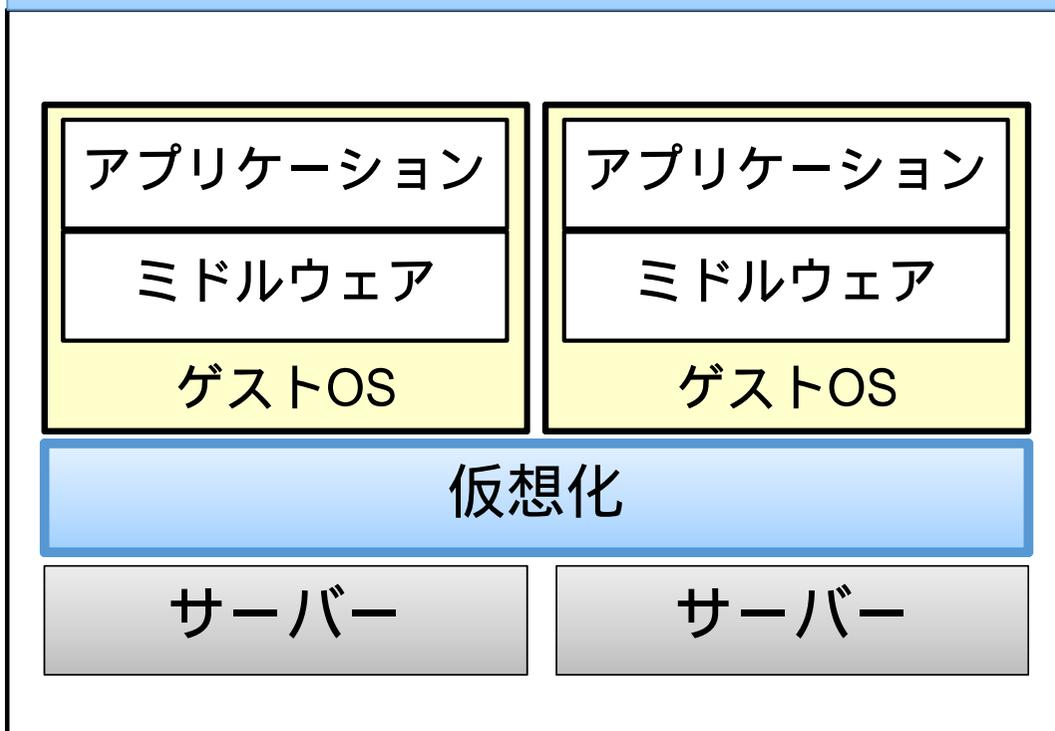
✓ VMイメージコンバート/IPアドレス体系/MACアドレスの変更が必要

落とし穴その2

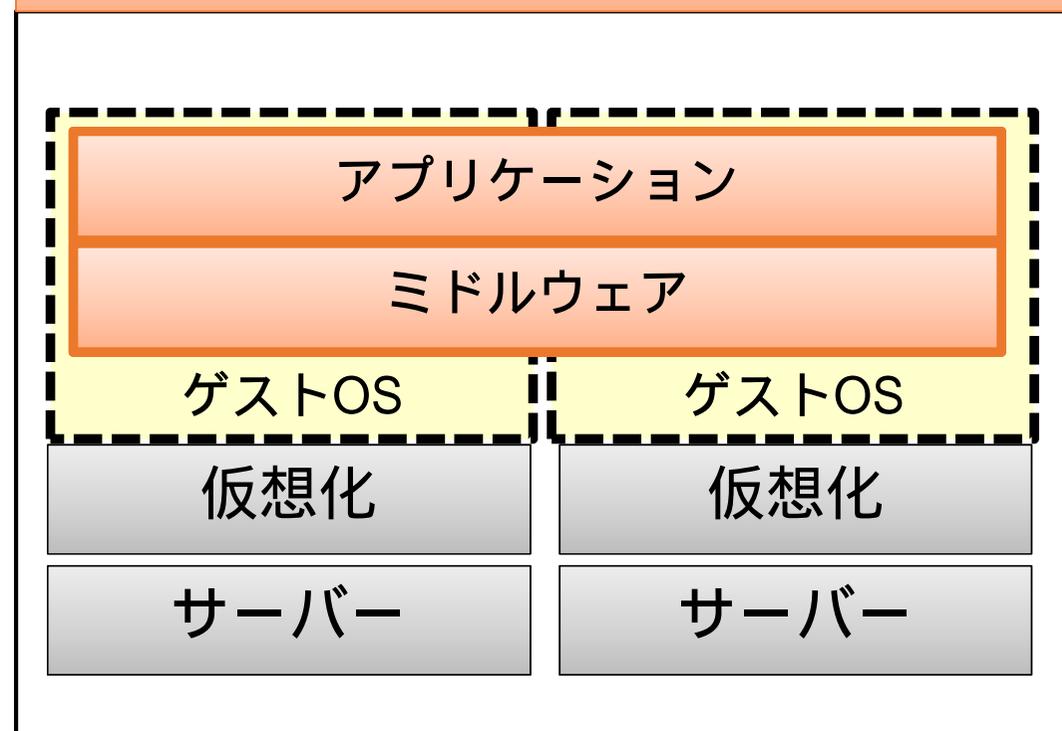
仮想化 クラウド

■ 落とし穴その2) HAに対する考え方

仮想化のHAアーキテクチャ



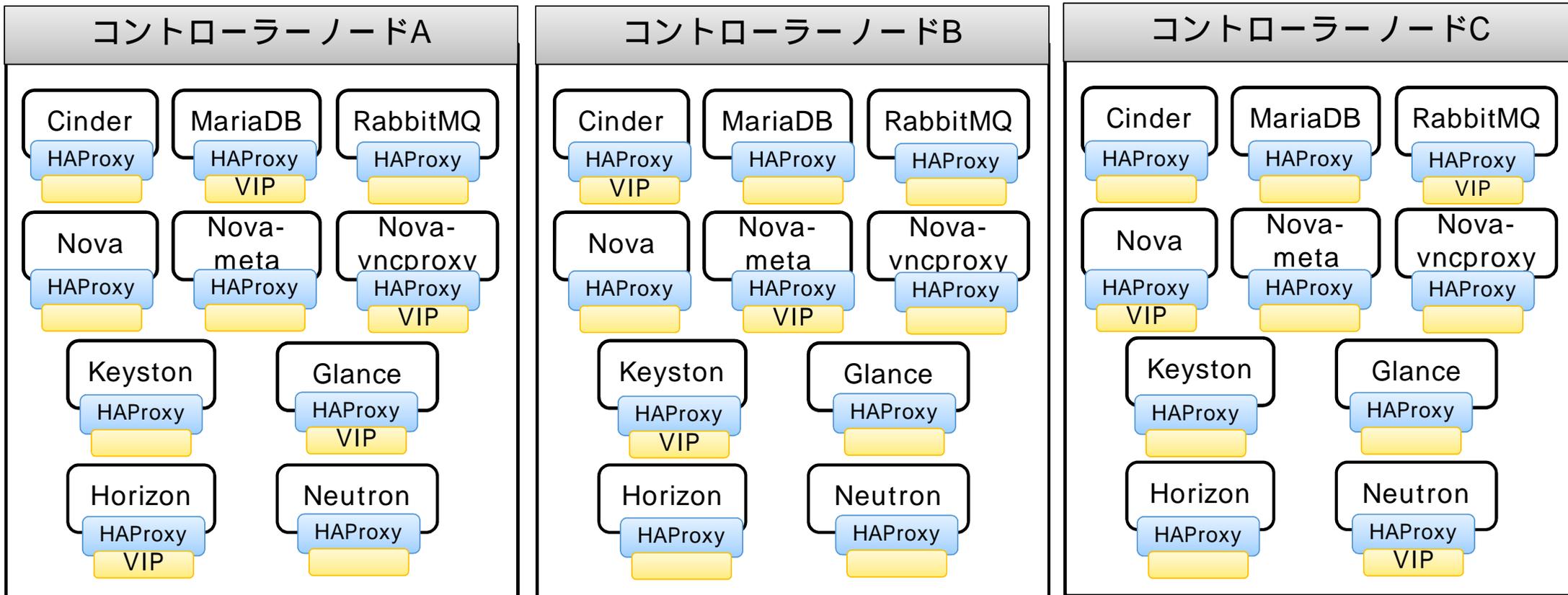
クラウドのHAアーキテクチャ



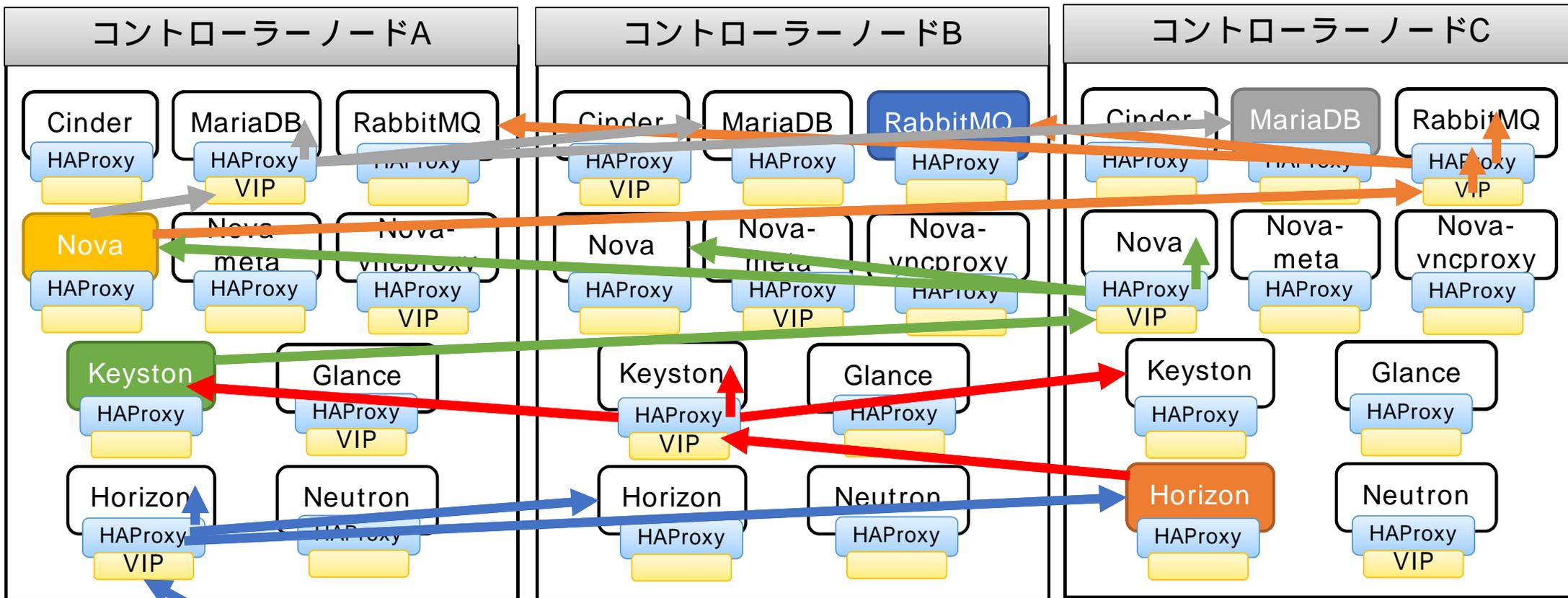
落とし穴その3

コントローラーノードの HA構成

■ 落とし穴その3) コントローラーHAの考え方



■ 落とし穴その3) コントローラーHAの考え方



✓ ユーザがHorizonから仮想マシンを操作する場合

【入門編】まとめ

1. 色々なOpenStackがあります
2. 落とし穴に気をつけましょう

Photo by Martin Fisch <https://www.flickr.com/photos/marfis75/14481855815>

Nova-Networkではなく
Neutronを選択する

■ Nova-NetworkではなくNeutronを選択する

OpenStackでネットワークを構築する場合の選択肢

■ Nova-Network

- > まだまだ現役な、いにしへの技術
- > OpenStackマニュアルでは「レガシーネットワーク」と表記

■ Neutron

- > 次世代のOpenStack Networkingを目指す後発プロジェクト

■ Nova-NetworkとNeutronのざっくりとした比較

■ Nova-Network

