RTBH実装例の紹介
～AS9370編～

さくらインターネット(株)
技術部　大久保修一
ohkubo@sakura.ad.jp

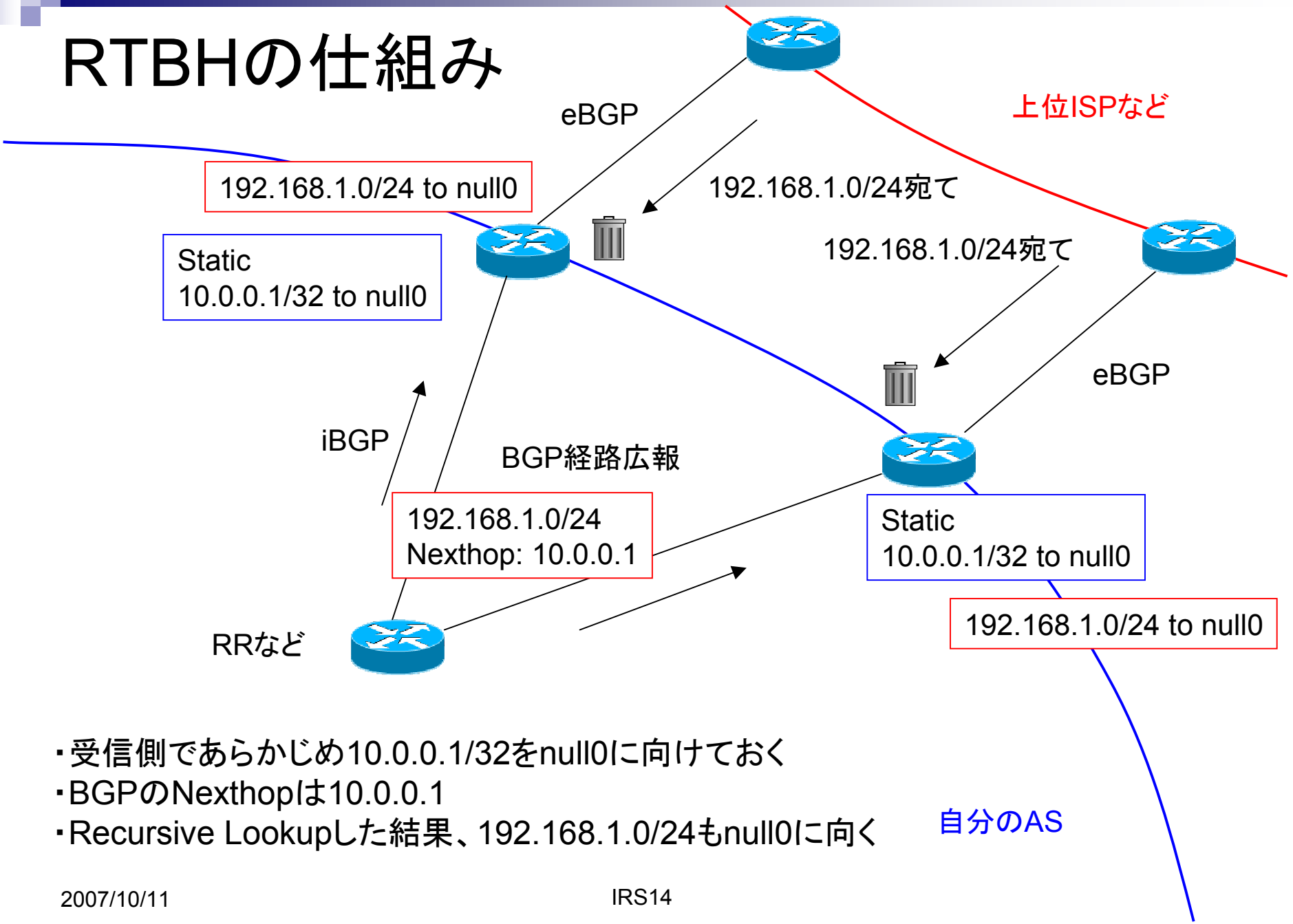
今日のAgenda

- はじめに
- RTBHとは？
- RTBH実装の背景
- 構成の検討
- ルータの試験
- OSPF vs BGP
- BGP広報経路のRTBH化
- まとめ

RTBHとは？

- Remotely Triggered Black Hole Filteringの略
- NANOG23(2001/10)で紹介されました
  - ISP Security - Real World Techniques
    Remote Triggered Black Hole Filtering and
    Backscatter Traceback
  - http://www.nanog.org/mtg-0110/greene.html
- BGPにてNexthopをnullに向けた経路を広報することにより、AS内の全BGPルータに、一斉にnull routingを設定できる。
- DoSアタックの対応方法の1つ

RTBHの仕組み



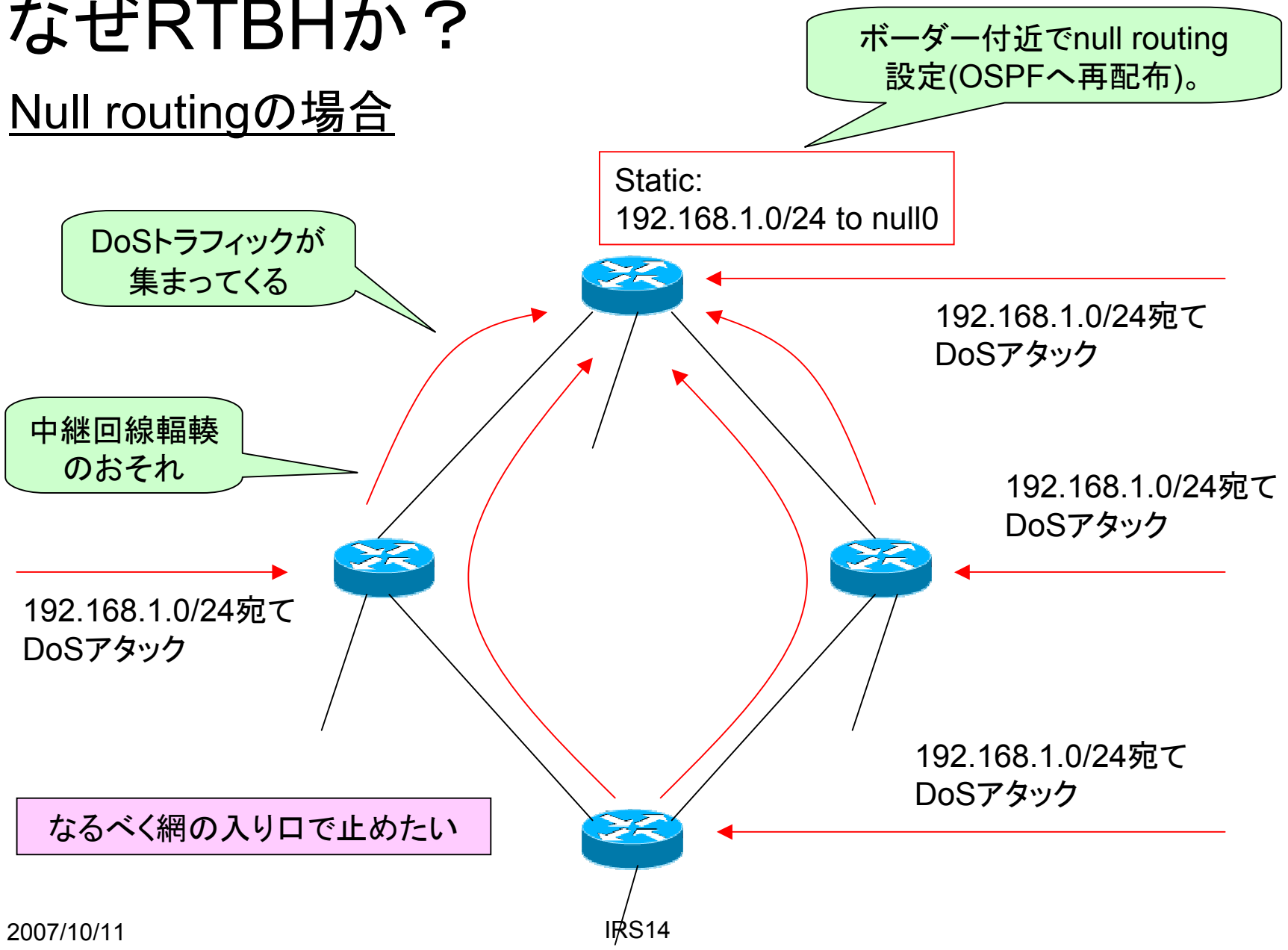
・受信側であらかじめ10.0.0.1/32をnull0に向けておく
・BGPのNexthopは10.0.0.1
・Recursive Lookupした結果、192.168.1.0/24もnull0に向く

