

# RouterOS 設定例

as of 2015/09/27

# 目次

- **設定例**

- Site-to-Site VPN (IPsec)
- eBGP
- iBGP RouteReflection

- **総括**

- 技術的なコメント
- 全体的なコメント
- ユーザ会への要望

# Site-to-Site VPN (IPsec)

RouterOS と Cisco ASA 間で Site-to-Site な IPsec を設定する

# 構成



IKE Shase 1 パラメータ	値
モード	メインモード
暗号化アルゴリズム	AES
ハッシュアルゴリズム	SHA1
ライフタイム	1 日(86,400 秒)
認証方式	事前共有鍵
DH グループ	グループ 2(1,024 bit)

IKE Shase 2 パラメータ	値
セキュリティprotocol	ESP
暗号化アルゴリズム	AES
認証アルゴリズム	HMAC-SHA1
ライフタイム	1 日(86,400 秒)
カプセル化モード	トンネルモード
DH グループ	グループ 2(1,024 bit)

# MikroTik の設定

```
Algorithm/ip ipsec proposal
add auth-algorithms=sha1 enc-algorithms=aes-256-cbc lifetime=1d pfs-group=modp1024 name=ESP-AES256-SHA

/ip address
add address=172.16.1.1/24 interface=ether3 network=172.16.1.0
add address=192.168.1.1/24 interface=ether2 network=192.168.1.0

/ip firewall nat
add chain=srcnat dst-address=172.16.2.0/24 src-address=172.16.1.0/24
add action=masquerade chain=srcnat out-interface=ether2 src-address=172.16.1.0/24

/ip ipsec peer
add address=192.168.2.1/32 dpd-interval=disable-dpd dpd-maximum-failures=1 enc-algorithm=aes-256 hash-algorithm=sha1 lifetime=1d nat-traversal=no secret=PSK

/ip ipsec policy
add dst-address=172.16.2.0/24 proposal=ESP-AES256-SHA sa-dst-address=192.168.2.1 sa-src-address=192.168.1.1 src-address=172.16.1.0/24 tunnel=yes

/ip route
add distance=1 gateway=192.168.1.254

/system identity
set name=RoS-2
```

# Cisco ASAv の設定

```
hostname ASAv-4
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 192.168.2.1 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.2.1 255.255.255.0
 no shutdown
!
object network LOCAL-172.16.2.0
 subnet 172.16.2.0 255.255.255.0
!
object network REMOTE-172.16.1.0
 subnet 172.16.1.0 255.255.255.0
!
object network ANY-0.0.0.0
 subnet 0.0.0.0 0.0.0.0
!
access-list ACL-PERMIT-VPN extended permit ip 172.16.2.0 255.255.255.0 172.16.1.0 255.255.255.0
!
no pager
!
nat (inside,outside) source static LOCAL-172.16.2.0 LOCAL-172.16.2.0 destination static REMOTE-
172.16.1.0 REMOTE-172.16.1.0
```

```
object network ANY-0.0.0.0
 nat (inside,outside) dynamic interface
!
route outside 0.0.0.0 0.0.0.0 192.168.2.254 1
!
crypto ipsec ikev1 transform-set ESP-AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map CRYPTO-MAP 1 match address ACL-PERMIT-VPN
crypto map CRYPTO-MAP 1 set peer 192.168.1.1
crypto map CRYPTO-MAP 1 set ikev1 transform-set ESP-AES256-SHA
crypto map CRYPTO-MAP interface outside
crypto ikev1 enable outside
!
crypto ikev1 policy 65535
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
!
tunnel-group 192.168.1.1 type ipsec-l2l
tunnel-group 192.168.1.1 ipsec-attributes
 ikev1 pre-shared-key PSK
!
policy-map global_policy
 class inspection_default
 inspect icmp
!
end
```