▶機能は限られるが**シンプルで動作実績が豊富**

▶高度なネットワークは実現出来ない

▶**将来的に廃止が予定**されている

▶いつかはNeutronへの移行を行う必要がある

▶廃止に関しては、微妙な動きがあった・・・

▶Neutronが廃止されることはない信じたい。

Nova-Networkは、Havanaで非推奨としたものの、Icehouseで一旦解除。解除の理由はFlatDHCPなどのマイグレーションパスが欠如していた。期間限定で、Nova-networkのパッチ受け付け再開

<http://docs.openstack.org/openstack-ops/content/nova-network-deprecation.html>

■ Nova-NetworkとNeutronのざっくりとした比較

■ Neutron

- ▶ OpenStack **商用環境の半数程度** で使われている
- ▶ Nova-Networkに無い **高度なネットワーク機能** をサポート
- ▶ Nova-Networkを代替する上で不足している部分も
 - ▶ マイグレーションパス、単一障害点
 - ▶ https://wiki.openstack.org/wiki/Governance/TechnicalCommittee/Neutron_Gap_Coverage
- ▶ 開発途上
 - ▶ 直近のIcehouseでプラグイン機構のアーキテクチャ変更（ML2化）があり、不安定な印象もある
- ▶ トラブルシューティングが難しい・・・

■ Neutronを選択する理由

(Nova-networkは枯れてますし
シンプルで間違いはないですが)

これから始めるなら
Neutronをオススメしたい!!