RTBH導入の背景

- DoSアタック発生時、以前はボーダー付近のnull routingで対応していた。
- 最近のDoSアタックは、、、
  - 規模が大きくなってきた。(数Gbps)
  - 分散型(DDoS)になってきた。
- 単純なnull routingでは、10Gbps中継回線の輻輳が懸念。
- RTBHにより、網の入り口で破棄できるようにしたい。

なぜRTBHか？

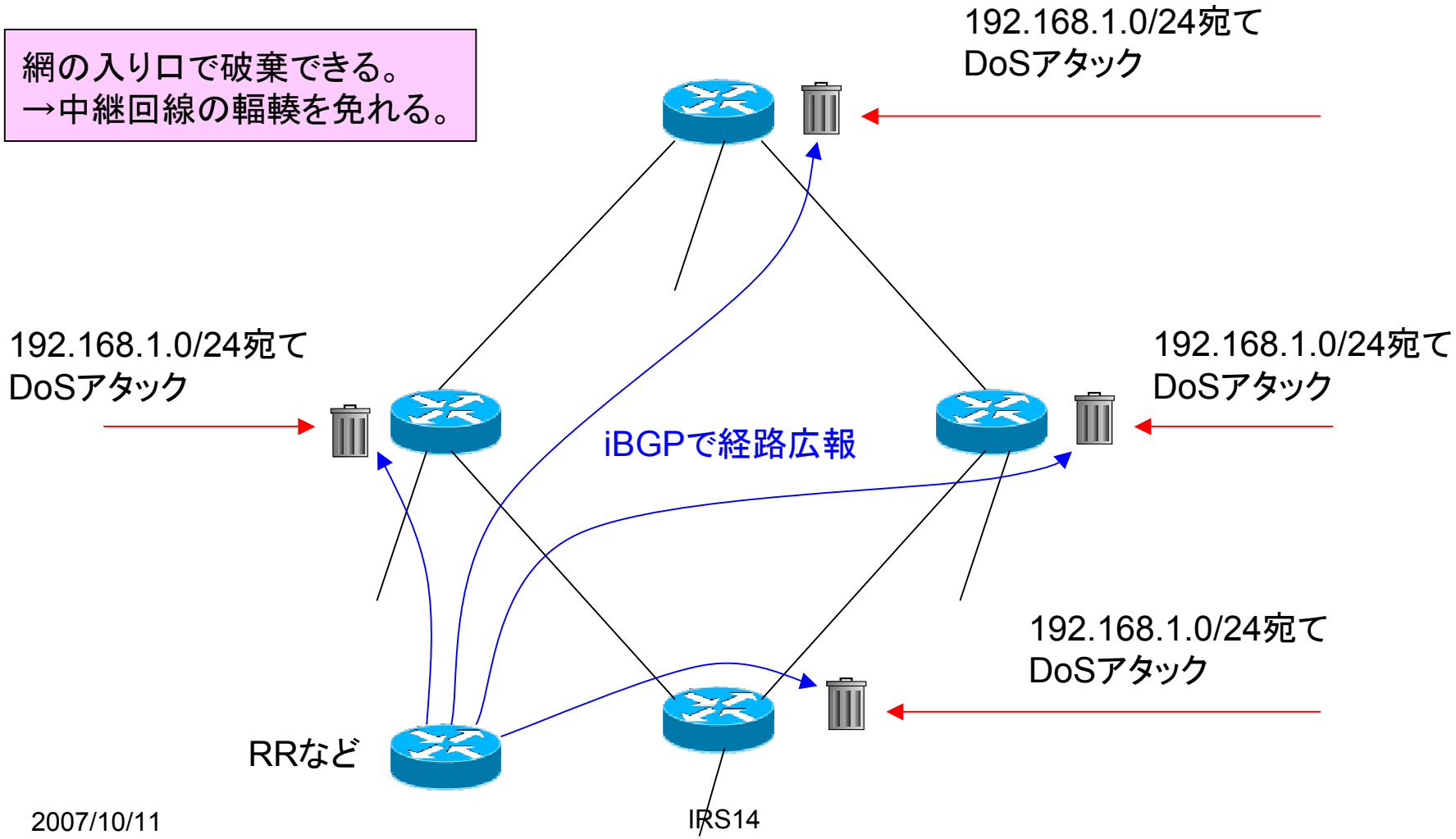
Null routingの場合



なぜRTBHか？

RTBHの場合

網の入り口で破棄できる。
→中継回線の輻輳を免れる。

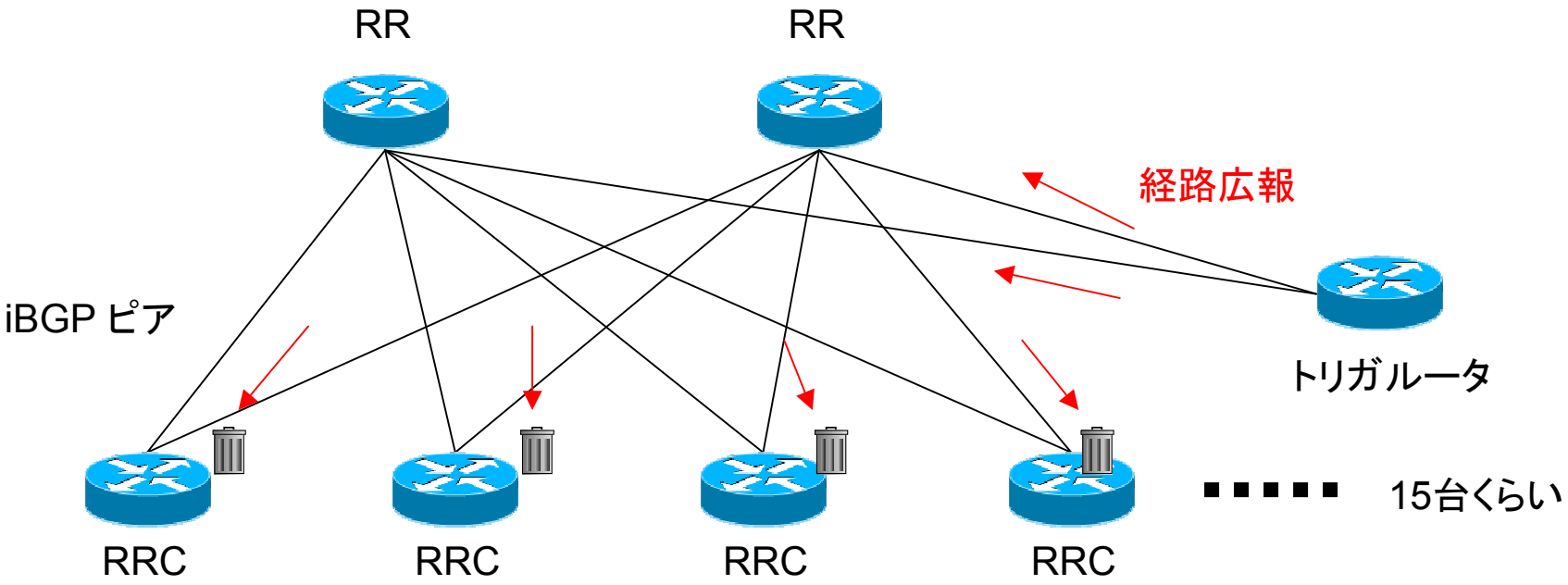


構成の検討

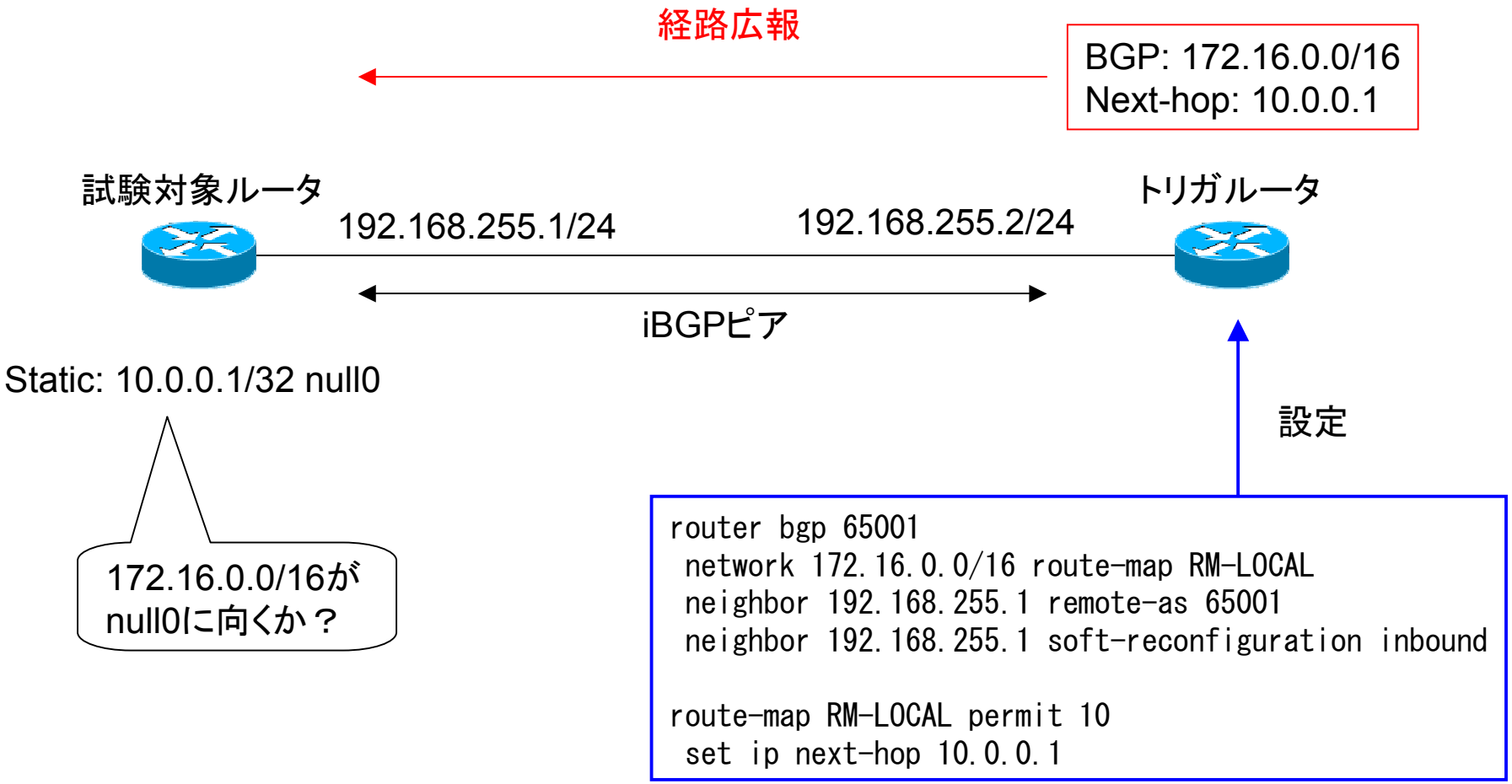
- BGP Community
  - 9370:XXX no-export
- あらかじめNullに向けておくアドレス
  - 他の実装例では、TestNet(192.0.2.0/24)を使ってるケースが多い？
  - 弊社では、グローバルアドレスのうち、Anycast用のブロックから/32のIPアドレスを確保
- 経路広報の方法
  - 既存のRRで生成するか？
  - トリガルータ（RTBH経路広報専用ルータ）を準備するか？

トリガルータ

- RRで経路生成するよりも、専用のトリガルータを用意するのが、オペレーション上よさそう。
  - →トリガルータを専用に準備
- FreeBSD-6.2RELEASE+quagga 0.99.7



ルータの試験


経路広報
BGP: 172.16.0.0/16
Next-hop: 10.0.0.1
試験対象ルータ
192.168.255.1/24
192.168.255.2/24
トリガルータ
iBGPピア
Static: 10.0.0.1/32 null0
172.16.0.0/16が
null0に向くか？
設定
router bgp 65001