# 設定量の比較

```
/ip ipsec proposal
add auth-algorithms=sha1 enc-algorithms=aes-256-cbc lifetime=1d pfs-group=modp1024 name=ESP-AES256-SHA

/ip address
add address=172.16.1.1/24 interface=ether3 network=172.16.1.0
add address=192.168.1.1/24 interface=ether2 network=192.168.1.0

/ip firewall nat
add chain=srcnat dst-address=172.16.2.0/24 src-address=172.16.1.0/24
add action=masquerade chain=srcnat out-interface=ether2 src-address=172.16.1.0/24

/ip ipsec peer
add address=192.168.2.1/32 dpd-interval=disable-dpd dpd-maximum-failures=1 enc-algorithm=aes-256 hash-algorithm=sha1
lifetime=1d nat-traversal=no secret=PSK

/ip ipsec policy
add dst-address=172.16.2.0/24 proposal=ESP-AES256-SHA sa-dst-address=192.168.2.1 sa-src-address=192.168.1.1 src-
address=172.16.1.0/24 tunnel=yes

/ip route
add distance=1 gateway=192.168.1.254

/system identity
set name=RoS-2
```

RouterOS

```
hostname ASA-4
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 192.168.2.1 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.2.1 255.255.255.0
 no shutdown
!
object network LOCAL-172.16.2.0
 subnet 172.16.2.0 255.255.255.0
!
object network REMOTE-172.16.1.0
 subnet 172.16.1.0 255.255.255.0
!
object network ANY-0.0.0.0
 subnet 0.0.0.0 0.0.0.0
!
access-list ACL-PERMIT-VPN extended permit ip 172.16.2.0 255.255.255.0 172.16.1.0 255.255.255.0
!
no pager
!
nat (inside,outside) source static LOCAL-172.16.2.0 LOCAL-172.16.2.0 destination static REMOTE-172.16.1.0 REMOTE-172.16.1.0
!
object network ANY-0.0.0.0
 nat (inside,outside) dynamic interface
!
route outside 0.0.0.0 0.0.0.0 192.168.2.254 1
!
crypto ipsec ikev1 transform-set ESP-AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map CRYPTO-MAP 1 match address ACL-PERMIT-VPN
crypto map CRYPTO-MAP 1 set peer 192.168.1.1
crypto map CRYPTO-MAP 1 set ikev1 transform-set ESP-AES256-SHA
crypto map CRYPTO-MAP interface outside
crypto ikev1 enable outside
!
crypto ikev1 policy 65535
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
!
tunnel-group 192.168.1.1 type ipsec-l2l
tunnel-group 192.168.1.1 ipsec-attributes
 ikev1 pre-shared-key PSK
!
policy-map global_policy
 class inspection_default
 inspect icmp
!
en
```