Photo by Stuart Chalmers

<https://www.flickr.com/photos/gertha/6945114788>

Neutronが目指す ネットワーク構成



■ OpenStackが目指しているのは

管理者



全部自分で管理するのは大変。利用者にある程度好きに設定して欲しいけど、コントロールが効かなくなるのは嫌だ

なるべく自分たちの思い通りにしたい。
管理者にいちいち頼むと遅いし。
だけど、必要以上の運用は嫌だ

利用者



管理者と利用者間で適切な権限移譲を行える基盤の実装

マルチテナント（テナント分割）機能で解決

- テナント = 一つのシステムやプロジェクト
- テナント単位で、管理対象を分けて利用者に移譲
- テナント内の操作の影響がテナントの外に及ばない

■ Neutronが目指すもの

■ テナント分割に必要なネットワーク機能の実装

1. テナント単位で仮想サーバーとネットワークを分離
2. 各テナント毎に仮想サーバへIPアドレスを割り当 / 管理
3. 各テナントから外部ネットワークへの通信
4. 外部ネットワークから仮想サーバーへの通信
5. 更に高度なネットワークの実装 (SDN連携やサービスチェイニング・自動化)

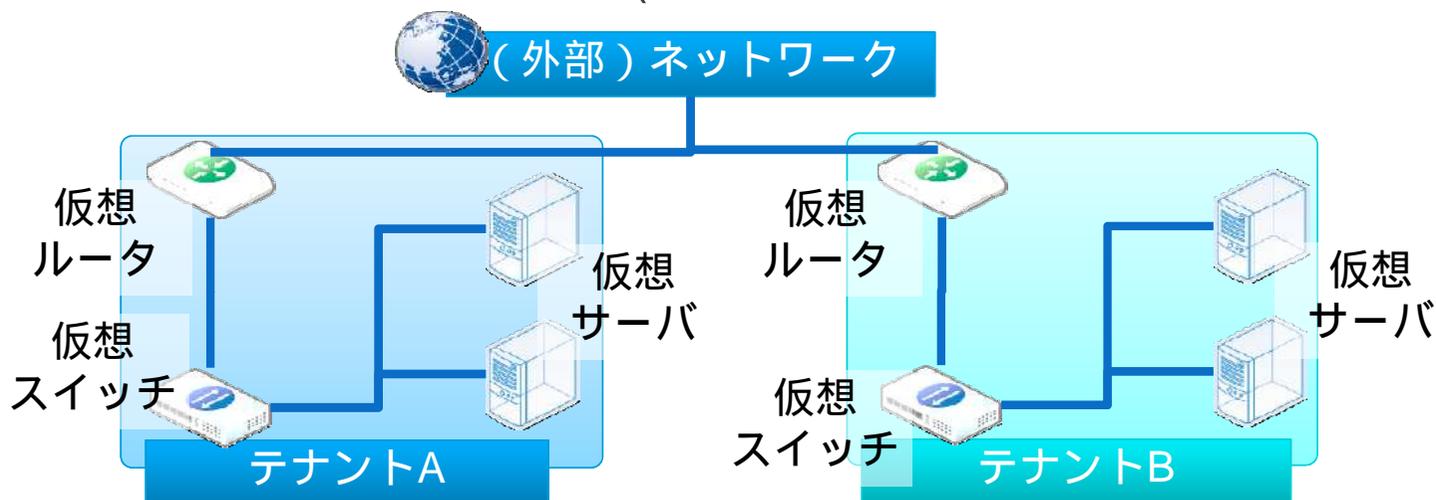




Photo by PEO ACWA

<https://www.flickr.com/photos/acwa/8677845611>

Neutronの実装

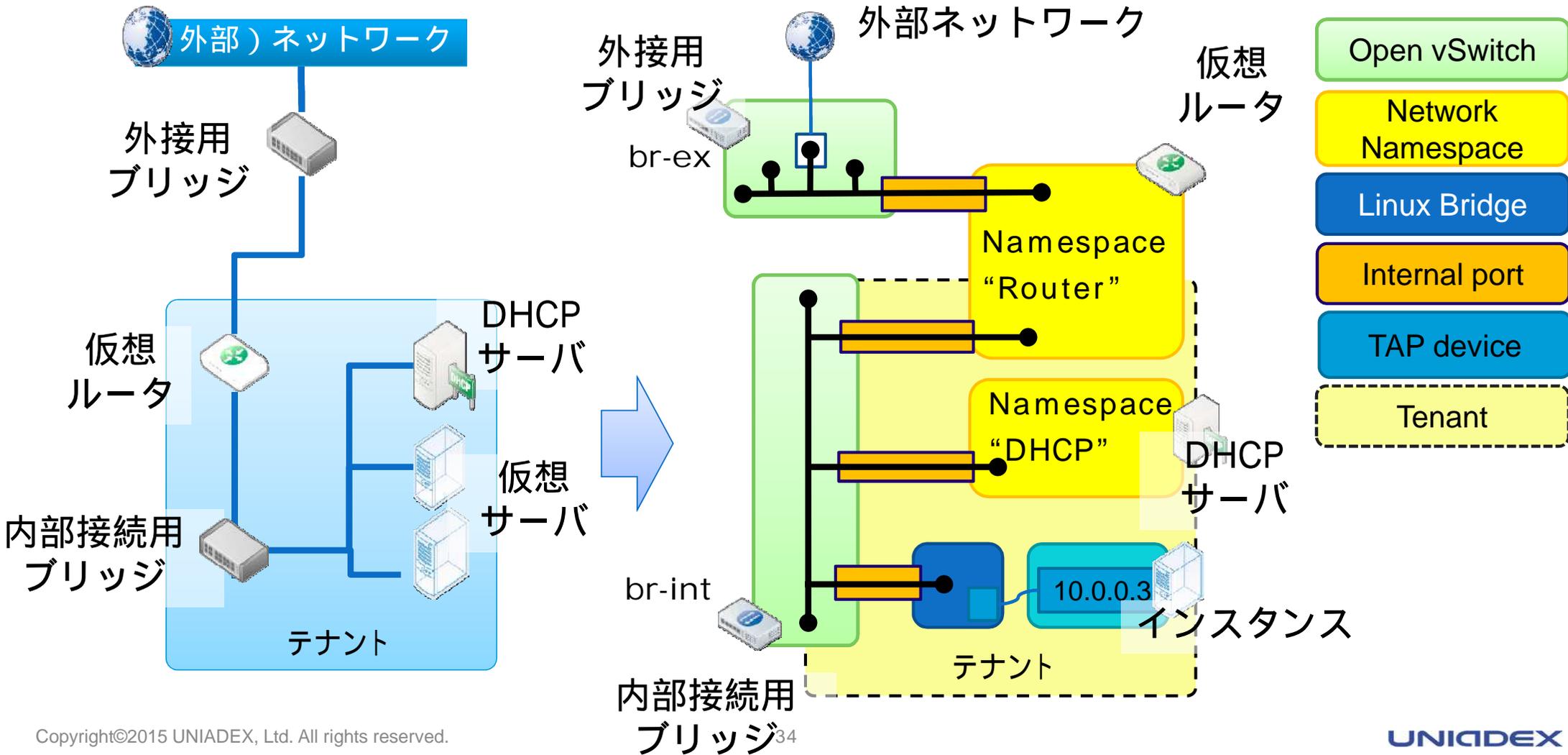
■ Neutronの実装

要件	実装
1. 各テナント毎に仮想サーバへIPアドレスを割当 / 管理	Network Namespace内で実行される dnsmasq
2. 各テナント内部から外部ネットワークへの通信	Network Namespace内で実行される iptables (NAT)、Linux ip forwarding
3. 外部ネットワークから各テナント内部への通信	Network Namespace内で実行される iptables (NAT)、Linux ip forwarding
4. テナント単位で仮想サーバとネットワークを分離	Network Namespace, VLAN, GRE, VXLAN
• その他 (ネットワーク接続)	Open vSwitch, veth pair, tap, Internal Port

■ 登場人物

- Linux Bridge
- Open vSwitch (OVS)
 - › ソフトウェアスイッチ
- Network Namespace
 - › 仮想ネットワーク, 仮想ルータ、マルチテナントネットワーク環境を作る
- veth pair
 - › 仮想NICのペア = 仮想LANケーブル
- Internal Port
 - › Junoで新しく採用された低負荷なveth pair
- TAP device
 - › 仮想サーバーが利用する仮想NIC

