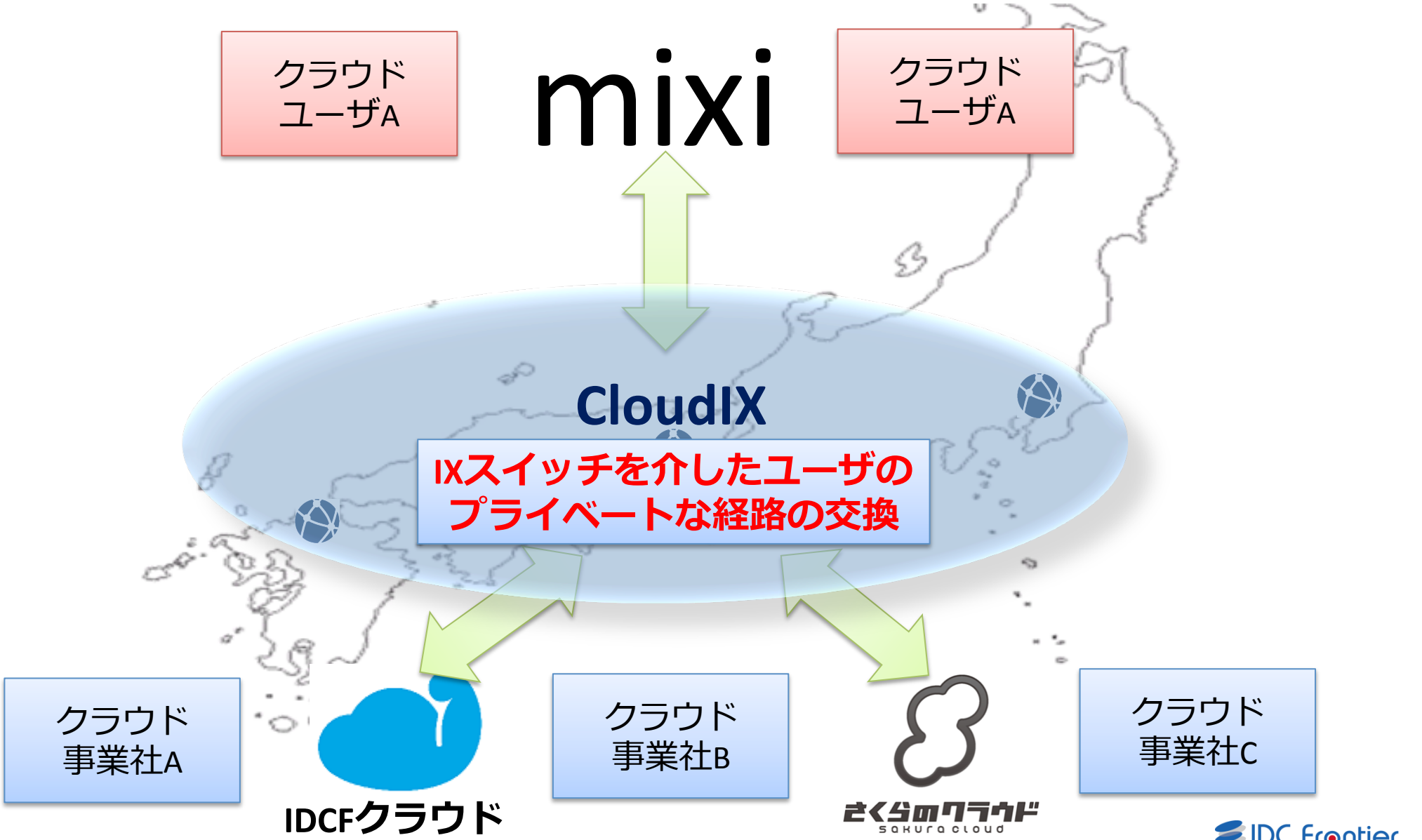
IDC Frontier
未来をささえる、Your Innovative Partner

