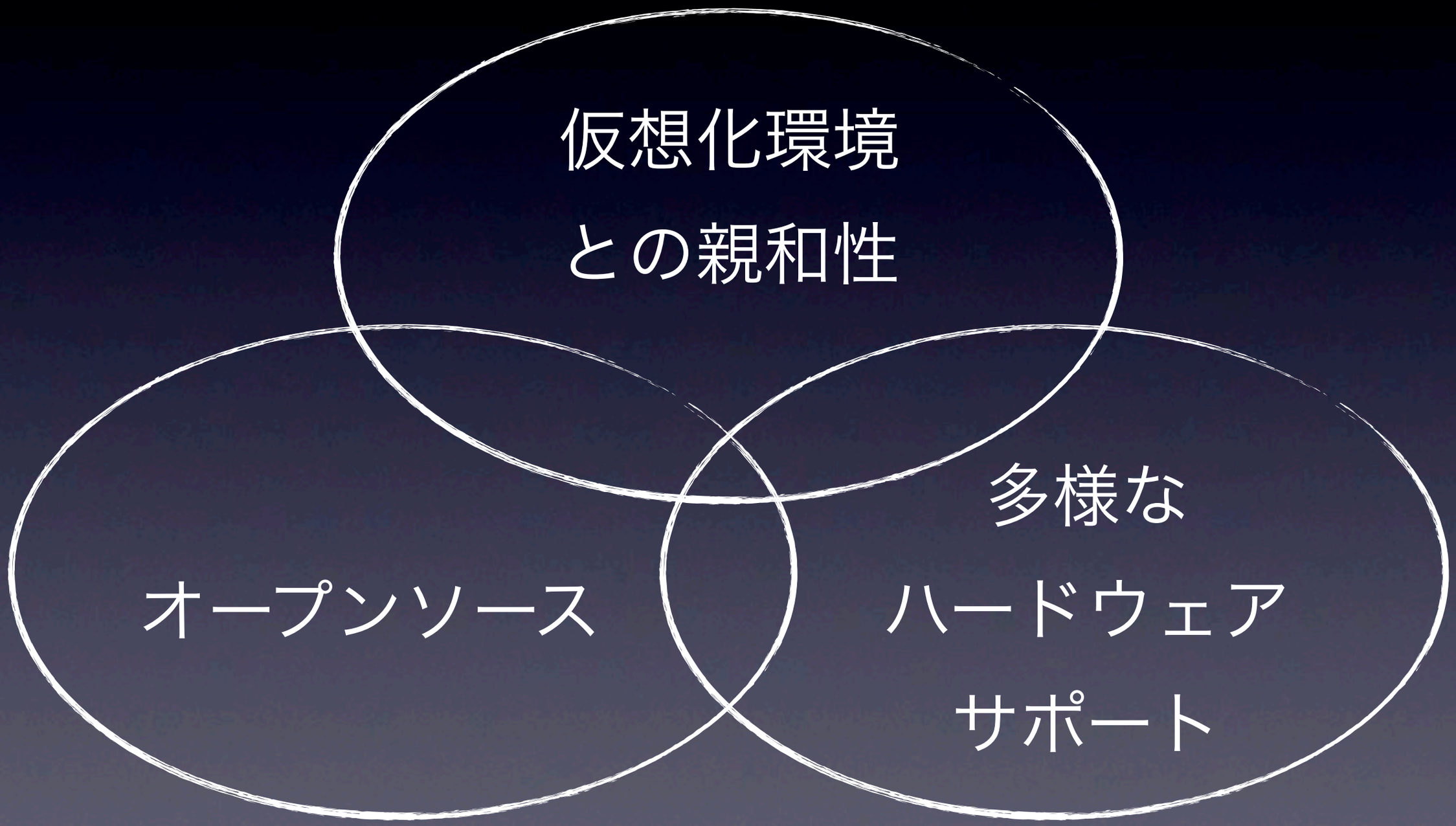
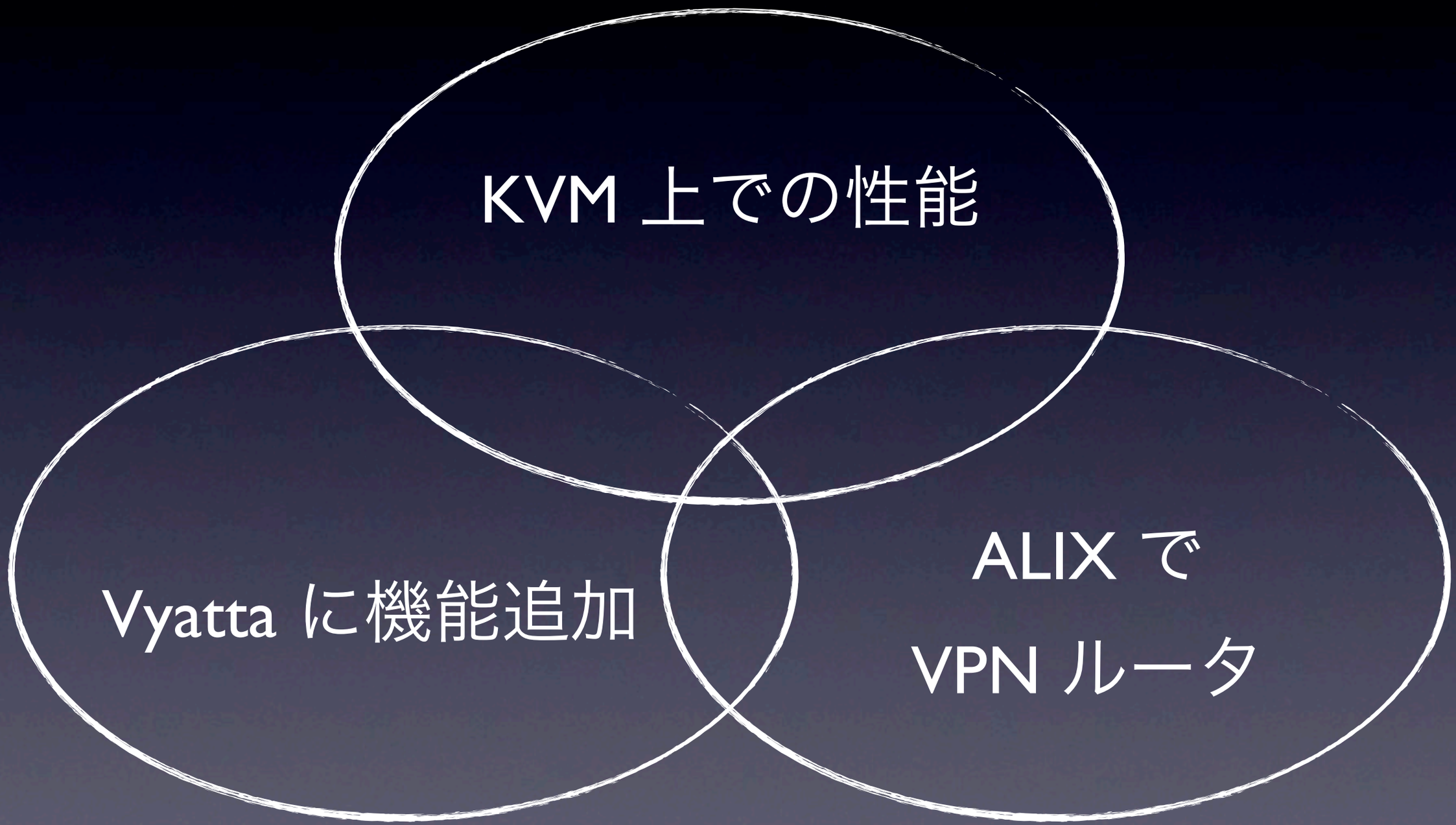
# Vyatta の利用例を
# いくつか...