Neutronの内部構成



■ Neutronの動作

- 特定の場面について，具体的な動作，通信の流れを説明します。
 - インスタンス（仮想サーバ）へ内部IPを割り当てる
 - インスタンスから外部ネットワークへの通信
 - 外部ネットワークからインスタンスへの通信
 - テナント単位でネットワークを分離

■ 仮想サーバへ内部IPアドレスを割り当てる

neutron-dhcp-agent
が、namespaceを
作成し、dnsmasq
を起動

neutron-dhcp-agent

dnsmasqが内部
IPアドレスを返す

dnsmasq

Namespace
“DHCP”

10.0.0.2

br-int

インスタンス

10.0.0.3

インスタンス起動、
DHCP問い合わせ

Open vSwitch

Network
Namespace

Linux Bridge

veth pair

Internal port

TAP device

Tenant

仮想サーバから外部ネットワークへの通信

外部ネットワーク

neutron-l3-agentが
Namespace内で
iptables, ip forwardingを
設定

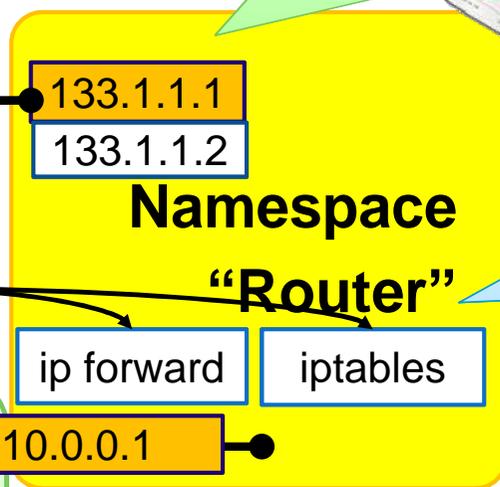
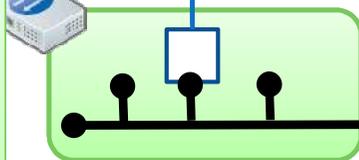
インスタンスに紐付いた
NAT用IPが生成される
(Floating IP)