クラウドインターコネクト

株式会社IDCフロンティア
技術開発本部R&D室
井上 一清
2015年4月17日

今回のクラウドインターコネクトの定義



検証の背景

時代は閉域（プライベートネットワーク）
閉域網ニーズは今後一層高まる

インターネットは人間向け
プライベートネットワークはMachine向け

IoTなどのM2M通信もプライベートの方が適しているものもあるのでは？？

クラウド間での柔軟な閉域接続が必要

ハイブリッド接続方法

オンプレ環境とクラウドの接続方法

	インターネットVPN	専用線	クラウド インターコネクト
コスト	○	×	△
スループット	×	◎	○
技術	面倒	楽	やや難しい
納期	早い	遅い	早い
例	Vyatta,VyOS	○△専用線	複数事業者間接続
メリット	回線費用がほぼかからない	安定 帯域専有	既存回線を活かせる場合がある IXスイッチに接続すれば1:nで接続できる
デメリット	相互接続性の問題 NW技術者がいる 冗長設計難しい	費用高い 納期かかる 都度回線敷設	高い技術が必要 事例が少ない

前からやってたこと。手段が増えただけ

クラウドインターコネクトの接続方法比較

	VxLAN	Option A (BGP per VRF)	Option B (MP-BGP)
Layer	L2	L3	L3/L2
冗長設計	難	普通	良
敷居	普通	少し高い	やや高い
自動化	難	やや難	比較的容易
インオペ	×	○	○
拡張性	×	△	○

MP-BGPが双方で使える場合には、Option Bが一番良いかと思う。
MP-BGPが使えない環境では、Option Aが良いかと思う。

Option A,B,Cの参考　https://tools.ietf.org/html/rfc4364

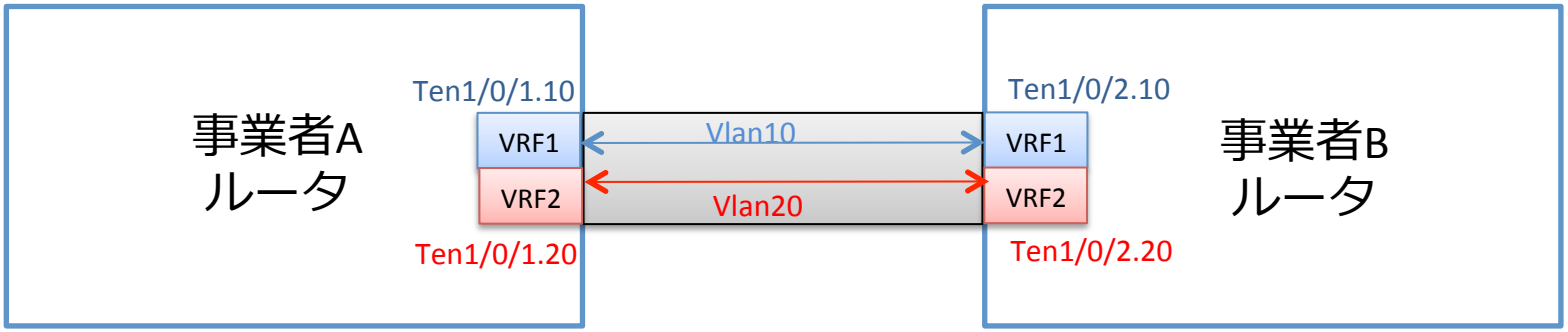
技術方式の検討（VxLAN v.s. MP-BGP）

- VxLAN
  - L2接続のみ
  - 冗長困難
  - インオペ難しい
  - スケール難しい（unicastだとメッシュでパス張って都度staticに設定が必要）
  - 導入自体は難しくはない

- MP-BGP
  - L3接続(MPLS)に加えてL2接続も(VPLS)可能
  - 冗長容易
  - インオペ比較的容易
  - スケールし易い
  - 技術的な敷居がやや高い

Option A BGP per VRF

- VRF to VRF
  - ルータ間はMPLSをしゃべる必要がない。
    VRF識別子(⇒Vlan Tag)があれば良い
  - テナント毎にVlanをフルメッシュで張る必要が出てくる
  - その代わり論理IF単位でトラフィック流量等の情報取得が可能