network 172.16.0.0/16 route-map RM-LOCAL
neighbor 192.168.255.1 remote-as 65001
neighbor 192.168.255.1 soft-reconfiguration inbound
route-map RM-LOCAL permit 10
set ip next-hop 10.0.0.1

ルータの試験

- 問題なく動作するルータ
  - Foundry BigIron-RXシリーズ
  - Force10 Eシリーズ
  - ALAXALA 7800Rシリーズ
- RTBHが動作しないルータ
  - Foundry NetIronシリーズ
  - BGP Next-hopがnull0を向いていると採用されない。
  - 仕様？バグ？

```
NetIron Router#sho ip bgp
Total number of BGP Routes: 1
Status codes: s suppressed, d damped, h history, * valid, > best, i internal
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            Next Hop        Metric      LocPrf Weight Path
*i  172.16.0.0/16      10.0.0.1        0           100    0      i
```

BESTにならない。。。

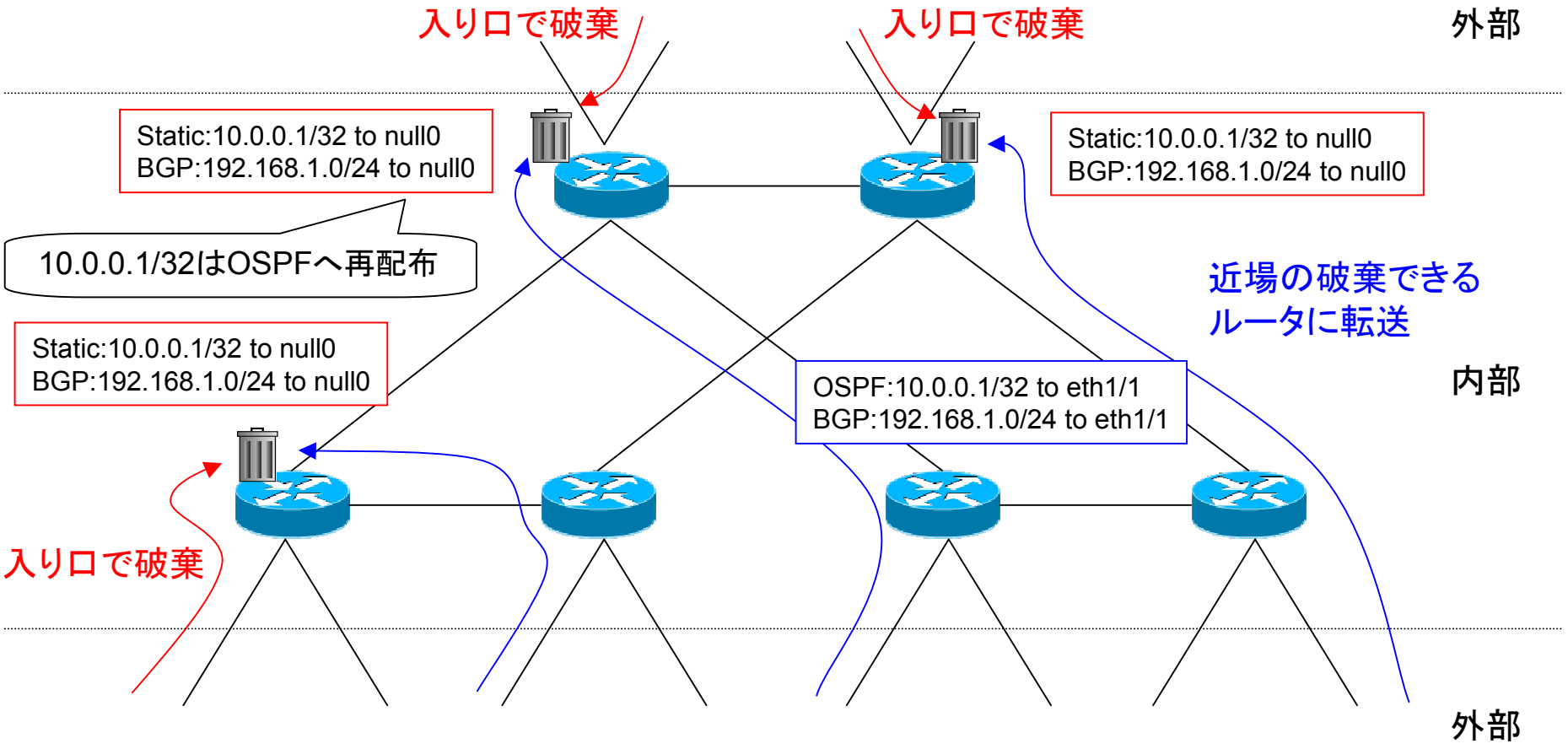
パケット破棄が遅いルータ

- Null0宛てのパケットをCPU処理するルータ
  - Forwardingはハードウェア処理
- 大量のトラフィックを破棄させると、、、
  - CPU負荷上昇
  - →BGPピアダウン
  - →通信障害
  - →Telnetログインもできない
- 破棄よりもForwardingしたほうが速い。。。