浅間 正和 @ 有限会社 銀座堂

# Vyatta の特徴

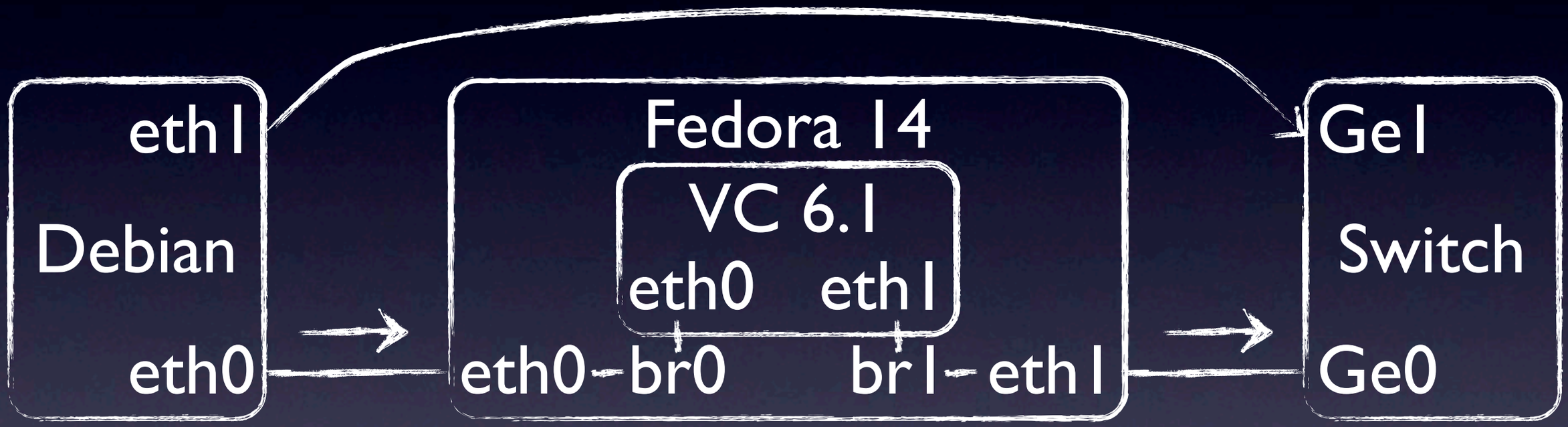


# Vyatta の特徴



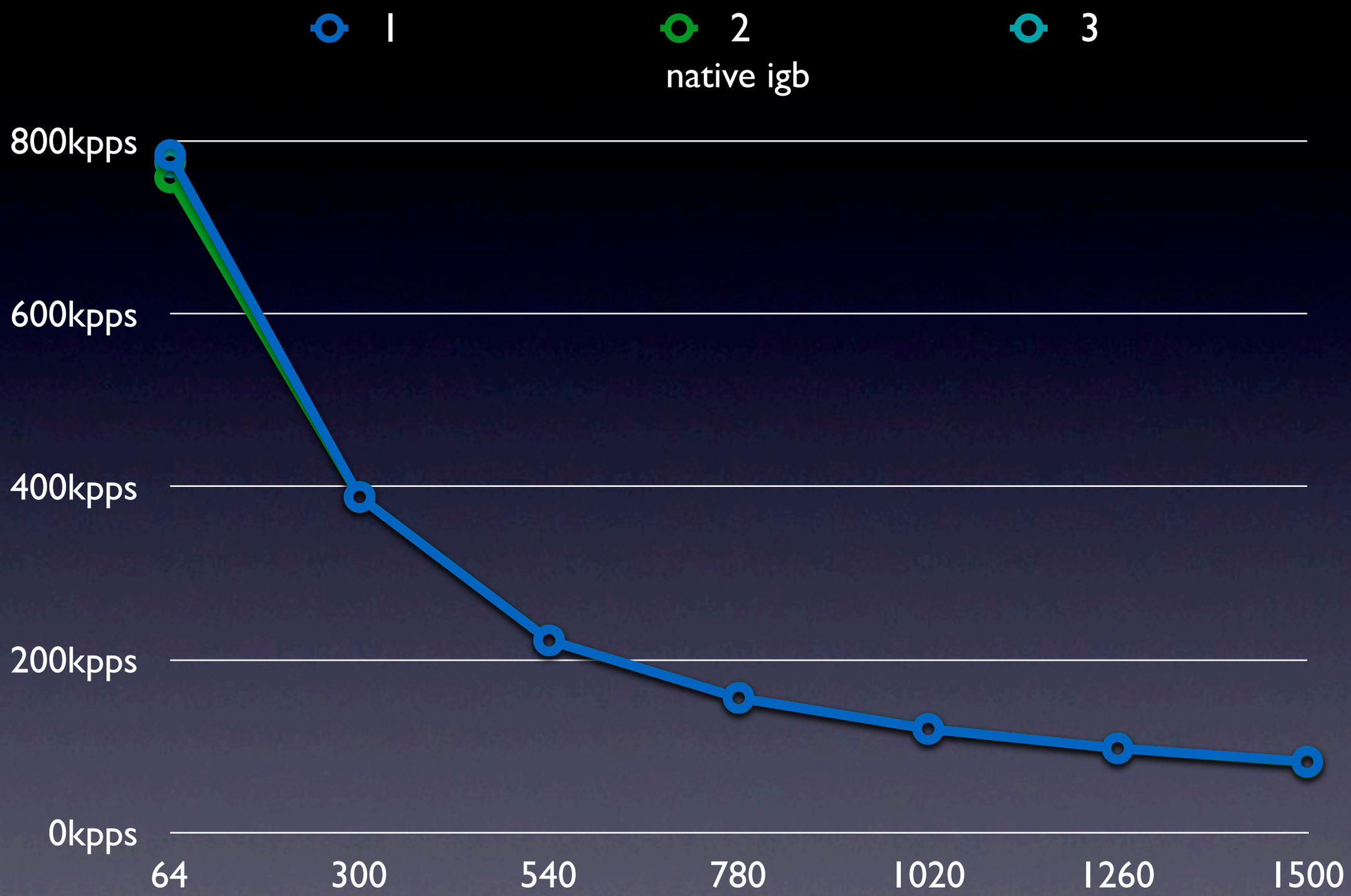
# KVM 上での性能

SNMP で Ge0 のカウンタ値を収集



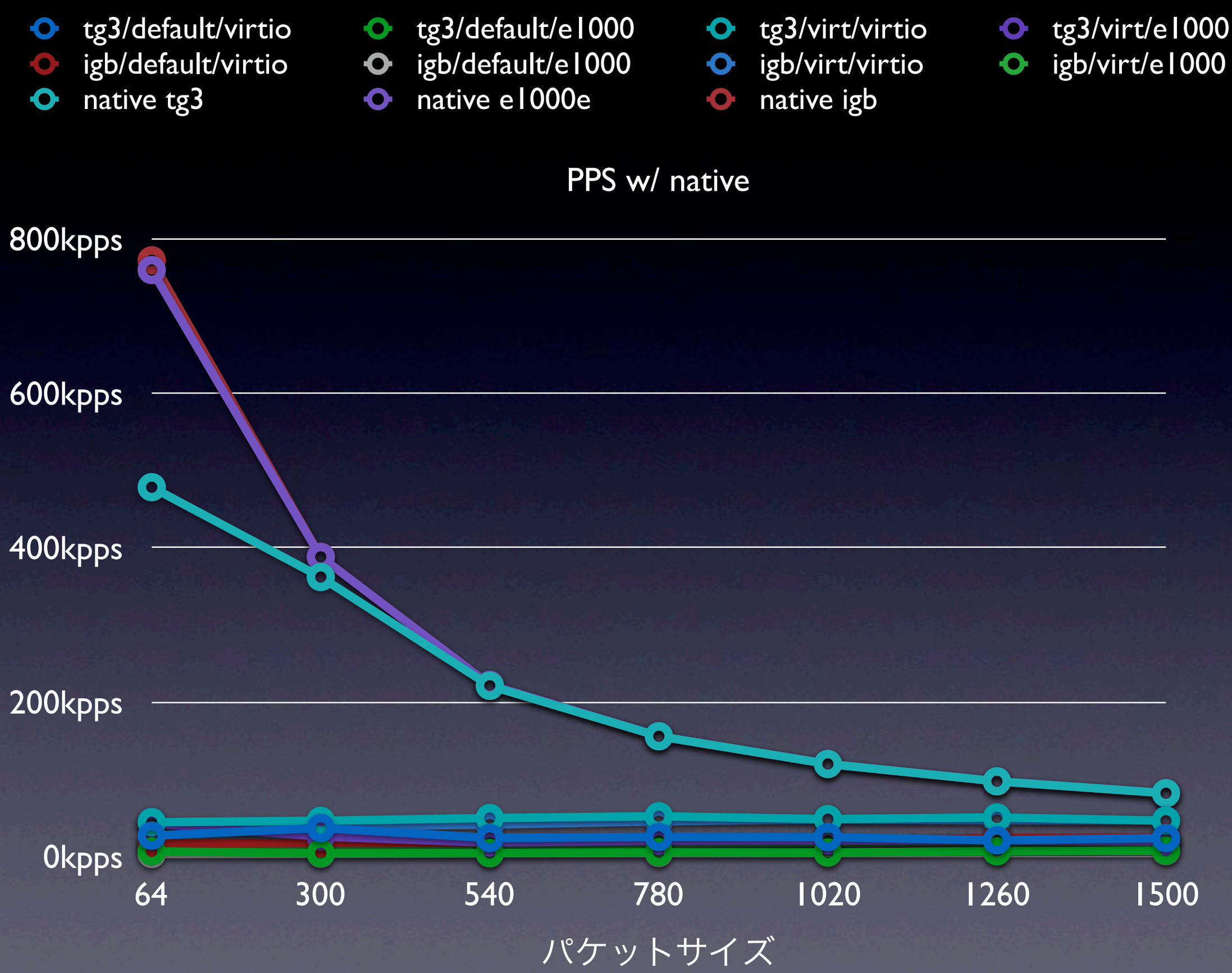

| CPU | Intel Xeon E5620 @ 2.40GHz (Quad Core) |
|---|---|
| Memory | DDR3 SDRAM 1333MHz 6GB |
| Physical NIC | Broadcom BCM5715(tg3) / Intel 82576EB(igb) |
| Install Image | Live CD iso(default) / Virtualization iso(virt) |
| Virtual NIC | Para-Virtual Driver(virtio) / Intel e1000 Emulation(e1000) |


1
2
native tg3
3
500kpps
375kpps
250kpps
125kpps
0kpps
64
300
540
780
1020
1260
1500