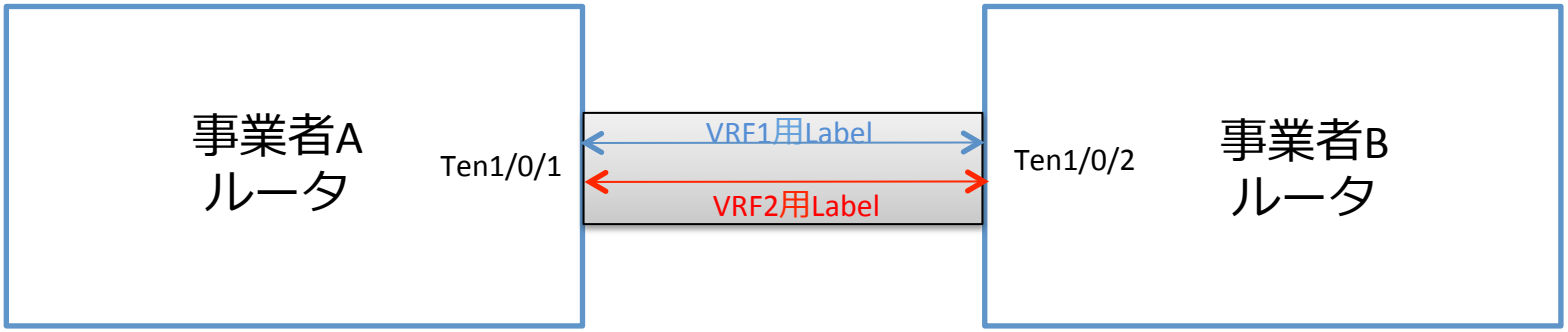
Option B MP-BGP

- ASBR to ASBR
  - ルータ間はMP-BGPをしゃべりLabel転送が必要

    ※ただしVPN Labelのみで可。転送Labelは不要！

    ⇒ルータ間のLDPは不要
  - ASBRでのflow取得が難しい

    Label見れるflow export/collectorが必要