ワークアラウンド

- RTBHが動作しないルータ
- パケット破棄が遅いルータ

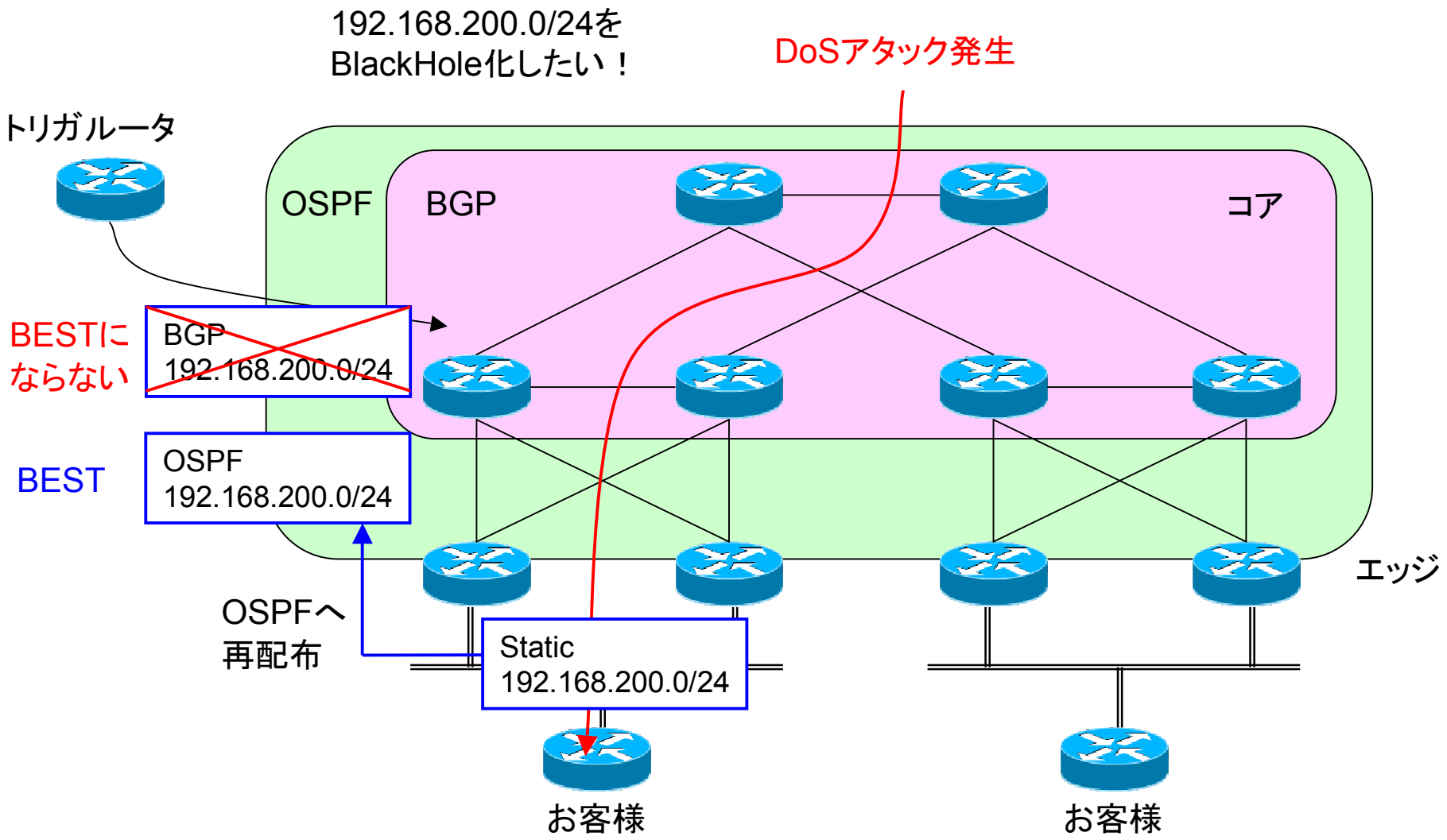
→ Anycast的に破棄させる



OSPF vs BGP

- BlackHoleしようとする経路がOSPFで観測されていると、BGP経路がBESTにならない。
- RTBHで破棄できず、OSPF経路に沿ってそのまま転送され続ける。

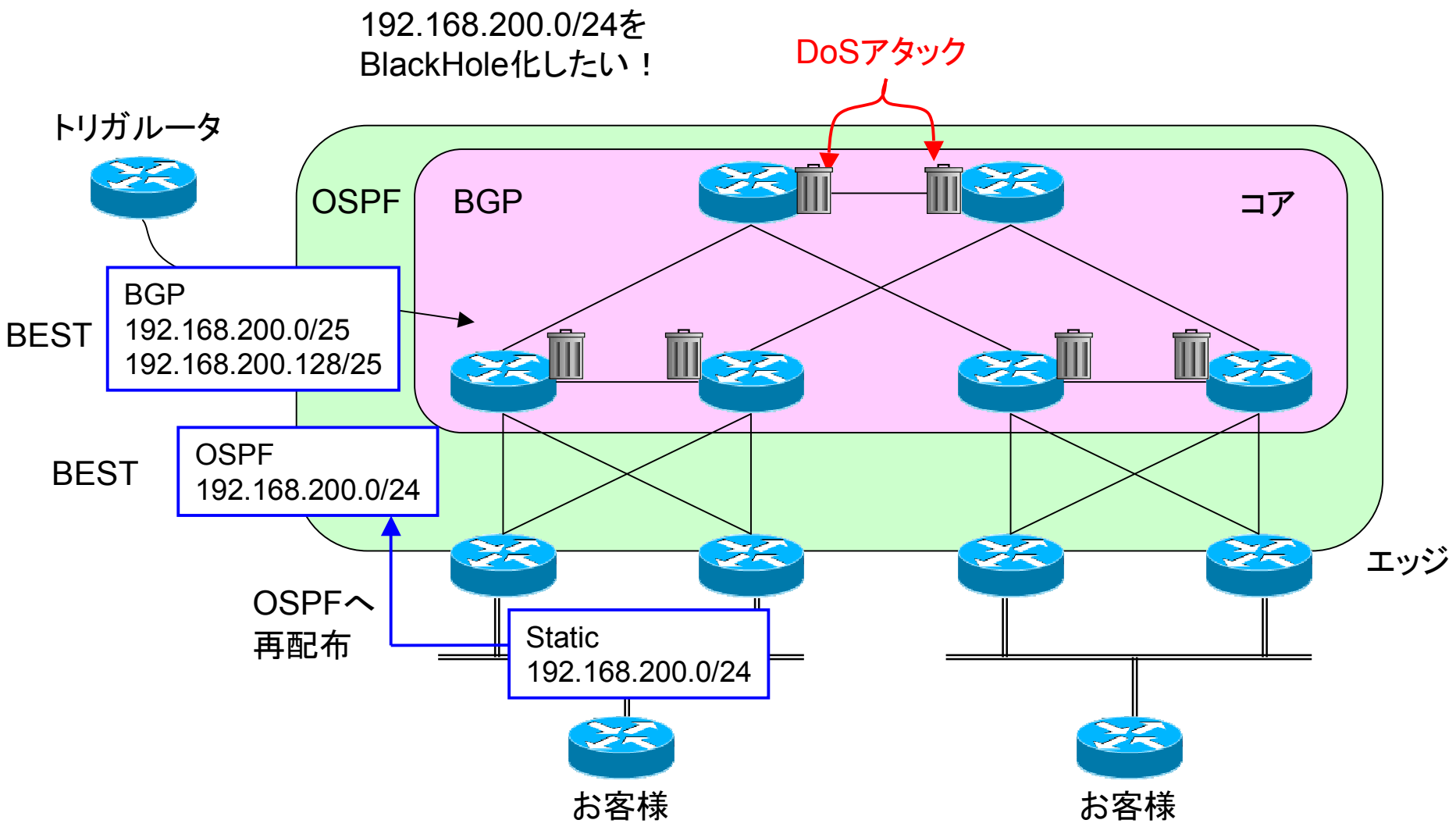
OSPF vs BGP


192.168.200.0/24を
BlackHole化したい！
DoSアタック発生
トリガルータ
OSPF
BGP
コア
BESTに
ならない
BGP
192.168.200.0/24
BEST
OSPF
192.168.200.0/24
エッジ
OSPFへ
再配布
Static
192.168.200.0/24
お客様
お客様