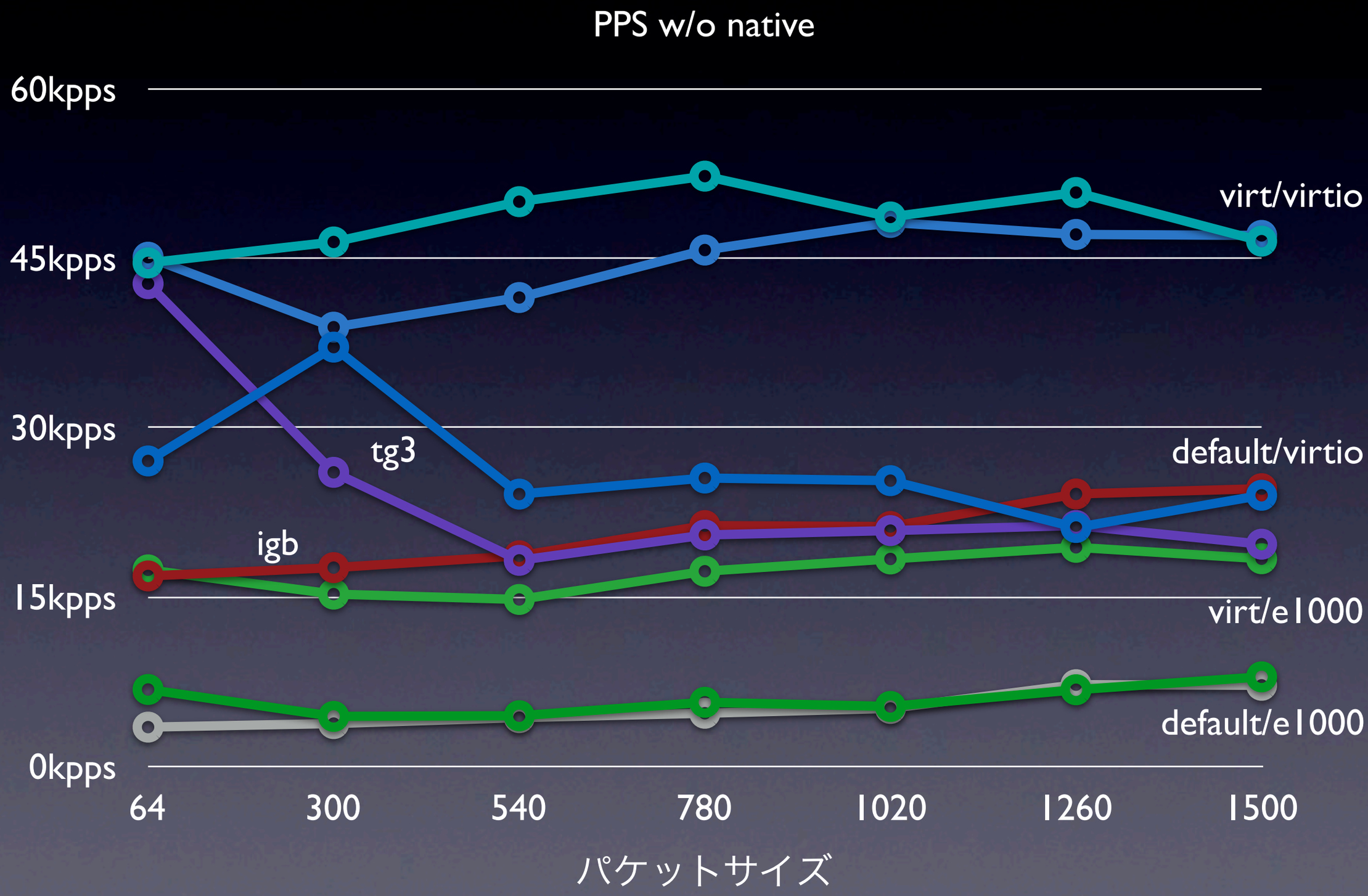

1
2
native igb
3
800kpps
600kpps
400kpps
200kpps
0kpps
64
300
540
780
1020
1260
1500


1
2
3
tg3/virt/virtio
80kpps
60kpps
40kpps
20kpps
0kpps
64
300
540
780
1020
1260
1500


1
2
3
tg3/default/e1000
8kpps
6kpps
4kpps
2kpps
0kpps
64
300
540
780
1020
1260
1500


tg3/default/virtio
igb/default/virtio
native tg3
tg3/default/e1000
igb/default/e1000
native e1000e
tg3/virt/virtio
igb/virt/virtio
native igb
tg3/virt/e1000
igb/virt/e1000
PPS w/ native
800kpps
600kpps
400kpps
200kpps
0kpps
64
300
540
780
1020
1260
1500
パケットサイズ

tg3/default/virtio
igb/default/virtio
tg3/default/e1000
igb/default/e1000
tg3/virt/virtio
igb/virt/virtio
tg3/virt/e1000
igb/virt/e1000



tg3/default/virtio
igb/default/virtio
native tg3
tg3/default/e1000
igb/default/e1000
native e1000e
tg3/virt/virtio
igb/virt/virtio
native igb
tg3/virt/e1000
igb/virt/e1000