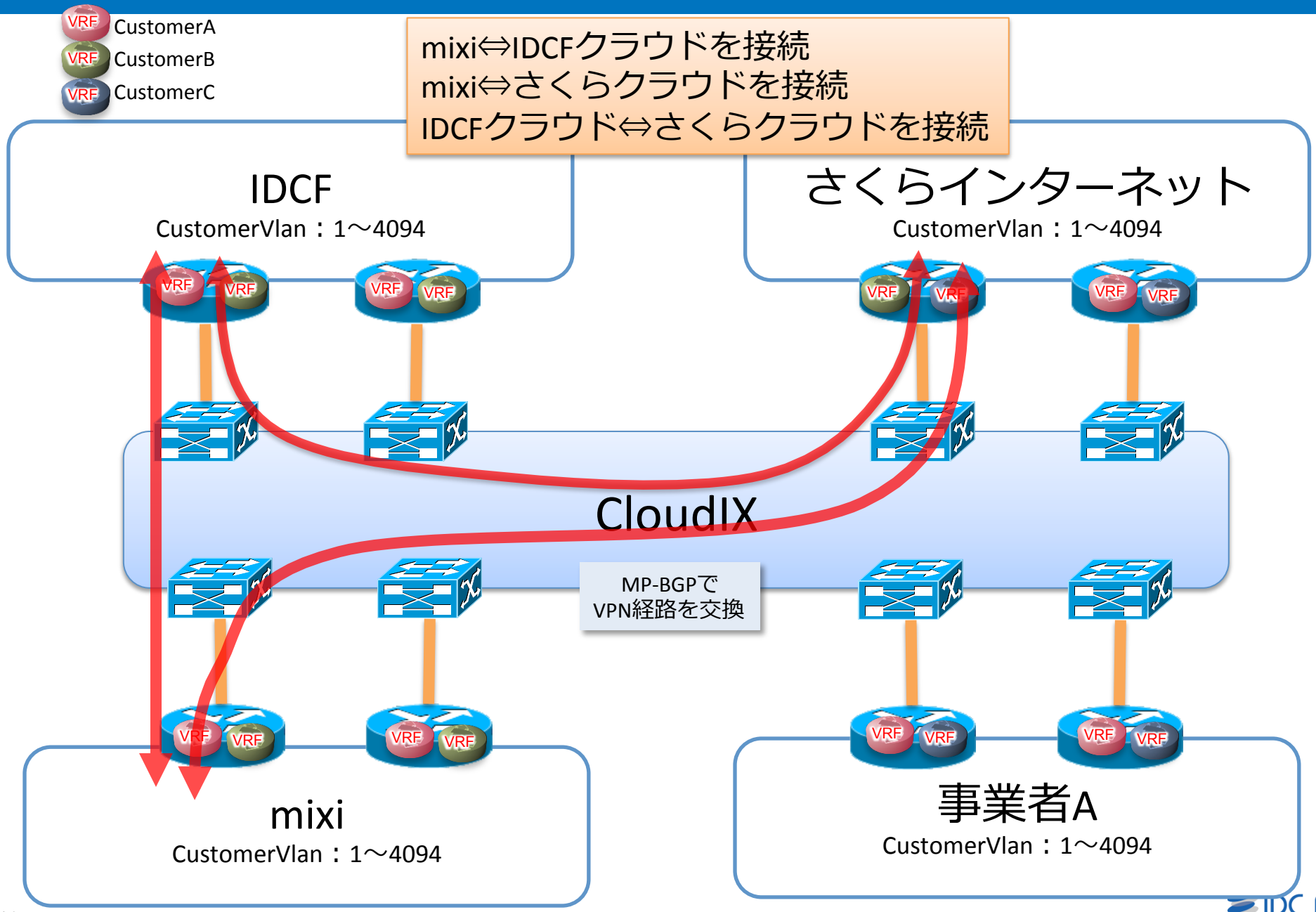
クラウドインターコネクトの接続方法比較（再掲）

	VxLAN	BGP Option A	MP-BGP Option B
Layer	L2	L3	L3/L2
冗長設計	難	普通	良
敷居	普通	少し高い	やや高い
自動化	難	やや難	比較的容易
インオペ	×	○	○
拡張性	▲	△	○