Cisco ASA

# コメント

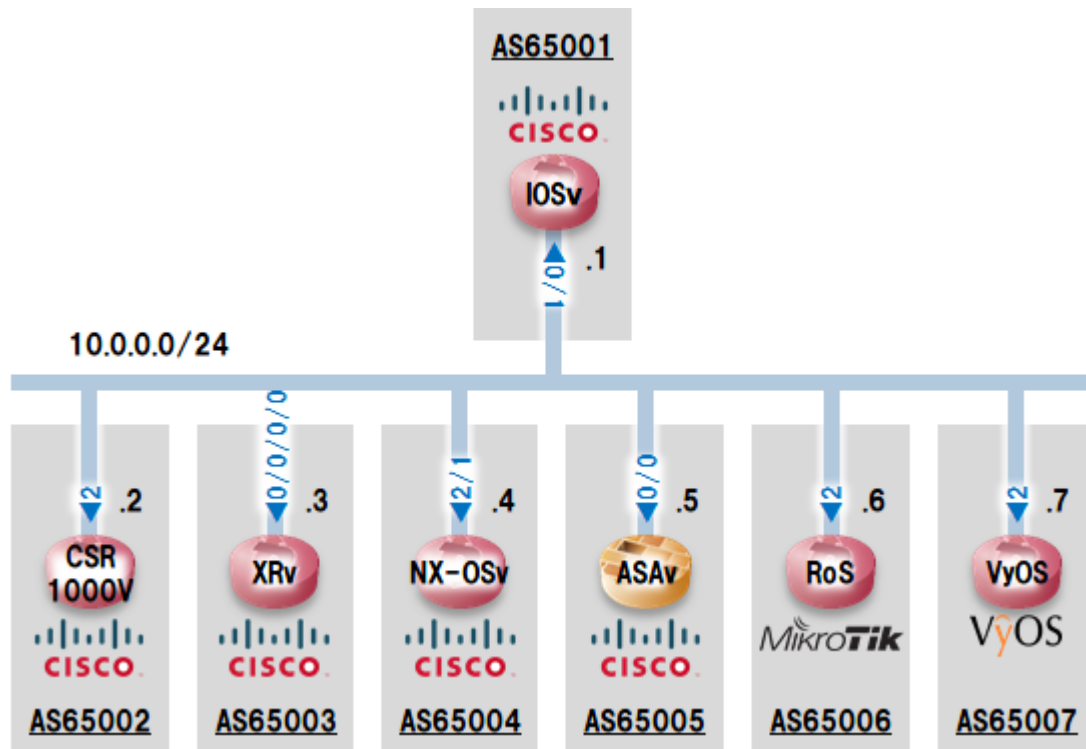
- MikroTik の方が設定がシンプル
  - MikroTik は複数パラメータをワンライナーで書ける
  - Cisco ASA は複数パラメータをワンライナーで書けない  
( 一行ずつ書く必要がある = 長くなる )
- 動作にも特に問題なし
  - ショートランテストでは問題なし
  - ロングランテストは未実施
  - 但し、RouterOS に限らず、IPsec には所謂「相性問題」がある為、長時間運用時の安定性には注意する必要がある



# eBGP

各ルータとの eBGP 設定比較

# 構成



Loopback	メーカー	OS	バージョン
10.0.0.1	Cisco	IOS	15.5 (2) T
10.0.0.2	Cisco	IOS-XEv	03.14.00.S
10.0.0.3	Cisco	IOS-XRv	5.3.0
10.0.0.4	Cisco	NX-OSv	7.2 (0) D1 (1)
10.0.0.5	Cisco	ASAv	9.3 (2) 200
10.0.0.6	MikroTik	RouterOS	6.30.2
10.0.0.7	VyOS	VyOS	1.1.5

# IOS の設定

```
hostname IOSv
!  
interface Loopback0  
 ip address 10.0.99.1 255.255.255.255  
!  
interface GigabitEthernet0/1  
 ip address 10.0.0.1 255.255.255.0  
 no shutdown  
!  
router bgp 65001  
 bgp router-id 10.0.99.1  
 neighbor 10.0.0.2 remote-as 65002  
 neighbor 10.0.0.3 remote-as 65003  
 neighbor 10.0.0.4 remote-as 65004  
 neighbor 10.0.0.5 remote-as 65005  
 neighbor 10.0.0.6 remote-as 65006  
 neighbor 10.0.0.7 remote-as 65007  
 network 10.0.99.1 mask 255.255.255.255  
!  
end
```

**業界スタンダード**

# IOS-XEv の設定

```
hostname XEv
!  
interface Loopback0  
 ip address 10.0.99.2 255.255.255.255  
!  
interface GigabitEthernet2  
 ip address 10.0.0.2 255.255.255.0  
 no shutdown  
!  
router bgp 65002  
 bgp router-id 10.0.99.2  
 network 10.0.99.2 mask 255.255.255.255  
 neighbor 10.0.0.1 remote-as 65001  
!  
end
```