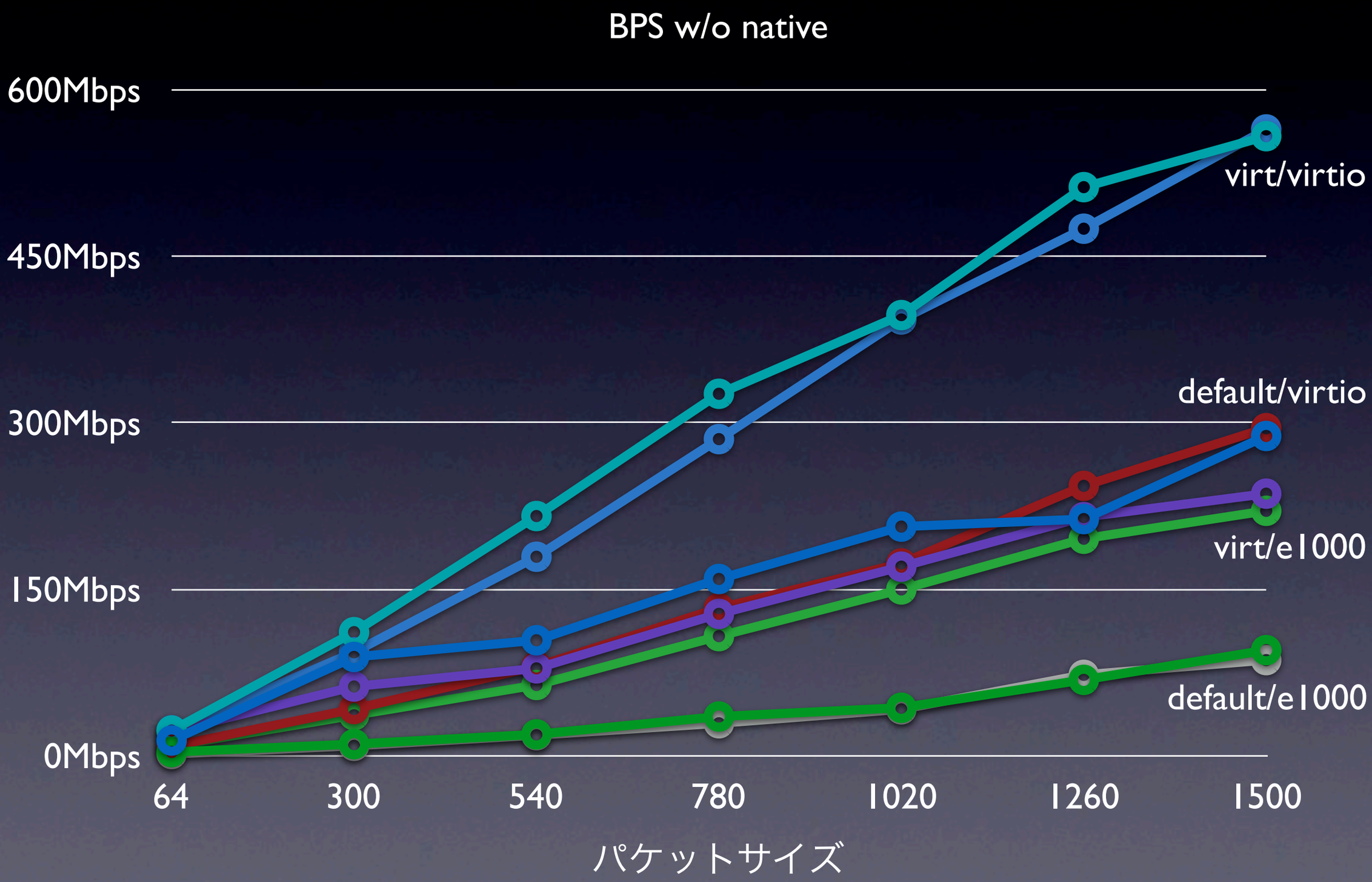
BPS w/ native

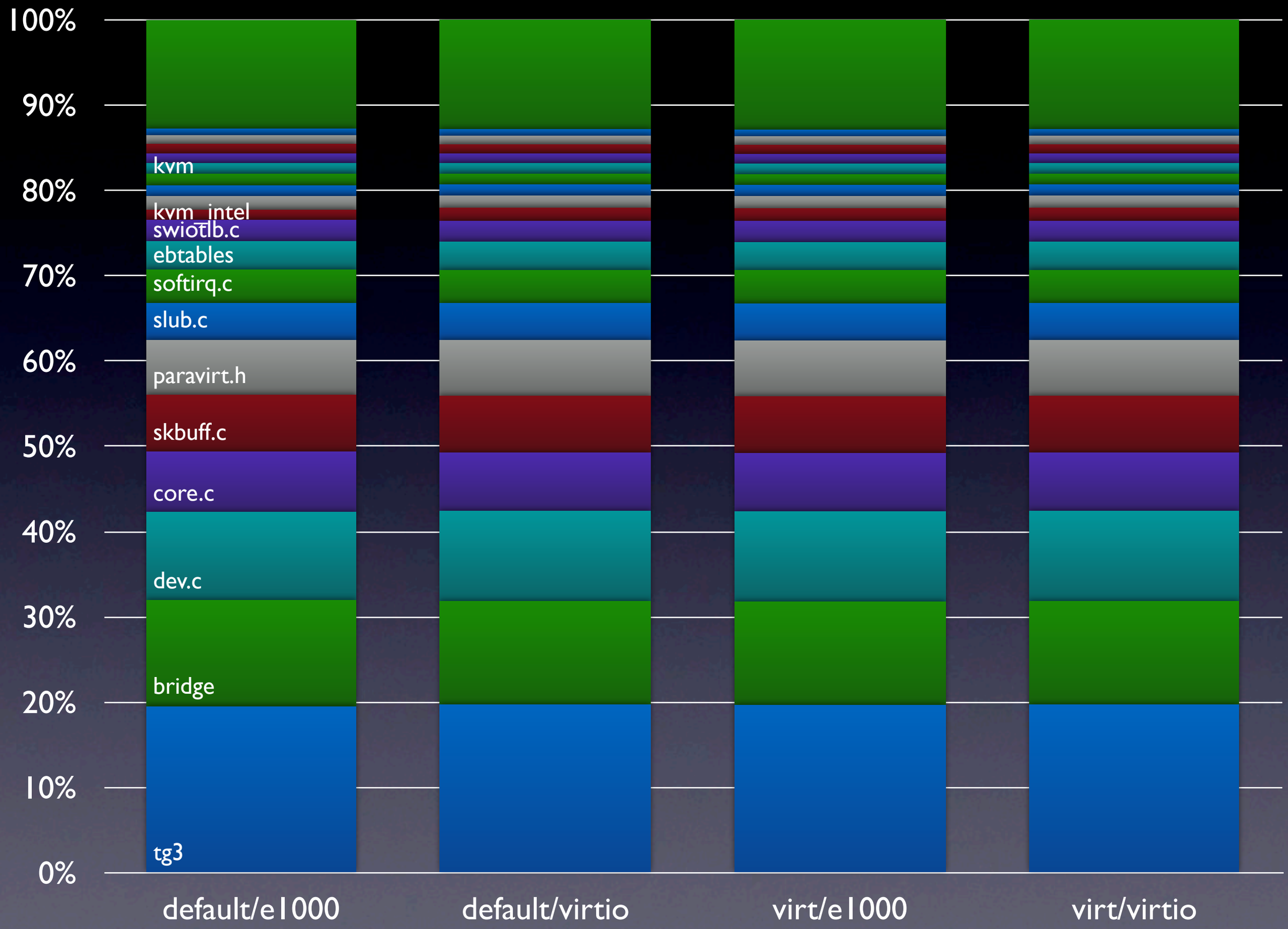
1000Mbps
750Mbps
500Mbps
250Mbps
0Mbps

64
300
540
780
1020
1260
1500

パケットサイズ

tg3/default/virtio
igb/default/virtio
tg3/default/e1000
igb/default/e1000
tg3/virt/virtio
igb/virt/virtio
tg3/virt/e1000
igb/virt/e1000




100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
kvm
kvm_intel
swiotlb.c
ebtables
softirq.c
slub.c
paravirt.h
skbuff.c
core.c
dev.c
bridge
tg3
default/e1000
default/virtio
virt/e1000
virt/virtio