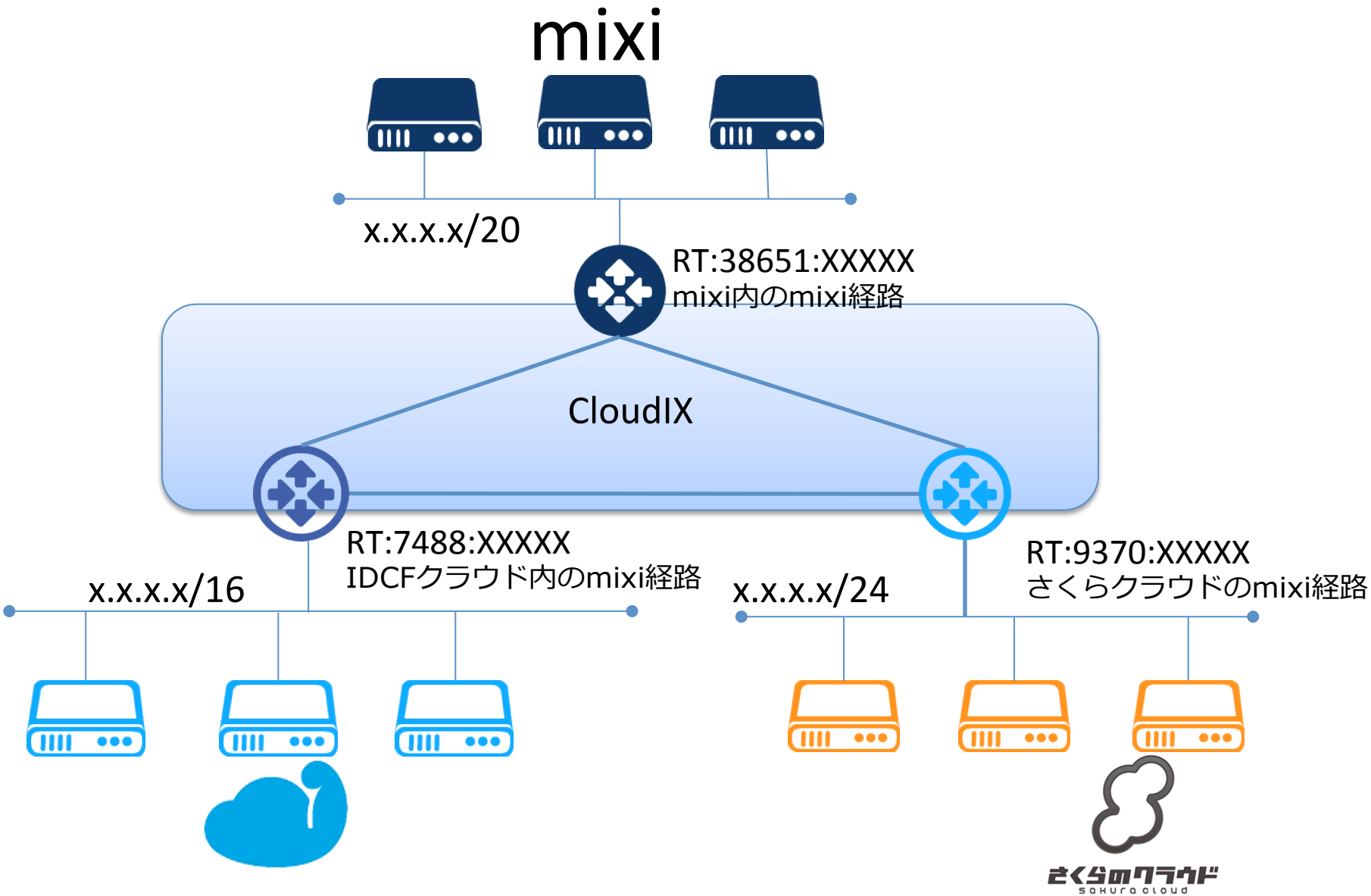
MP-BGPが双方で使える場合には、Option Bが一番良いかと思う。
MP-BGPが使えない環境では、Option Aが良いかと思う。

Option A,B,Cの参考　https://tools.ietf.org/html/rfc4364

検証構成イメージ（物理）



検証構成イメージ（論理）



ハマったこと①

既存BGPセッションの全down/up

・事象

MP-eBGPの設定をしたタイミングで、既存のMP-iBGPセッションが全てFlap(down/up)した。

Jan 20 19:05:03 <host-name> rpd[1309]: bgp_adv_main_update:7975: NOTIFICATION sent to x.x.x.x (Internal AS xxxx): code 6 (Cease) subcode 6 (Other Configuration Change), Reason: Configuration change - VPN table advertise

・原因

inet-vpnの場合でMP-eBGPやRRが一つもない状態だと、MP-iBGPセッションはinet.0のrouting-tableを使用する。
MP-eBGP,RRが一つもない状態からMP-eBGPを設定すると、bgp.l3vpn.0のtableに経路情報をinet.0からコピーする動作を行う。
このため、既存のiBGPセッションはリセットされる。
というJuniperの仕様。。

参考資料

Preventing BGP Session Resets

ハマったこと②

想定外の経路広報

・事象

bgp exportのフィルタが効かず想定外のVPN経路が広報された

・原因

最近のJuniper機器のdefaultではbgp export policyはbgp.l3vpn.0テーブルの経路にしか効かず、VRFで学習した経路（vrfxx.inet.0の経路）には効かず、全vrfxx.inet.0の経路を出してしまう。
VRFで学習した経路についてもbgp export policyが効くようにするには下記の設定が必要

set protocols bgp group <グループ名> vpn-apply-export

参考資料

Applying Both the VRF Export and the BGP Export Policies

ハマったこと③

communityのない経路が見えない

・事象

設定ミス等でcommunityがついていない経路を広報すると、広報側ルータでのshow route adv-proto bgpでは経路が見えていたが、受信側ルータのshow route received-protocol bgp では経路がhiddenでも見えなかった。