ほぼ IOS の設定そのまま

# IOS-XRv の設定

```
hostname XRv
!
interface Loopback0
  ipv4 address 10.0.99.3 255.255.255.255
!
interface GigabitEthernet0/0/0/0
  ipv4 address 10.0.0.3 255.255.255.0
  no shutdown
!
route-policy PASS
  pass
end-policy
!
router bgp 65003
  bgp router-id 10.0.99.3
  address-family ipv4 unicast
    network 10.0.99.3/32
  !
  neighbor 10.0.0.1
    remote-as 65001
    address-family ipv4 unicast
      route-policy PASS in
      route-policy PASS out
  !
!
end
```

明示的に「pass」定義した route-policy が無いと  
経路を送信 / 受信しない

# NX-OSv の設定

```
license grace-period
!
hostname NX-OSv
!
feature bgp
!
interface Ethernet2/1
 no switchport
 ip address 10.0.0.4/24
 no shutdown
!
interface loopback0
 ip address 10.0.99.4/32
!
router bgp 65004
 router-id 10.0.99.4
 address-family ipv4 unicast
  network 10.0.99.4/32
 neighbor 10.0.0.1 remote-as 65001
  address-family ipv4 unicast
!
end
```

ライセンスを購入しておらず、評価利用するには  
「license grace-period」でライセンス猶予期間を  
開始する必要がある（120 日間有効）

利用したい機能を  
「feature」コマンドで指定し、有効化する

# ASAv の設定

```
hostname ASAv
!
interface GigabitEthernet0/0
 nameif OUTSIDE
 security-level 0
 ip address 10.0.0.5 255.255.255.0
 no shutdown
!
router bgp 65005
 bgp router-id 10.0.99.5
 address-family ipv4 unicast
  neighbor 10.0.0.1 remote-as 65001
  neighbor 10.0.0.1 activate
  network 10.0.99.5 mask 255.255.255.255
!
route Null0 10.0.99.5 255.255.255.255 254
!
end
```

ASA では Loopback を作成出来ない  
(※ 後述する RouterOS と同じ)

よって、BGP の Router-ID にするアドレスを  
null0 にヘルーティングさせつつ、  
eBGP で広報している

ASA では AD 値 255 はルーティングテーブルに  
インストールされない為、AD = 254 にしている

# RouterOS の設定

```
/system identity set name=RoS  
  
/interface bridge add name=loopback  
  
/ip address add address=10.0.99.6/32 interface=loopback  
/ip address add address=10.0.0.6/24 interface=ether2  
  
/routing bgp instance set default as=65006 router-id=10.0.99.6  
/routing bgp peer add remote-address=10.0.0.1 remote-as=65001  
/routing bgp network add network=10.0.99.6/32
```

(ASA 同様)RouterOS でも Loopback を作成できない

よって、物理インターフェースの所属しないブリッジを作成し、Loopback の代用とする

BGP の設定は非常にシンプル！



# VyOS の設定

```
set system host-name VyOS  
  
set interfaces loopback lo address 10.0.99.7/32  
set interfaces ethernet eth2 address 10.0.0.7/24  
  
set protocols bgp 65007 parameters router-id 10.0.99.7  
set protocols bgp 65007 neighbor 10.0.0.1 remote-as 65001  
set protocols bgp 65007 network 10.0.99.7/32
```

**構文は違うが、設定量/ニュアンスが  
RouterOS とほぼ同じ**

# 設定量の比較

```
hostname IOSv
!
interface Loopback0
ip address 10.0.99.1 255.255.255.255
!
interface GigabitEthernet0/1
ip address 10.0.0.1 255.255.255.0
no shutdown
!
router bgp 65001
bgp router-id 10.0.99.1
neighbor 10.0.0.2 remote-as 65002
neighbor 10.0.0.3 remote-as 65003
neighbor 10.0.0.4 remote-as 65004
neighbor 10.0.0.5 remote-as 65005
neighbor 10.0.0.6 remote-as 65006
neighbor 10.0.0.7 remote-as 65007
network 10.0.99.1 mask 255.255.255.255
!
end
```