OSPF vs BGP

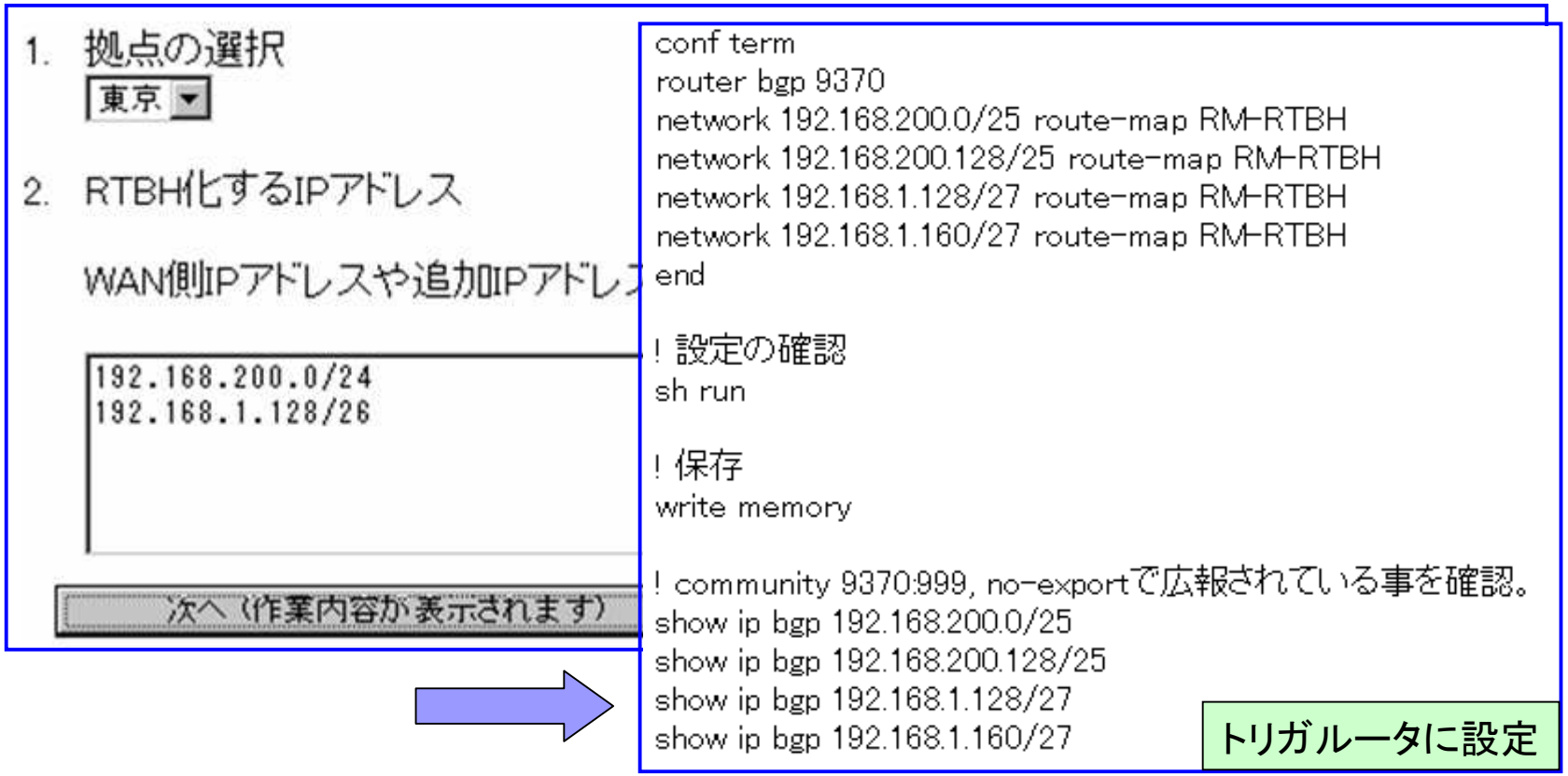
- 通常は、狙われているIPアドレス(/32)単位で落とすので問題はない。
- 問題は、既存ルーティングの単位(/27など)で落としたい場合。
- BGPがOSPFに勝つように、distance値を変更する。
  - インパクトを考えると、すぐには変更できない。
- カスタマ経路をOSPFではなく、BGPに載せる。
  - 構成変更が大変。BGPに対応していないエッジルータもあるし。。
- カスタマ向けルーティングを削除する。
  - コアで落ちる。冗長化している2台のエッジルータで設定が必要。
  - 復旧時のオペレーションに注意が必要。
- 経路を分割して広報する。
  - 手順化すれば、なんとかオペレーションできそう。
  - 今回はこちらで運用

経路分割広報

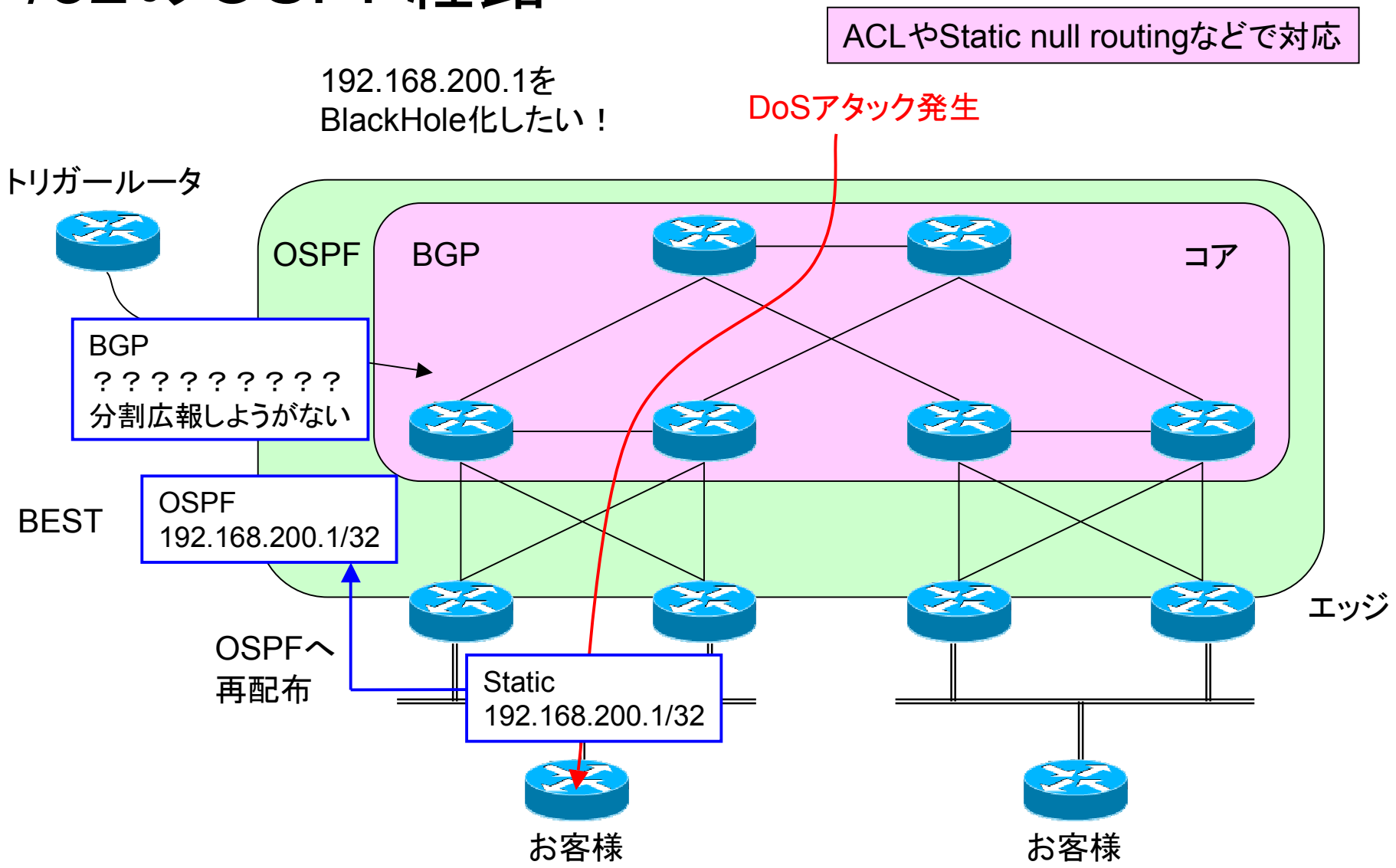

192.168.200.0/24を
BlackHole化したい！
DoSアタック
トリガルータ
OSPF
BGP
コア
BGP
192.168.200.0/25
192.168.200.128/25
BEST
BEST
OSPF
192.168.200.0/24
エッジ
OSPFへ
再配布
Static
192.168.200.0/24
お客様
お客様

config生成フォーム

- Prefixの分割
  - 192.168.1.126/26を2つに分割すると？？？？



/32のOSPF経路


ACLやStatic null routingなどで対応
192.168.200.1を
BlackHole化したい！
DoSアタック発生
トリガールータ
OSPF
BGP
コア
BGP
？？？？？？？？？
分割広報しようがない
BEST
OSPF
192.168.200.1/32
エッジ
OSPFへ
再配布
Static
192.168.200.1/32
お客様
お客様