・原因

広報側ルータでcommunityが付いていなかったため、受信側ルータではinvalidな経路と判定され、hiddenでも表示されなかった。

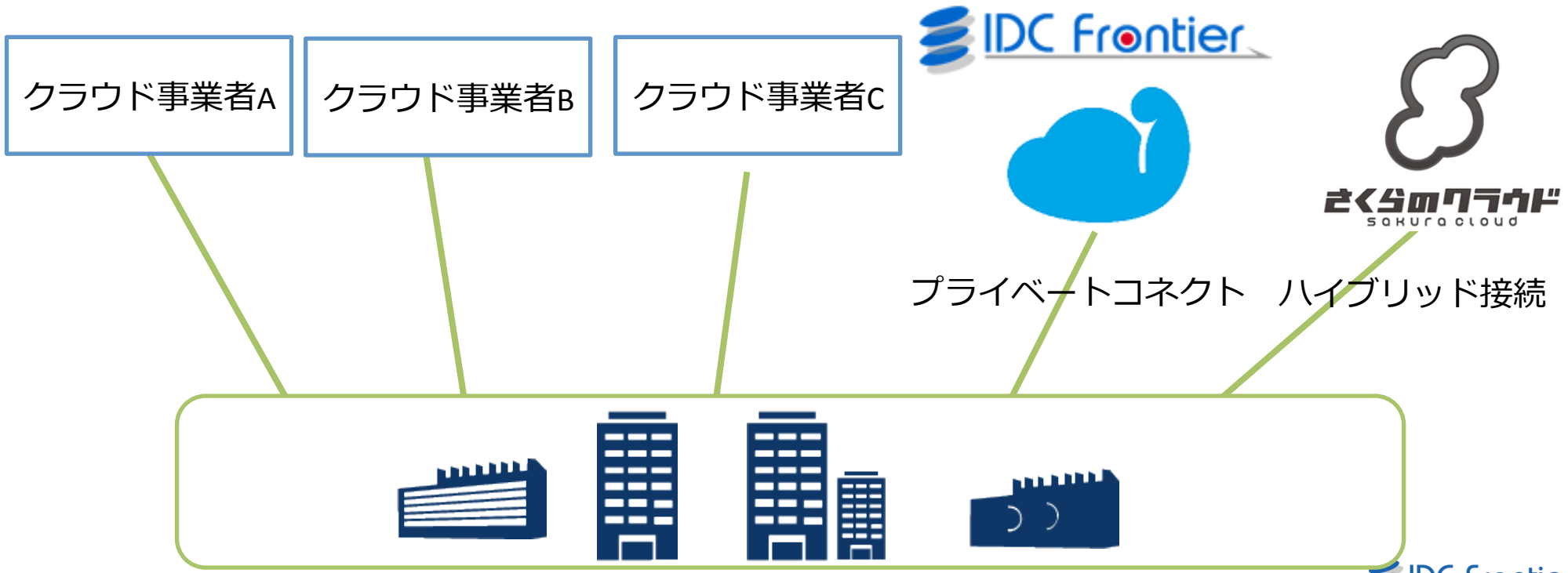
・参考

以下のように、vrf-targetとvrf-export両方設定している場合、 vrf-exportが勝ってvrf-targetのtarget communityが付与されないので、 vrf-exportのpolicy中でtarget communityを付与する必要がある。（vrf-importの場合も同様）

```
routing-instances {
   vrf1 {
      vrf-target target:1:1
      vrf-export export-vrf1;
```