Open vSwitch

Network
Namespace

Linux Bridge

Internal port



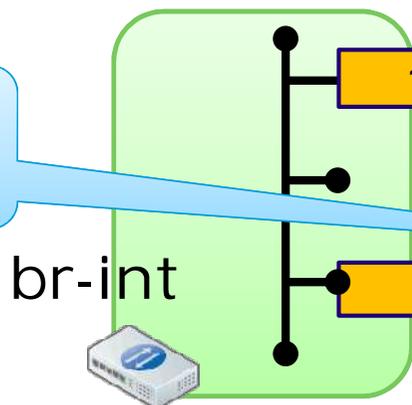
neutron-l3-agent

src:133.1.1.2とな
るようNATされる

インスタンスが外
部向けに通信開始

TAP device

Tenant



10.0.0.1

インスタンス

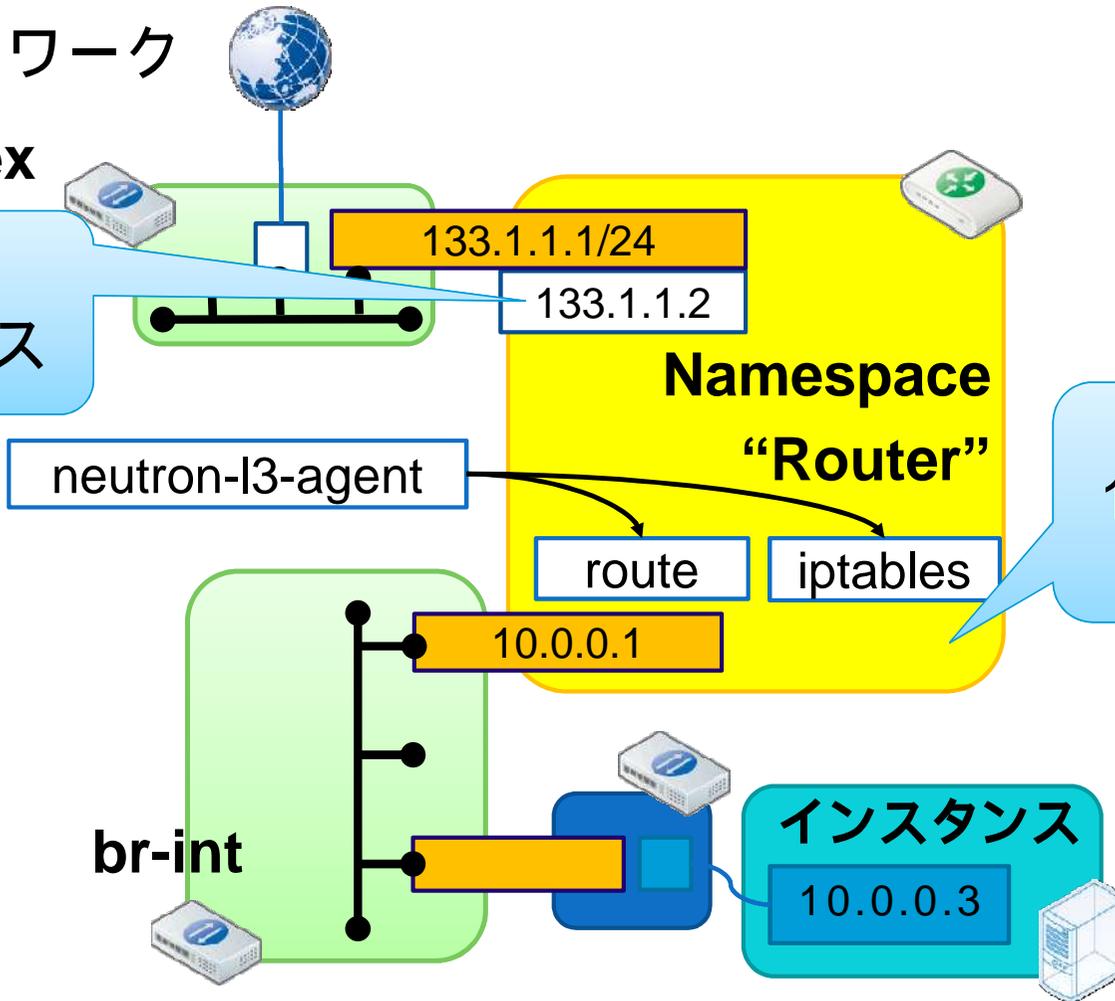
10.0.0.3

外部ネットワークから仮想サーバへの通信

外部ネットワーク

br-ex

外部からは
133.1.1.2にアクセス



宛先アドレス
10.0.0.3でNATされ
パケット転送

Open vSwitch

Network Namespace

Linux Bridge

Internal port

TAP device

Tenant

テナント単位でネットワークを分離

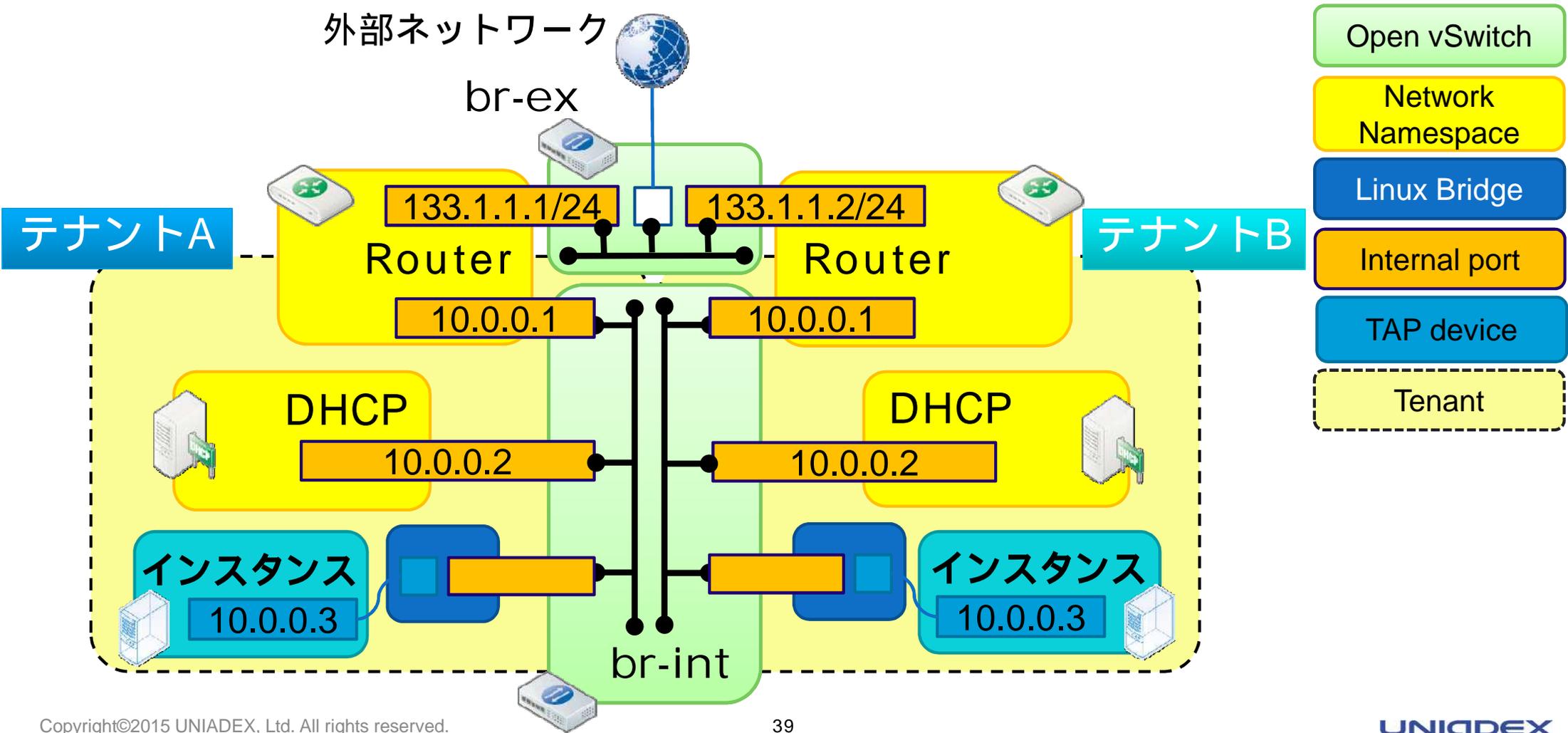


Photo by Tim Dorr <https://www.flickr.com/photos/timdorr/20017127/>

OpenStackの実環境適用と SDN製品連携の必要性



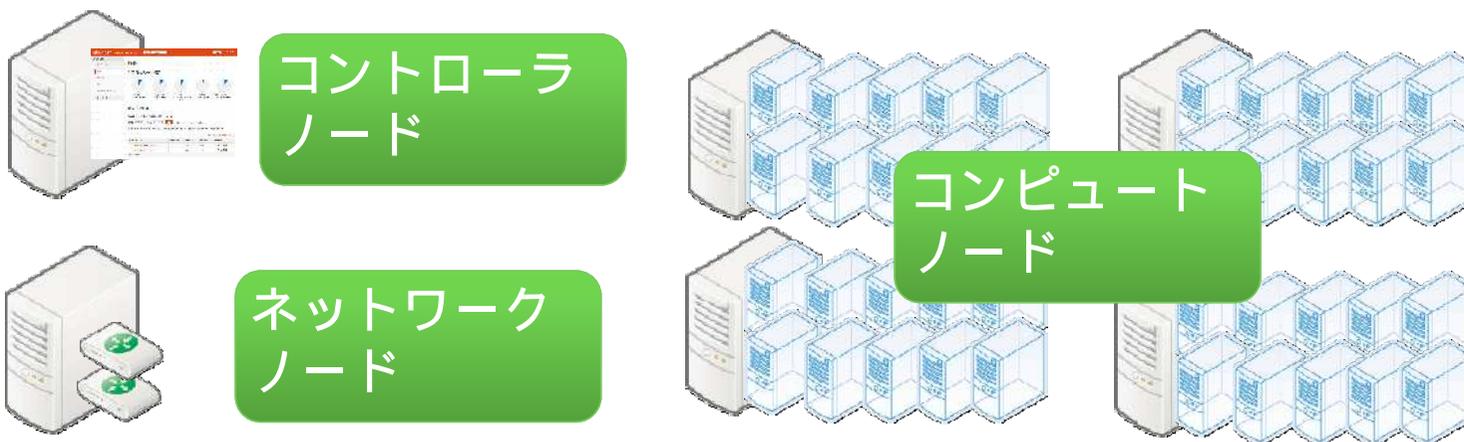
■ OpenStackの実環境適用

■ 我々が最初に通る道

- ▶ オールインワン（シングルノード）構成のOpenStack

■ 実環境

- ▶ マルチノード構成のOpenStack
- ▶ 重要なのはノード間を繋ぐ“ネットワーク”
- ▶ 例えば、スケーラビリティ、構成の柔軟性と管理、品質の維持 / 管理



■ OpenStack実環境における**ネットワークの課題**

■ スケーラビリティ

- ＞物理サーバ追加時にネットワークを追加できるか？
- ＞複数データセンタ間の接続と管理
- ＞4k VLAN問題

■ 構成の柔軟性と管理

- ＞冗長設計がネットワーク設計を硬直化
- ＞商用ファイアウォールやロードバランサなどの導入

■ 品質の維持 / 管理

- ＞仮想マシン集約による物理ネットワークトラフィックの増大に耐えうるか？
- ＞ヒューマンエラーを防止するには？

■ OpenStack実環境におけるSDNの効果

■ スケーラビリティ

- ▶ OpenStack ノード / スイッチ追加のゼロタッチコンフィグを実現
- ▶ 複数データセンタ間のネットワークを一元管理
- ▶ VLAN数制限制限なし