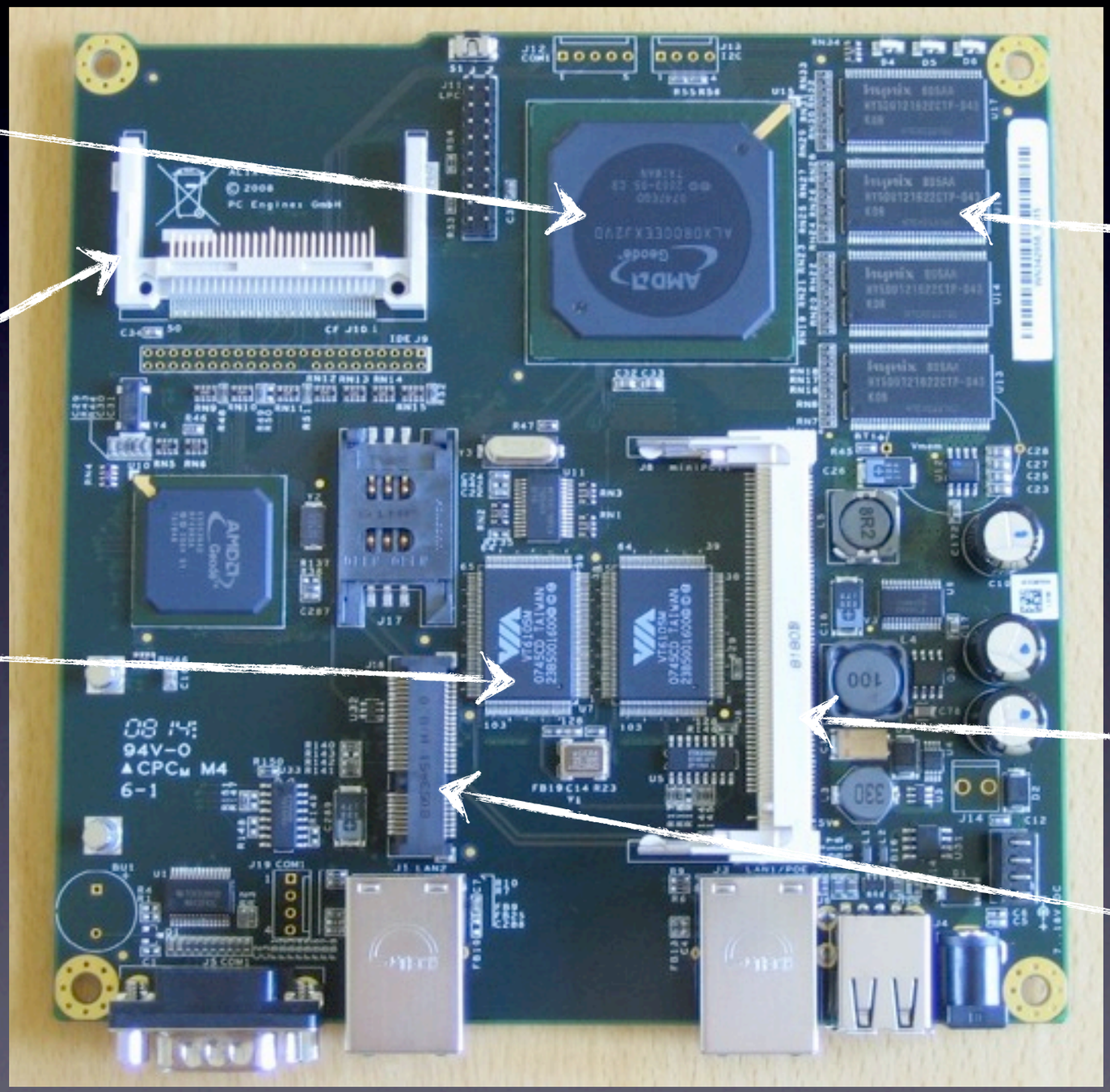
# ALIX でVPN ルータ

AMD Geode
LX800 500MHz

CompactFlash
socket

VIA VT6105M
x 2

PC Engines
alix6b2




Memory
256MB DDR

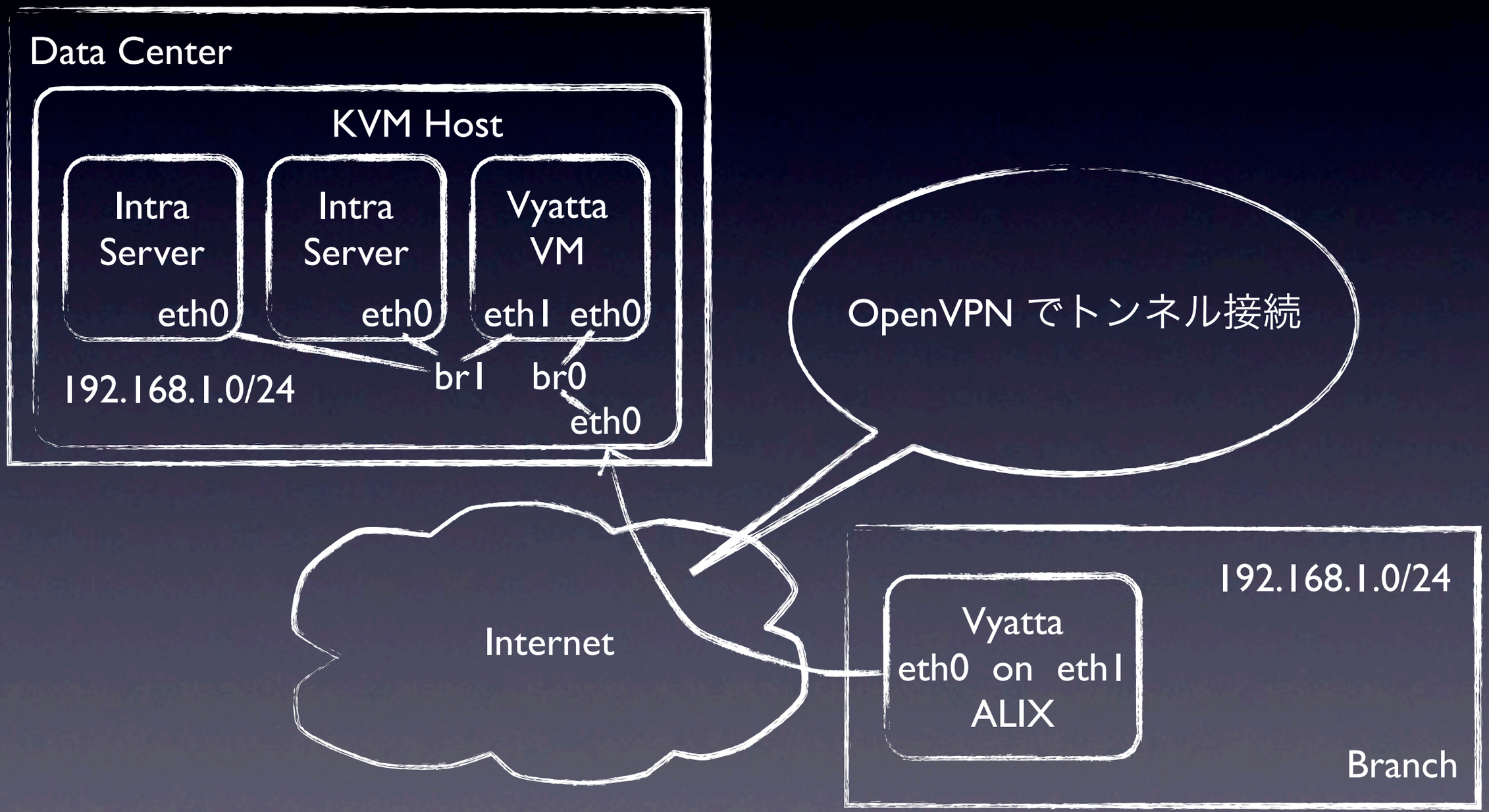
miniPCI slot

miniPCI
Express slot
(USB only)

# ALIX でVPN ルータ

- CF slot か PC card slot のあるパソコンを準備
- Vyatta の CD-ROM から起動
- install-system でインストール先に CF を指定(GRUB も CF にインストール)
- パソコンの OS を消さないように注意

# ALIX で VPN ルータ



# ALIX でVPN ルータ

```
vyatta@vyatta:~$ sudo su -
vyatta:~# cd /usr/share/doc/openvpn/examples/easy-rsa/2.0
vyatta:/usr/share/doc/openvpn/examples/easy-rsa/2.0# . ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /usr/share/doc/openvpn/
examples/easy-rsa/2.0/keys
vyatta:/usr/share/doc/openvpn/examples/easy-rsa/2.0# ./clean-all
```

# ALIX でVPN ルータ

```
vyatta:/usr/share/doc/openvpn/examples/easy-rsa/2.0# ./build-ca
Generating a 1024 bit RSA private key
.............++++++
.........................................++++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:JP
State or Province Name (full name) [CA]:Niigata
Locality Name (eg, city) [SanFrancisco]:Sanjo
Organization Name (eg, company) [Fort-Funston]:Ginzado
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [Fort-Funston CA]:Ginzado
Name []:
Email Address [me@myhost.mydomain]:m-asama@ginzado.ne.jp
```

# ALIX でVPN ルータ

```
vyatta:/usr/share/doc/openvpn/examples/easy-rsa/2.0# ./build-key-server server
Generating a 1024 bit RSA private key
.........................++++++
.....++++++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:JP
State or Province Name (full name) [CA]:Niigata
Locality Name (eg, city) [SanFrancisco]:Sanjo
Organization Name (eg, company) [Fort-Funston]:Ginzado
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [server]:
Name []:
Email Address [me@myhost.mydomain]:m-asama@ginzado.ne.jp

...
```

# ALIX でVPN ルータ

```
vyatta:/usr/share/doc/openvpn/examples/easy-rsa/2.0# ./build-key client
Generating a 1024 bit RSA private key
.............++++++
..........++++++
writing new private key to 'client.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:JP
State or Province Name (full name) [CA]:Niigata
Locality Name (eg, city) [SanFrancisco]:Sanjo
Organization Name (eg, company) [Fort-Funston]:Ginzado
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [client]:
Name []:
Email Address [me@myhost.mydomain]:m-asama@ginzado.ne.jp

...
```

# ALIX でVPN ルータ

```
vyatta:/usr/share/doc/openvpn/examples/easy-rsa/2.0# ./build-dh
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
.....................+.....................................
+.........++*++*++*
vyatta:/usr/share/doc/openvpn/examples/easy-rsa/2.0# ls -l keys/
total 68
-rw-r--r-- 1 root root 3864 Dec 20 07:08 01.pem
-rw-r--r-- 1 root root 3747 Dec 20 07:09 02.pem
-rw-r--r-- 1 root root 1208 Dec 20 07:07 ca.crt
-rw------- 1 root root  887 Dec 20 07:07 ca.key
-rw-r--r-- 1 root root 3747 Dec 20 07:09 client.crt
-rw-r--r-- 1 root root  672 Dec 20 07:09 client.csr
-rw------- 1 root root  887 Dec 20 07:09 client.key
-rw-r--r-- 1 root root  245 Dec 20 07:09 dh1024.pem
-rw-r--r-- 1 root root  216 Dec 20 07:09 index.txt
-rw-r--r-- 1 root root   20 Dec 20 07:09 index.txt.attr
-rw-r--r-- 1 root root   21 Dec 20 07:08 index.txt.attr.old
-rw-r--r-- 1 root root  108 Dec 20 07:08 index.txt.old
-rw-r--r-- 1 root root    3 Dec 20 07:09 serial
-rw-r--r-- 1 root root    3 Dec 20 07:08 serial.old
-rw-r--r-- 1 root root 3864 Dec 20 07:08 server.crt
-rw-r--r-- 1 root root  672 Dec 20 07:08 server.csr
-rw------- 1 root root  887 Dec 20 07:08 server.key
```