**IOS**

```
hostname XEv
!
interface Loopback0
ip address 10.0.99.2 255.255.255.255
!
interface GigabitEthernet2
ip address 10.0.0.2 255.255.255.0
no shutdown
!
router bgp 65002
bgp router-id 10.0.99.2
network 10.0.99.2 mask 255.255.255.255
neighbor 10.0.0.1 remote-as 65001
!
end
```

**IOS-XEv**

```
hostname XRv
!
interface Loopback0
ipv4 address 10.0.99.3 255.255.255.255
!
interface GigabitEthernet0/0/0/0
ipv4 address 10.0.0.3 255.255.255.0
no shutdown
!
route-policy PASS
pass
end-policy
!
router bgp 65003
bgp router-id 10.0.99.3
address-family ipv4 unicast
network 10.0.99.3/32
!
neighbor 10.0.0.1
remote-as 65001
address-family ipv4 unicast
route-policy PASS in
route-policy PASS out
!
!
!
end
```

**IOS-XRv**

```
license grace-period
!
hostname NX-OSv
!
feature bgp
!
interface Ethernet2/1
no switchport
ip address 10.0.0.4/24
no shutdown
!
interface loopback0
ip address 10.0.99.4/32
!
router bgp 65004
router-id 10.0.99.4
address-family ipv4 unicast
network 10.0.99.4/32
neighbor 10.0.0.1 remote-as 65001
address-family ipv4 unicast
!
end
```

**NX-OSv**

```
hostname ASAv
!
interface GigabitEthernet0/0
nameif OUTSIDE
security-level 0
ip address 10.0.0.5 255.255.255.0
no shutdown
!
router bgp 65005
bgp router-id 10.0.99.5
address-family ipv4 unicast
neighbor 10.0.0.1 remote-as 65001
neighbor 10.0.0.1 activate
network 10.0.99.5 mask
255.255.255.255
!
route Null0 10.0.99.5 255.255.255.255
254
!
!
end
```

**ASAv**

```
/system identity set name=RoS
!
/interface bridge add name=loopback
!
/ip address add address=10.0.99.6/32
interface=loopback
/ip address add address=10.0.0.6/24
interface=ether2
!
/routing bgp instance set default
as=65006 router-id=10.0.99.6
/routing bgp peer add remote-
address=10.0.0.1 remote-as=65001
/routing bgp network add
network=10.0.99.6/32
!
```

**RouterOS**

```
set system host-name VyOS
!
set interfaces loopback lo address
10.0.99.7/32
set interfaces ethernet eth2 address
10.0.0.7/24
!
set protocols bgp 65007 parameters
router-id 10.0.99.7
set protocols bgp 65007 neighbor
10.0.0.1 remote-as 65001
set protocols bgp 65007 network
10.0.99.7/32
!
```

**VyOS**

# コメント

- **設定の類似性**

- IOS, IOS-XEv, NX-OSv, ASA v はある程度、似ている
- IOS-XRv は(Cisco の中でも)独自路線
- **RouterOS と VyOS は意外と似ている**
- Vyatta と VyOS は構文が同じではあるものの、細かいパラメータがかなり異なる為、コンフィグの互換性は無い

- **eBGP における TTL の扱い**

- Cisco の場合、「ebgp-multihop」を指定しない限り、TTL = 1
- **RouterOS の場合、「ttl」を指定しない限り、TTL = 255**
- 一般的な eBGP においては TTL = 1 の方がベター