■ 構成の柔軟性と管理

- ▶ 冗長設計は考慮不要（自動的に冗長）
- ▶ 商用ファイアウォール / ロードバランサ製品との連携

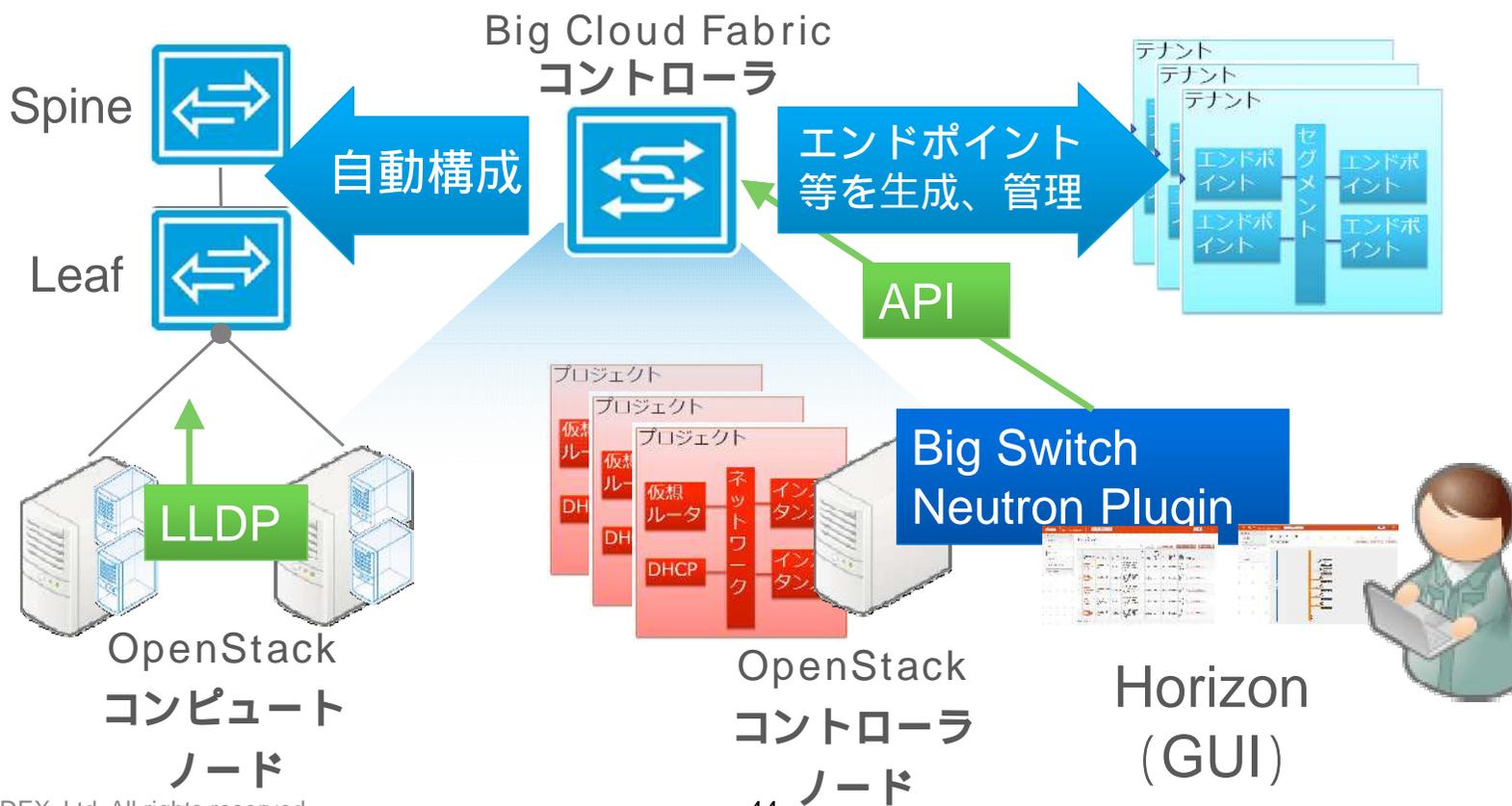
■ 品質の維持 / 管理

- ▶ 物理ネットワークと仮想ネットワークを紐付けて監視
- ▶ 設定の大半をソフトウェアが実施（SDN）

SDN製品によるNeutron実装 連携パターン

BigSwitch Networks

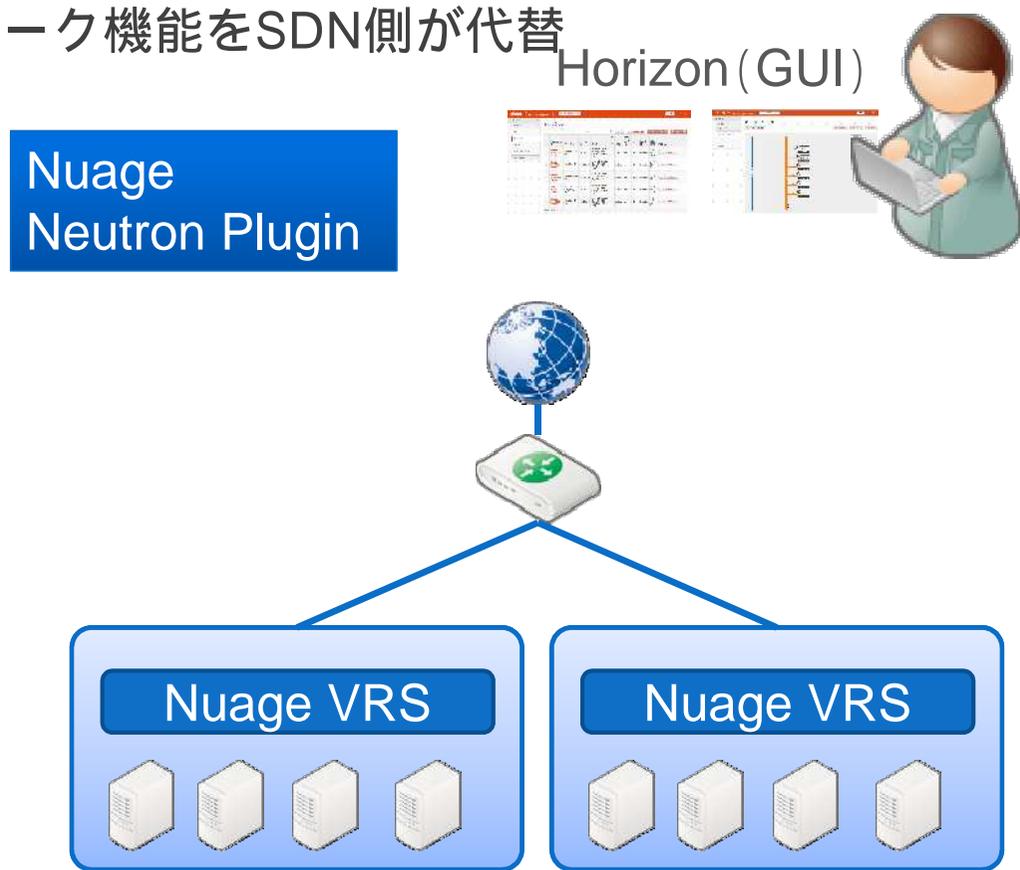
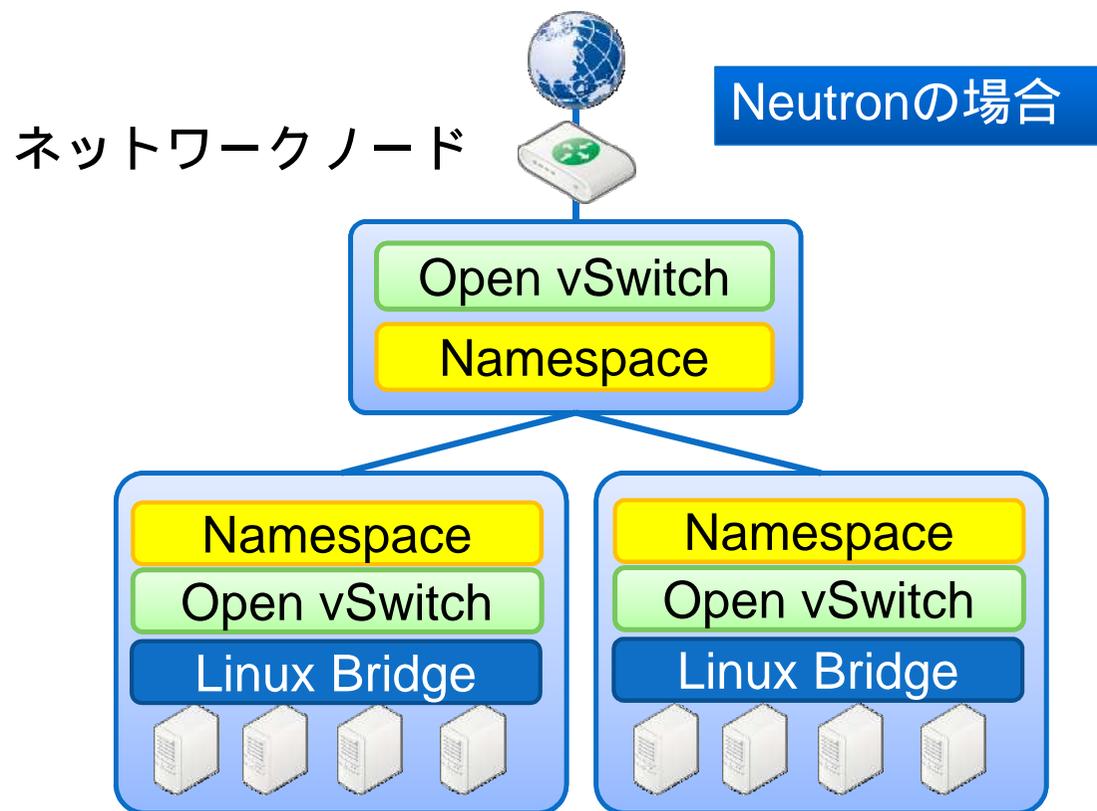
› Neutron Pluginの情報とLLDPを使ってNeutronに必要なネットワークを自動構成