やっぱりDistance値変更か？

Force10の例

0	Connected interface
1	Static route
20	External Border Gateway Protocol (BGP)
110	OSPF
115	Intermediate System-to-Intermediate System (IS-IS)
120	Routing Information Protocol (RIP)
200	Internal BGP

route-mapで個別に制御できるとうれしいんだけど。。。

```
route-map RM-XXXX perm 10
 match community 9370:xxx
 set distance 50
```

こんな感じ！？実装しているルータありますか？

BGP広報経路のRTBH化

- インターネット向けに広報する集約経路は、RRにて生成
  - Staticにてnull routingの設定
  - BGP networkコマンド
  - StaticはOSPFに再配布
- 使われていないアドレス宛のごみパケットは、RRが破棄

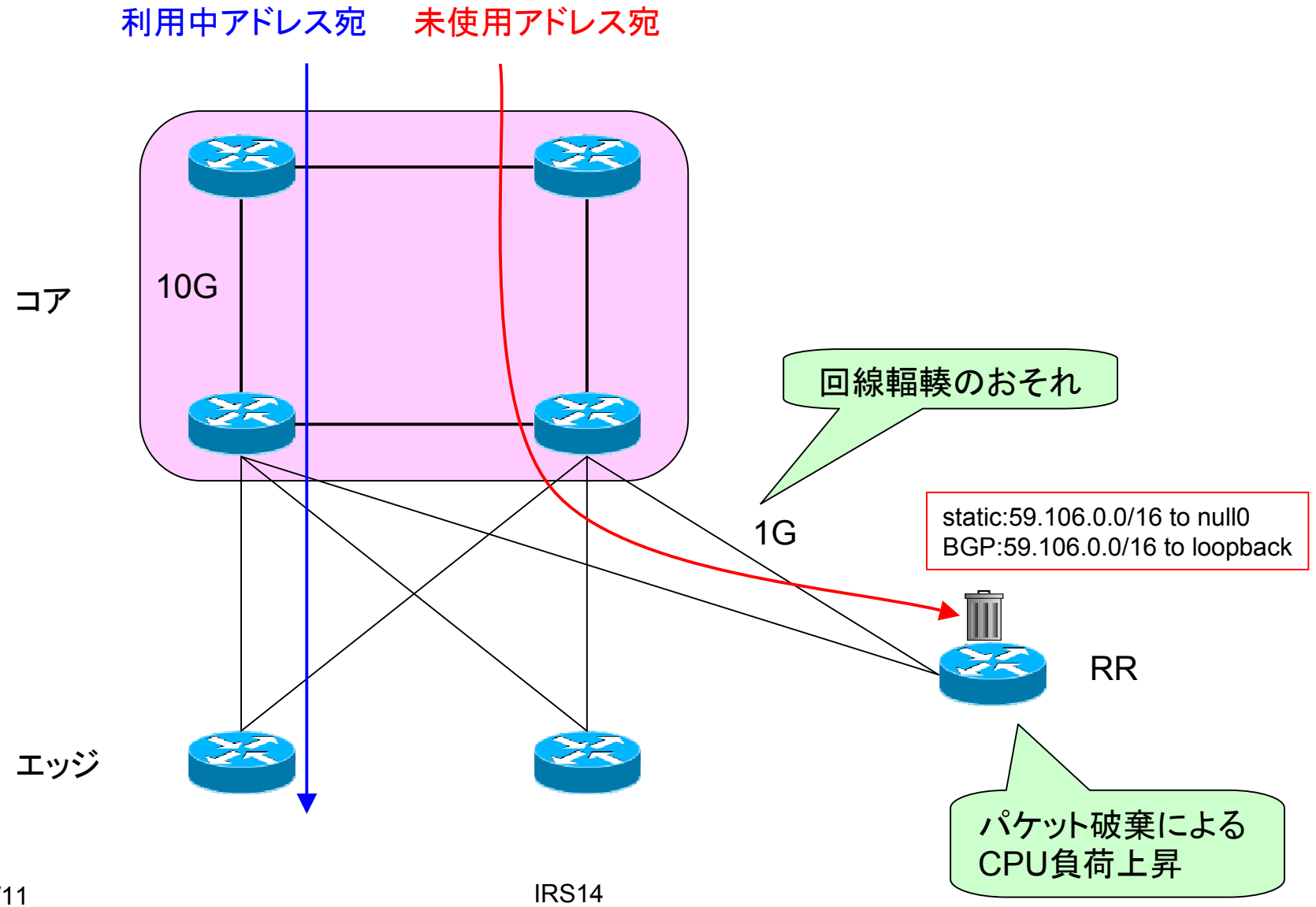
しかし。。。

- RRのリンクは細く(1Gbps)、パケット破棄能力も高くない
- DoSを食らうとCPU負荷上昇→RRが死ぬ→バックボーン全滅

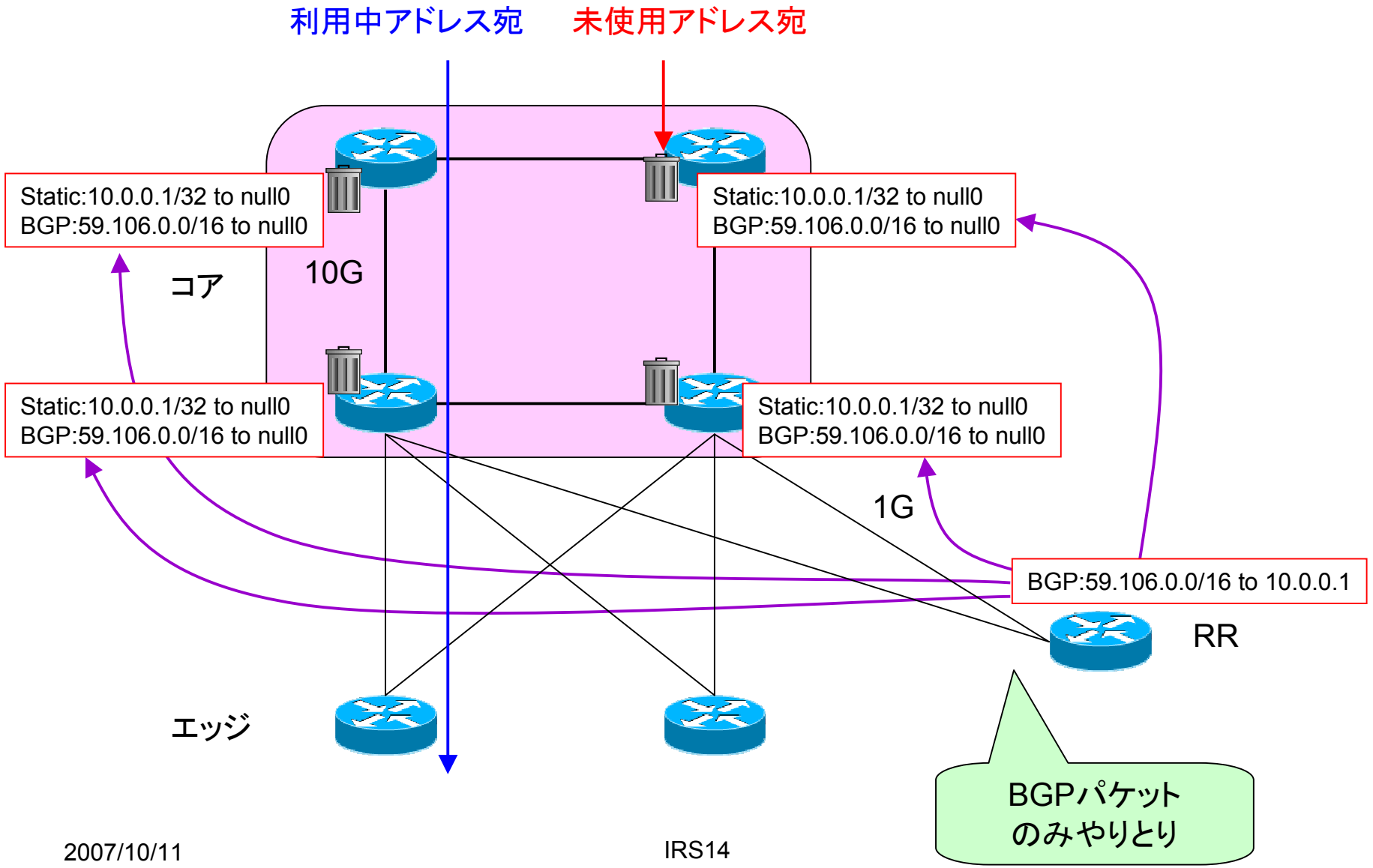
そこで！

- 広報する集約経路もRTBH化すればよさそう！！

従来の構成 – RRで破棄


利用中アドレス宛
未使用アドレス宛
コア
10G
エッジ
回線輻輳のおそれ
1G
static:59.106.0.0/16 to null0
BGP:59.106.0.0/16 to loopback
RR
パケット破棄による
CPU負荷上昇