- **回避策はあるが、RouterOS でも Loopback 設定が出来るとベター**

- **試した限り、メーカー間の相互接続性も今のところ問題無し**

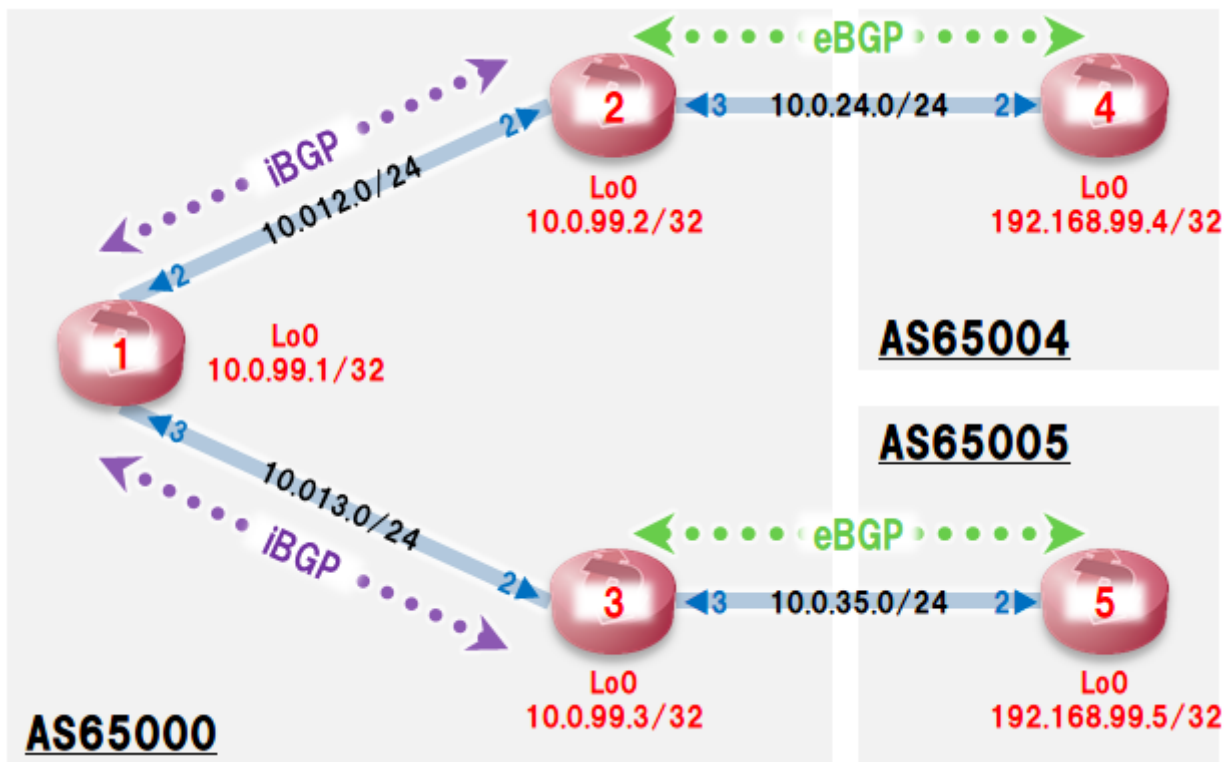
# iBGP RouteReflection

RouterOS を Route Reflector として設定する

# 構成

※ RR … Route Reflector

1 を RR として設定する



対象	メーカー	OS バージョン
全ルータ(1 ~ 5)	MikroTik	6.30.1

# RouterOS の設定

```
/system identity set name=R1
```

```
/interface bridge add name=loopback
```

```
/ip address add address=10.0.99.1/32 interface=loopback
```

```
/ip address add address=10.0.12.1/24 interface=ether2
```

```
/ip address add address=10.0.13.1/24 interface=ether3
```

```
/ip route add dst-address=10.0.0.0/8 type=blackhole
```

```
/routing ospf instance set 0 router-id=10.0.99.1
```

```
/routing ospf interface add interface=loopback passive=yes
```

```
/routing ospf network add network=10.0.12.0/24 area=backbone
```

```
/routing ospf network add network=10.0.13.0/24 area=backbone
```

```
/routing ospf network add network=10.0.99.1/32 area=backbone
```

```
/routing bgp instance set default as=65000 router-id=10.0.99.1
```

```
/routing bgp peer add remote-address=10.0.99.2 remote-as=65000 update-source=loopback
```

```
/routing bgp peer add remote-address=10.0.99.3 remote-as=65000 update-source=loopback
```

```
/routing bgp network add network=10.0.0.0/8
```

```
/routing bgp peer set 0 route-reflect=yes
```

```
/routing bgp peer set 1 route-reflect=yes
```