SDN製品によるNeutron実装 代替パターン

Nuage Networks

Neutron Plugin経由でほぼ全てのネットワーク機能をSDN側が代替



おわりに

■ OpenStack Neutronについて更に知りたい方へ

<http://www.atmarkit.co.jp/ait/articles/1412/08/news009.html>

@IT > Server & Storage > いま覚えておくべきOpenStack Neutronの基本 (1) : OpenStac...

» 2014年12月08日 18時36分 更新

いま覚えておくべきOpenStack Neutronの基本 (1) :

OpenStack Neutronとは何か？ (1/3)

オープンなIaaSプラットフォーム構築の本命といわれるOpenStack。そのネットワーク部分の管理を担うコンポーネントであるNeutronはどのようなものでしょうか。基本的な構成や内部の動作、実践的なネットワークの構成方法を解説します。

[SDNエバンジェリスト吉本昌平, ユニアドックス株式会社]

印刷/PDF ツイート 16 いいね! 46 BI 8 g+1 3 Pocket 74 メールで送信
類似記事の掲載をメールで通知 連載「いま覚えておくべきNeutronの基本」の新着をメールで通知

PR 攻撃者の視点で明かす、ソーシャルエンジニアリングの心理学

ユニアドックスでSDNエバンジェリストを担当している吉本です。今回から本連載を担当いたします。よろしくお願いいたします。

openstack neutron

ウェブ 動画 画像 ニュース ショッピング もっと見る 検索ツール

日本語のページを検索 期間指定なし すべての結果 リセット

OpenStack Neutronとは何か？ (1/3) - IT

www.atmarkit.co.jp > Server & Storage

2014/12/08 - オープンなIaaSプラットフォーム構築の本命といわれるOpenStack。そのネットワーク部分の管理を担うコンポーネントであるNeutronはどのようなものでしょうか。基本的な構成や内部の動作、実践的なネットワークの構成方法を解説します。

OpenStackとネットワーク仮想化(SDN) - IT

www.atmarkit.co.jp > Server & Storage

2014/05/26 - 現在稼働しているOpenStack環境ではOpen vSwitch Pluginが使われていますが、Modular Layer 2(ML2) PluginがNeutronのリファレンス実装になり、Open vSwitch PluginおよびLinux Bridge Pluginを削除する方向にあります。

Neutronになって理解するOpenStack Network - Slideshare

www.slideshare.net/VirtualITech-JP/20140929-rev-r

2014/10/06 - 講師:ユニアドックス 吉本 日時:2014/10/08 タイトル:「Neutronになって理解するOpenStack Network」～Neutron/Open vSwitchなどNeutronと周辺技術の解説～ 概要: -はじめに - Nova-Networkではなく、Neutronを選択する - Neutro...