ALIX で必要

KVM で必要

# ALIX でVPN ルータ

```
vyatta@server# set interfaces ethernet eth0 address 192.0.2.123/24
vyatta@server# set interfaces gateway-address 192.0.2.1
vyatta@server# set interfaces name-server 192.0.2.2
vyatta@server# set interfaces openvpn vtun0
vyatta@server# set interfaces openvpn vtun0 mode server
vyatta@server# set interfaces openvpn vtun0 server subnet 192.168.123.0/24
vyatta@server# set interfaces openvpn vtun0 tls ca-cert-file /root/keys/ca.crt
vyatta@server# set interfaces openvpn vtun0 tls cert-file /root/keys/server.crt
vyatta@server# set interfaces openvpn vtun0 tls key-file /root/keys/server.key
vyatta@server# set interfaces openvpn vtun0 tls dh-file /root/keys/dh1024.pem
vyatta@server# set interfaces bridge br0
vyatta@server# set interfaces ethernet eth1 bridge-group bridge br0
vyatta@server# set interfaces openvpn vtun0 bridge-group bridge br0

vyatta@client# set interfaces ethernet eth0 address dhcp
vyatta@client# set interfaces openvpn vtun0
vyatta@client# set interfaces openvpn vtun0 mode client
vyatta@client# set interfaces openvpn vtun0 remote-host 192.0.2.123
vyatta@client# set interfaces openvpn vtun0 tls ca-cert-file /root/keys/ca.crt
vyatta@client# set interfaces openvpn vtun0 tls cert-file /root/keys/client.crt
vyatta@client# set interfaces openvpn vtun0 tls key-file /root/keys/client.key
vyatta@client# set interfaces bridge br0
vyatta@client# set interfaces ethernet eth1 bridge-group bridge br0
vyatta@client# set interfaces openvpn vtun0 bridge-group bridge br0
```

# Vyatta に機能追加

- 次期 Vyatta は Linux Kernel 2.6.35 らしい
- どうも最初から
  CONFIG_IPV6_SIT_6RD=y らしい

- 6RD Border Relay 対応の Vyatta を作ってみましょうか

# Vyatta に機能追加

- Linux 6RD HOWTO* によると以下のコマンドで設定するらしい * http://www.litech.org/6rd/

```
# ip tunnel add tun0 mode sit local 10.0.0.1
# ip tunnel 6rd dev tun0 6rd-prefix 2001:db8:0:1000::/52 ¥
                         6rd-relay_prefix 10.0.0.0/20
# ip addr add 2001:db8:0:1001::/52 dev tun0
```

- それならVyatta はこんな感じ？？

```
# set interfaces tunnel tun0
# set interfaces tunnel tun0 encapsulation sit
# set interfaces tunnel tun0 local-ip 10.0.0.1
# set interfaces tunnel tun0 6rd-prefix 2001:db8:0:1000::/52
# set interfaces tunnel tun0 6rd-relay_prefix 10.0.0.0/20
# set interfaces tunnel tun0 address 2001:db8:0:1001::/52
# commit
```

# Vyatta に機能追加

1) Debian Squeeze の環境を用意
2) apt-get install git-core で git を用意
3) git clone http://git.vyatta.com/build-iso.git
4) git checkout --track -b mendocino origin/mendocino
5) cd build-iso; less README; less INSTALL
6) git submodule init
7) git submodule update pkgs/vyatta-cfg-system
8) （vyatta-cfg-system の中身を改造）
9) autoreconf -i && ./configure
10) make vyatta-cfg-system
11) sudo make iso

mendocino は
次期Vyatta の
開発コードネーム
（ロードマップ参照）

README には build に
必要なパッケージ一覧
とかが書かれています

改造したいパッケージ
のみの update で OK

パッケージの build

livecd に binary.iso が
出来る

# Vyatta に機能追加

```
diff -Naru vyatta-cfg.orig/templates/interfaces/tunnel/node.def ...
--- vyatta-cfg.orig/templates/interfaces/tunnel/node.def
+++ vyatta-cfg/templates/interfaces/tunnel/node.def
@@ -8,7 +8,7 @@

 commit:expression: $VAR(./local-ip/) != "" ;                          \
                    "Must configure the tunnel local-ip for $VAR(@)"
-commit:expression: $VAR(./remote-ip/) != "" ;                         \
+commit:expression: $VAR(./remote-ip/) != "" || $VAR(./6rd-prefix/) != "" ; \
                    "Must configure the tunnel remote-ip for $VAR(@)"
 commit:expression: $VAR(./encapsulation/) != "" ;                     \
                    "Must configure the tunnel encapsulation for $VAR(@)"
@@ -26,6 +26,9 @@
         if [ "$VAR(./encapsulation/@)" == "gre-bridge" ]; then
            ip link add $VAR(@) type gretap local $VAR(./local-ip/@) remote $VAR(./remote-
ip/@) ||
               echo "interfaces tunnel $VAR(@): error creating tunnel interface"
+       elif [ "$VAR(./encapsulation/@)" == "sit" ]; then
+          ip tunnel add $VAR(@) local $VAR(./local-ip/@) mode $VAR(./encapsulation/@)
$KEY ||
+             echo "interfaces tunnel $VAR(@): error creating tunnel interface"
         else
            ip tunnel add $VAR(@) local $VAR(./local-ip/@) remote $VAR(./remote-ip/@) mode
$VAR(./encapsulation/@) $KEY ||
               echo "interfaces tunnel $VAR(@): error creating tunnel interface"
```

# Vyatta に機能追加

```
diff -Naru vyatta-cfg.orig/templates/interfaces/tunnel/node.tag/6rd-prefix/node.def ...
--- vyatta-cfg.orig/templates/interfaces/tunnel/node.tag/6rd-prefix/node.def
+++ vyatta-cfg/templates/interfaces/tunnel/node.tag/6rd-prefix/node.def
@@ -0,0 +1,11 @@
+type: ipv6net
+help: 6rd-prefix
+syntax:expression: exec "${vyatta_sbindir}/check_prefix_boundary $VAR(@)"
+
+update:if [ x$VAR(../6rd-relay_prefix/@) != x"" ]; then
+          ip tunnel 6rd dev $VAR(../@) 6rd-prefix $VAR(@) 6rd-relay_prefix $VAR(../6rd-
relay_prefix/@);
+       else
+          ip tunnel 6rd dev $VAR(../@) 6rd-prefix $VAR(@);
+       fi
+
+delete:ip tunnel 6rd dev $VAR(../@) 6rd-reset
diff -Naru vyatta-cfg.orig/templates/interfaces/tunnel/node.tag/6rd-relay_prefix/node.def
--- vyatta-cfg.orig/templates/interfaces/tunnel/node.tag/6rd-relay_prefix/node.def
+++ vyatta-cfg/templates/interfaces/tunnel/node.tag/6rd-relay_prefix/node.def
@@ -0,0 +1,6 @@
+type: ipv4net
+help: 6rd-relay_prefix
+syntax:expression: exec "${vyatta_sbindir}/check_prefix_boundary $VAR(@)"
+
+update:expression: "true"
+delete:expression: "true"
```