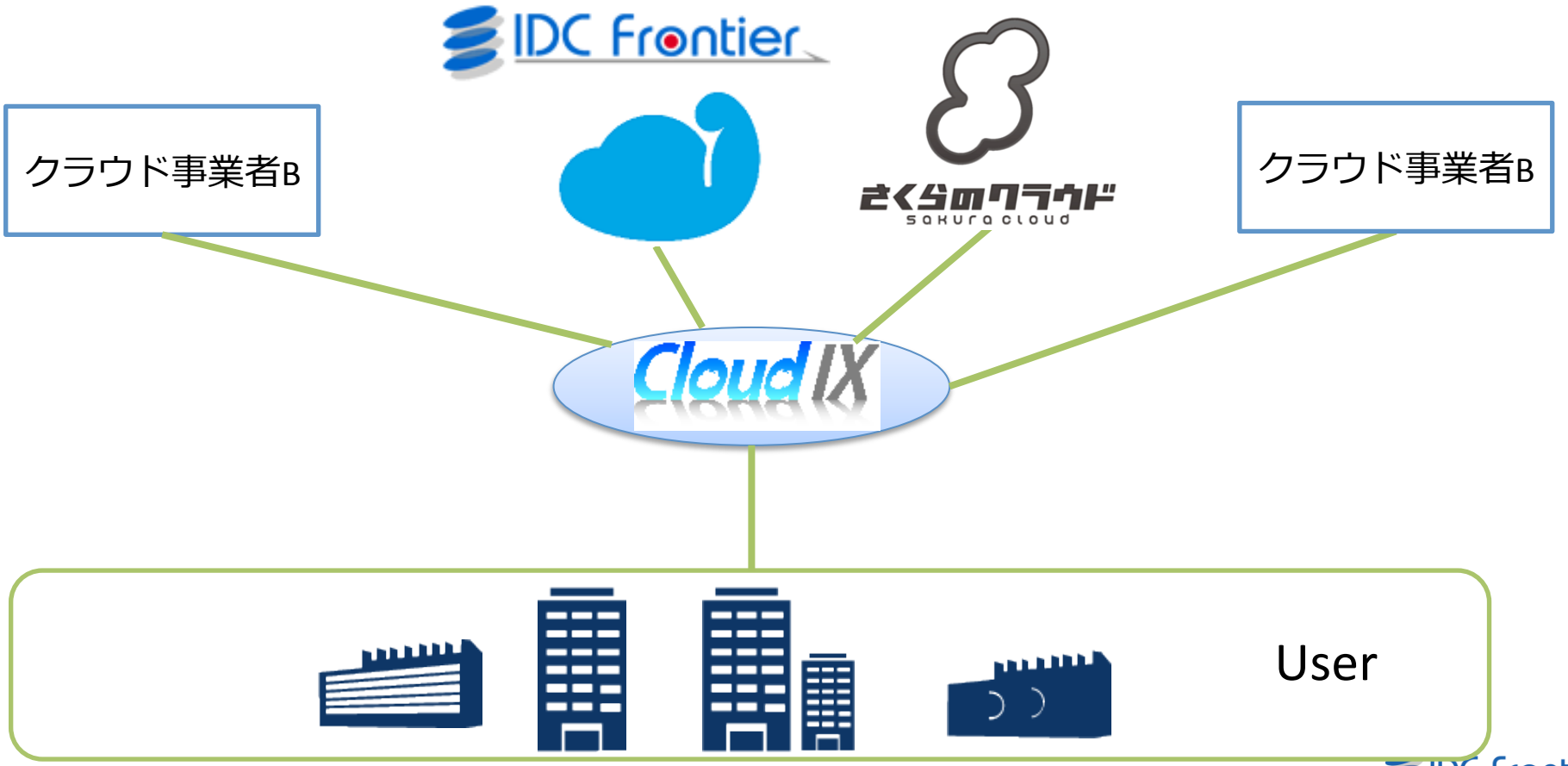
2015年クラウド事業者

各IaaS事業者の特色が出てくる
クラウドダイバーシティ（1:n, n:n）
事業者間の接続が必要になってくる。



今後の展開（勝手なイメージ）

こんな感じになっていったら面白い？？
参加されたい方是非ご連絡下さい。



未来をささえる、Your Innovative Partner