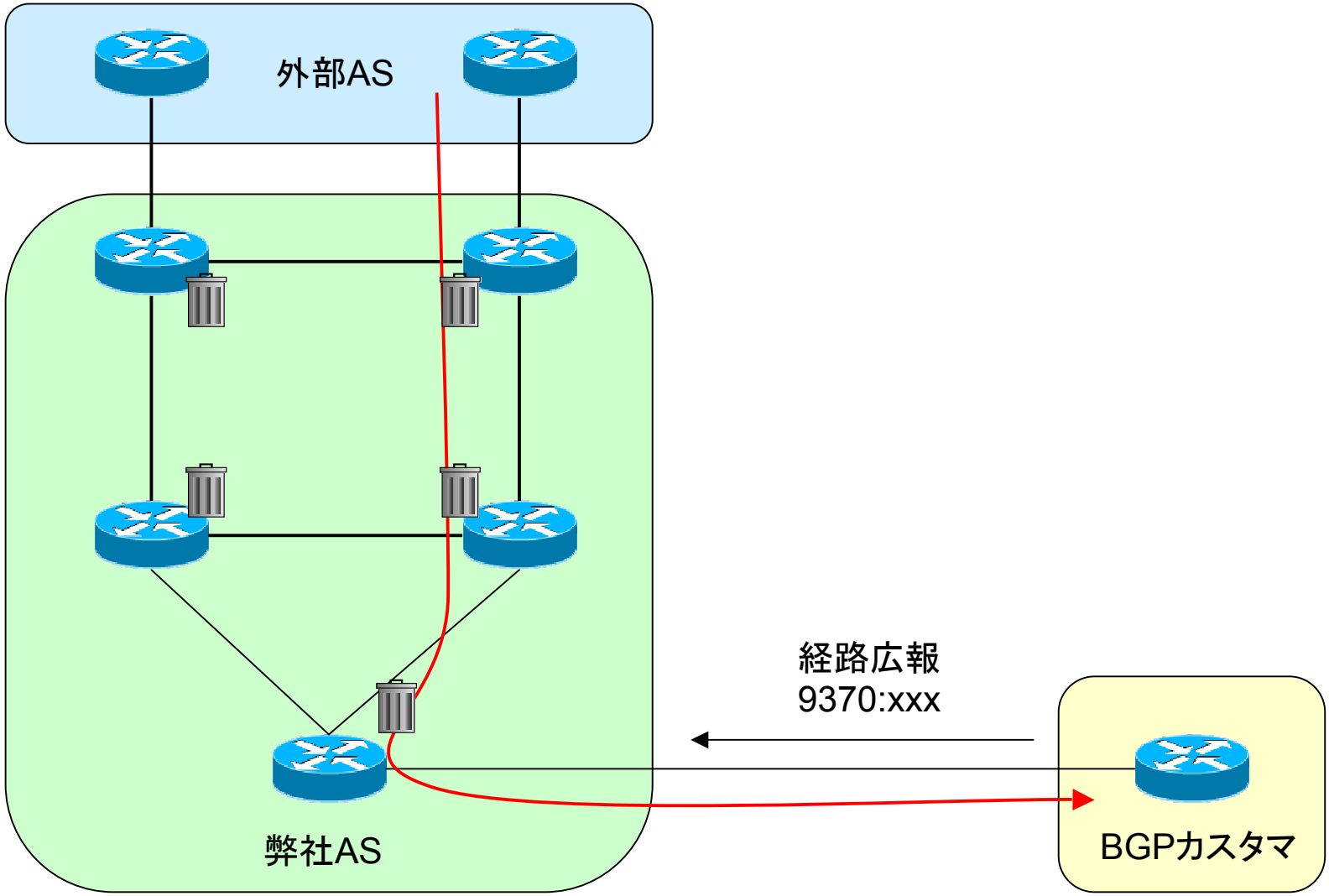
新構成 – RTBH化


利用中アドレス宛
未使用アドレス宛
Static:10.0.0.1/32 to null0
BGP:59.106.0.0/16 to null0
Static:10.0.0.1/32 to null0
BGP:59.106.0.0/16 to null0
コア
10G
Static:10.0.0.1/32 to null0
BGP:59.106.0.0/16 to null0
Static:10.0.0.1/32 to null0
BGP:59.106.0.0/16 to null0
1G
BGP:59.106.0.0/16 to 10.0.0.1
RR
エッジ
BGPパケット
のみやりとり

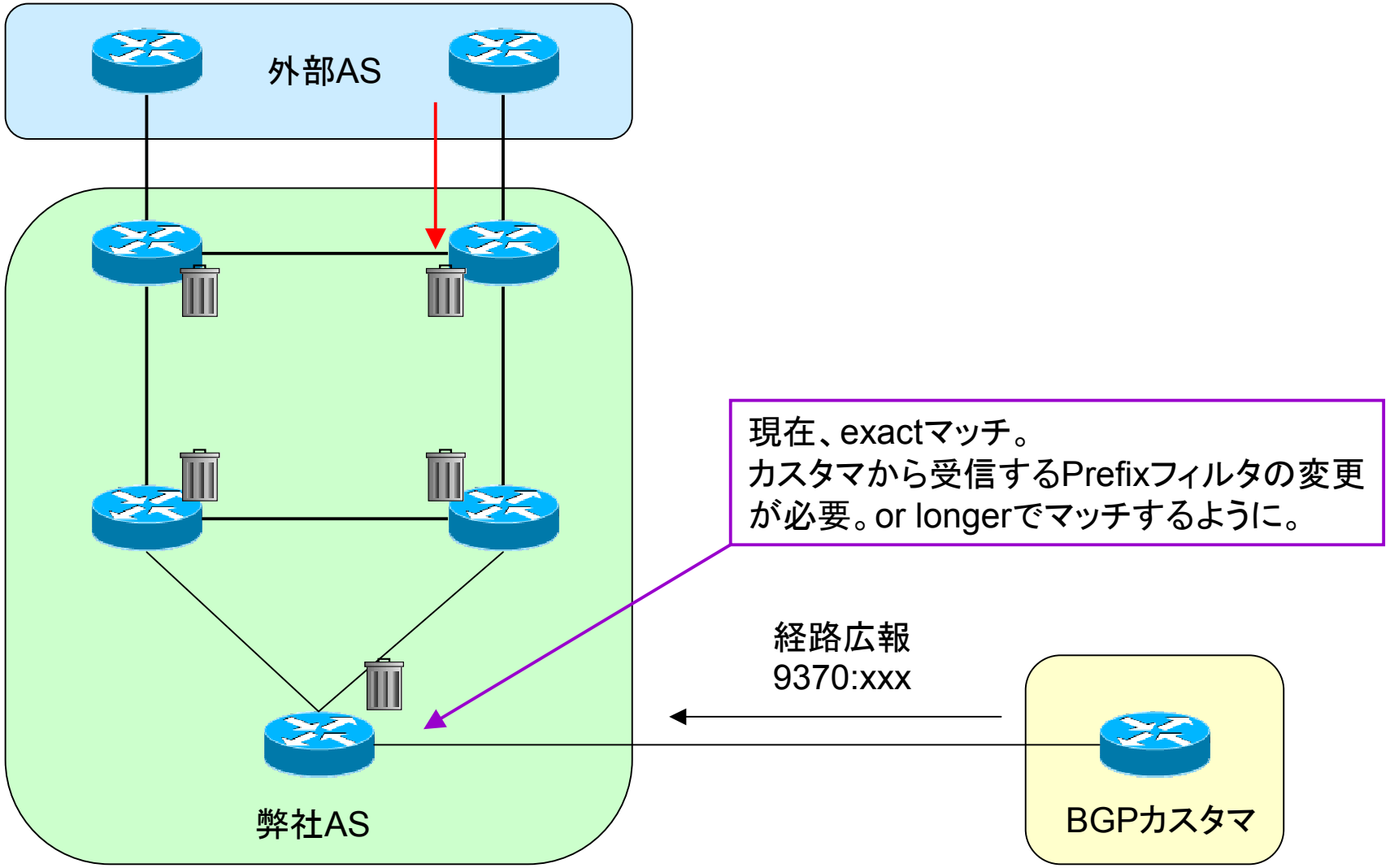
今後考えていること

- BGPカスタマ向け提供
- 東京、大阪、2ASにまたがってRTBHが効くとより良さそう
- さらに、上位ISPにもRTBH経路を広報
  - 上位でトラフィックを止めてくれると良さそう