■ ユニアデックスとOpenStack



■ パブリッククラウドU-Cloudのご紹介

U-Cloud[®] ユークラウド

U-Cloud[®] IaaS【2008/10～】

企業様向け
高いサービス品質

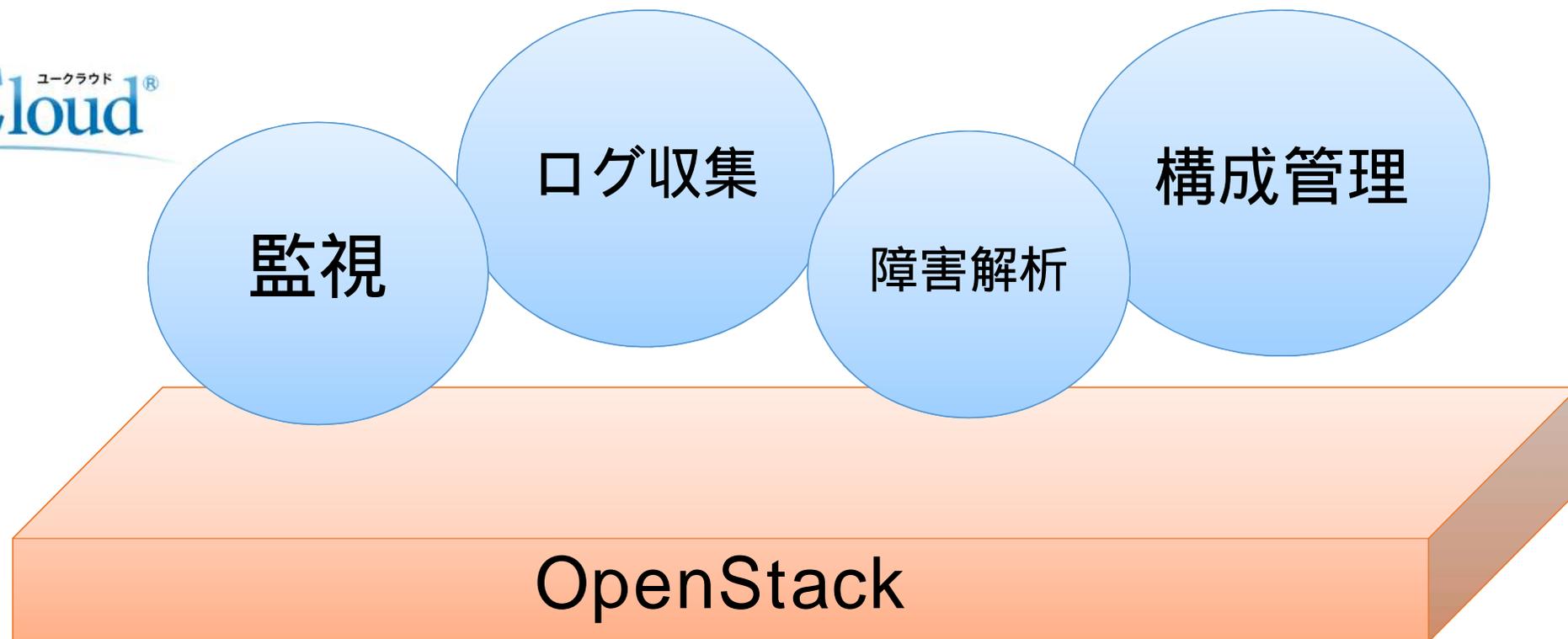
安全・安心な
クラウドサービス

24時間365日
万全な監視体制

お客様のご要望に合わせる
マネージドクラウド

■ U-CloudとOpenStack

U-Cloud[®]
ユークラウド



クラウド事業者として**長年培ったノウハウ・設備・システム**と
OpenStackを組み合わせたIaaSサービスを検討中



U-Cloud サポートポータル

メールアドレス

パスワード

ログイン

[パスワードを忘れた方はこちら](#)

UNISYS
個人情報保護について [情報セキュリティ基本方針](#)

Powered By **UNIADEX** **U-Cloud**
日本ユニシスグループ ユー・クラウド

ICTサポートポータルはU-Cloudサポートポータルに名称を変更致しました。
U-Cloudは日本ユニシスグループが日本国内で提供するサービスです。
Copyright © Nihon Unisys Group All Rights Reserved.

U-Cloudサポートポータル x

← → ↻ <https://www2.u-cloud.jp/support/self/FwPolicySettingEditList.form> ☆ ☰

U-Cloud U-Cloud サポートポータル

ログインユーザ: 青沼 崇生 さん
 前回ログイン日時: 2015/01/16 18:45:35

パスワード変更 ログアウト ヘルプ

TOP > プロビテスト >

メニュー

CN0533-R13
プロビテスト

サーバ管理

- ・サーバ(起動・停止・リセット)
- ・監視設定変更

ネットワーク管理

- ・ファイアウォール設定変更
- ・ロードバランサー設定変更

ユーザ管理

- ・お客様窓口情報の変更

サービス要求一覧

サーバリソース利用状況のお知らせ

電力使用量・CO2排出量報告書

問合せ受付窓口

作業依頼

ファイアウォールポリシー編集

送信元 共用インターネット

編集内容をファイアウォールへ反映する場合は、一覧下にある[確認]ボタンをクリックしてください。
 編集内容を破棄する場合は[キャンセル]ボタンをクリックしてください。

追加

送信元セグメント: 共用インターネット

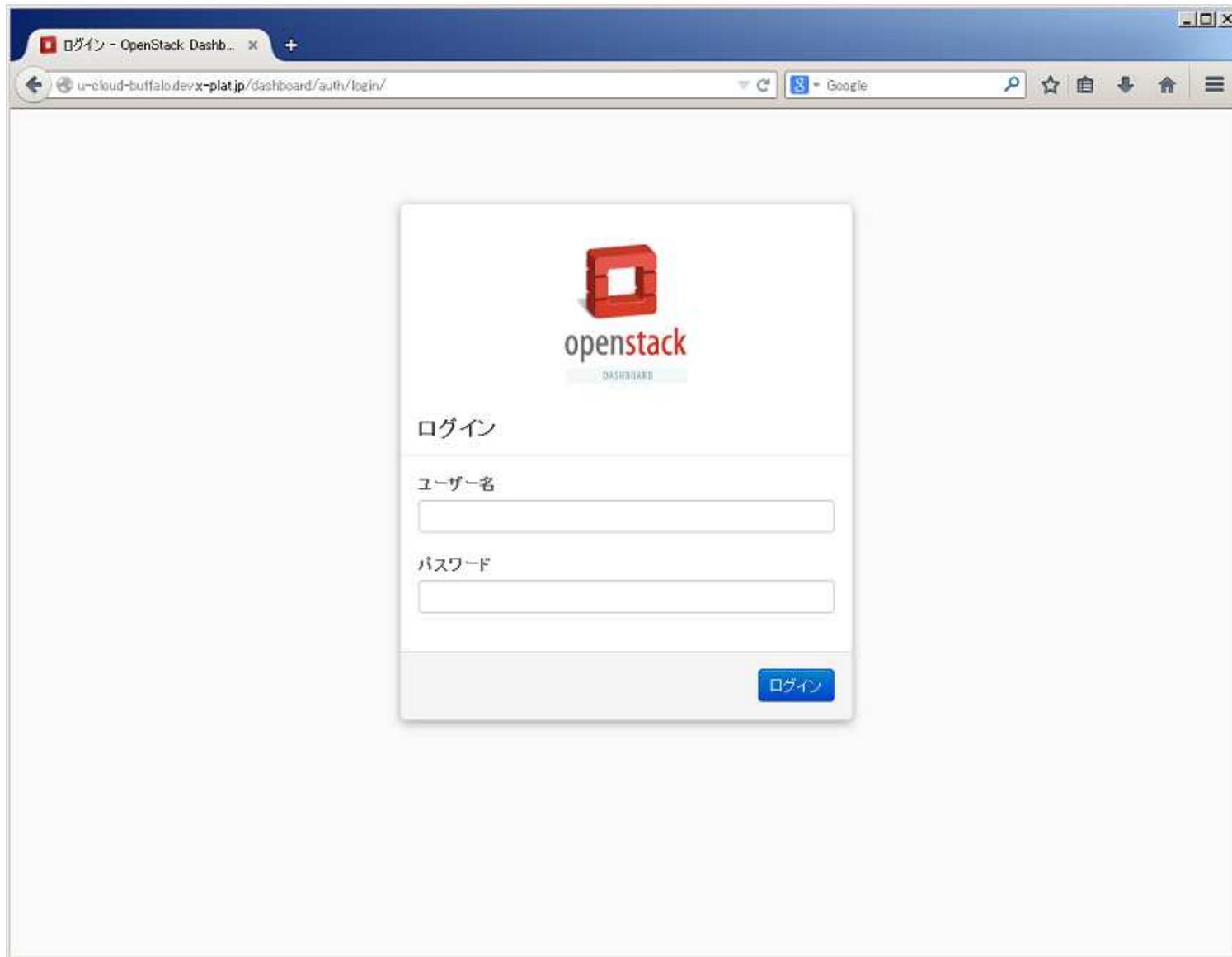
No	送信元	送信先		サービス プロトコル port	アクセス 制御	操作
	ホスト名/ ネットワークアドレス	ホスト名/ ネットワークアドレス				
1	any	()		tcp 80	許可	
2	any	()		tcp 443	許可	
	any	any		ip	拒否	

キャンセル
確認

個人情報保護について | 情報セキュリティ基本方針 | マイクロソフトライセンス条項
U-Cloud IaaS 利用規約

Powered By

ICTサポートポータルは U-Cloudサポートポータル に名称を変更致しました
 U-Cloudは日本ユニシスグループが日本国内で提供するサービスです
 Copyright © Nihon Unisys Group All Rights Reserved.







まとめ

1. OpenStackをキチンと動かすにはノウハウが必要です
2. 構築・設計の勘所さえ分かれば意外と動きます
3. OpenStack環境構築はユニアデックスにご相談ください



OpenStackへ関わる全ての皆様へ感謝します