**各ルータを Route Reflector Client として設定  
その他は基本的に通常の iBGP と同じ設定で、特別な設定は無し**

# コメント

- **設定は簡単**
  - 基本的に RR の設定はどのメーカー製品でも簡単
  - RouterOS にはシンプルな CLI もリッチな GUI もある  
(※ 他メーカーには CLI しか無いケースも多い)
- RR にはトラフィック転送能力より、計算能力を要求される
  - よって、ホストマシンの CPU / メモリを潤沢に使える  
仮想化版の方が向いている場合も多い
  - Juniper には仮想化版「VRR(Virtual Route Reflector)」がある
  - Cisco には仮想化版「IOS-XRv」があり、これを RR として動作させることで  
Juniper の VRR 相当のことが可能
  - MikroTik の CHR (Cloud Hosted Router ) にも同じ可能性もある
- **特定経路の検索が非常にやりにくい**
  - 出来なくはないが、ISP ではかなり厳しい…

# 総括

技術的 / 全体的な観点からコメント



# 技術的な総括コメント

## • 設定について

- Cisco は情報量が多いが、「複雑な構文」等、歴史的な負の遺産も多い
- その点、RouterOS は構文もシンプルで理解しやすい
- 更に、構文を覚えたくないければ「リッチな GUI」も選択できる

## • ダイナミックルーティング＋アルファについて

- VRF、OSPF (v2 / v3)、BGP (iBGP / eBGP) を試した限り、問題無く動作する
- 特に「バグでハマる」等も無し
- Cisco や Juniper と比較すると、やや確認系コマンドが弱いように感じる  
例. ルーティングテーブルを検索する  
例. BGP テーブルを検索する  
→ 今後の充実に期待！

# 全体的な総括コメント

- **ビジネス的な観点について**
  - MikroTik 製品にはハードウェア性能/価格比に優れたものが多い
  - ローエンドマーケットは狙えると思うが、安価な Cisco もローエンド機器を投入しており、混戦必須、かも??
- **仮想化製品としての使い道**
  - 必ずしもハードウェア製品に頼らない使い方も面白いかも
    - 例 1. CHR を VRR 的な使い方をする
    - 例 2. AWS でルータとして使う
    - 例 3. SDN コントローラと組み合わせて、データプレーンとして利用する
- **OpenFlow 対応について**
  - JP マーケットでは、興味を持っている人が結構多い！！
  - しかし、現在は 1.0 しか対応していないので、使い物にならない…
  - **Extra Package を 1.3 以上に対応してください m(\_ \_)m**

# ユーザ会への要望

- **設定例について**
  - 公式 Wiki の掲載情報量が多い
  - 但し、OS のバージョンアップに追従出来ておらず、古い情報も散見される
- **ユーザ会サイトに掲載する情報について**
  - 相互接続実績等、個人では集めづらい情報が掲載されていると有り難い
  - IPsec、BGP 等の「設定値 / メーカー / 機種 / 接続結果」等  
→ ユーザ会というより、ちょっと業務っぽいですが…(^^;
- **妄想**
  - ニーズがあれば、公式 Wiki のローカライズもイイかも？
  - 「はじめての RouterOS」出版するとか？ 電子書籍ならハードル低い??

**ご清聴、ありがとうございました**

**多謝！**