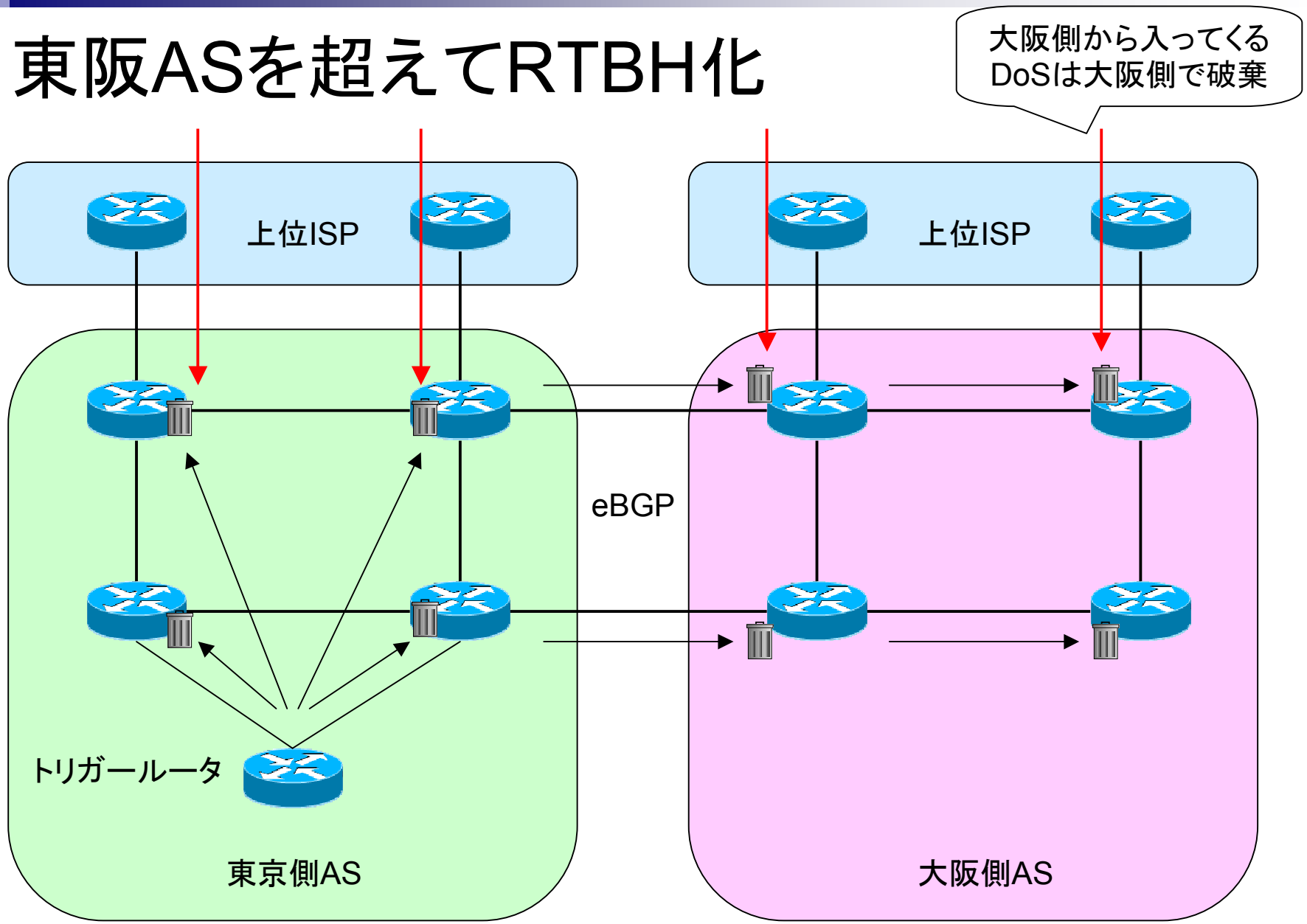
BGPカスタマ向けに提供



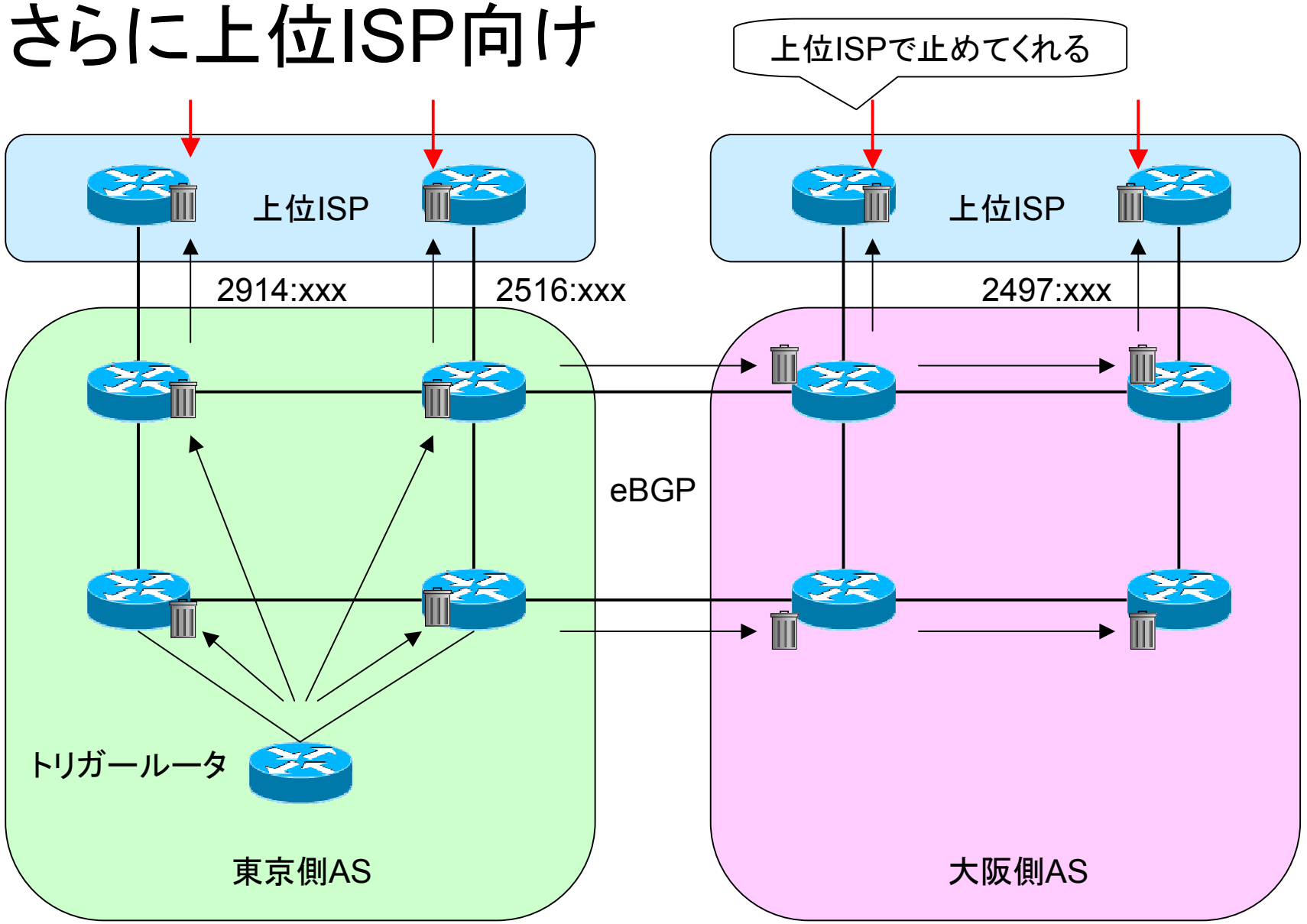
BGPカスタマ向けに提供



東阪ASを超えてRTBH化



さらに上位ISP向け


上位ISPで止めてくれる
上位ISP
上位ISP
2914:xxx
2516:xxx
2497:xxx
eBGP
トリガールータ
東京側AS
大阪側AS

まとめ

- DoSアタックに対するバックボーンの耐性向上。
  - RTBHの仕組みを実装していると、多少安心。
- OSPF経路との兼ね合いは難しい。
- RTBHは万能では無い。
  - DoSアタック対応の１手段
  - ACLなどの他の対応方法も含め、ケースバイケースで対応方法を考える必要がある。