

IXにRTBHフィルタリングを導入してみた ～L2網上で設計と運用の課題～

2023/1/25 JANOG51

インターネットマルチフィード株式会社

宮地 瑠香 / 萩原 昂

この発表について

■ 概要

- JPNAPでのRTBHフィルタリングサービス導入に際して
IXならではの事情の共有や、今後のIXでのRTBH利用に向けた情報共有・議論を行いたい

■ 発表者

- インターネットマルチフィード株式会社 JPNAP ルートサーバ開発担当
 - ◆ 宮地 瑠香 (Ruka MIYACHI)
 - ✓ Email: miyachi@mfeed.ad.jp / Slack (janog-meeting): @r.miyachi
 - ◆ 萩原 昂 (Noboru HAGIWARA)
 - ✓ Email: hagiwara@mfeed.ad.jp / Slack (janog-meeting): @Noboru Hagiwara

自己紹介

- 名前: 宮地 瑠香
- 所属: インターネットマルチフィード株式会社 JPNAP
- JANOGとの関わり
 - JANOG49: 会場NW構築に参加 (初現地参加)
 - JANOG51: 初登壇
- ひとこと
 - 吉田のうどん大好きです (硬い麺が好き)



自己紹介

- 名前: 萩原 昂
- 所属: インターネットマルチフィード株式会社 JPNAP
- 過去の発表
 - JANOG46: ハッカソン Wrap-up
 - JANOG47: IXのルートサーバにおけるRPKIの取り組み
- ひとつこと
 - ようやく初の現地登壇できました



目次

- 背景・RTBHについて
 - RTBHの概要、導入のきっかけ
 - IXのNW構成上の制約・課題
- JPNAPで採用した、RTBHフィルタリングサービスの実現方式と仕様について
 - 実装方式
 - 設計で悩んだこと
- 議論したいポイント

本セッションへのコメントについて

- ぜひ率直な感想・忌憚なきご意見をいただけると嬉しいです
 - 発表終了後のコメントや、匿名での回答用にFormsも用意しました
 - <https://forms.office.com/r/kBsRaTYkqw>

フォーム QRコード

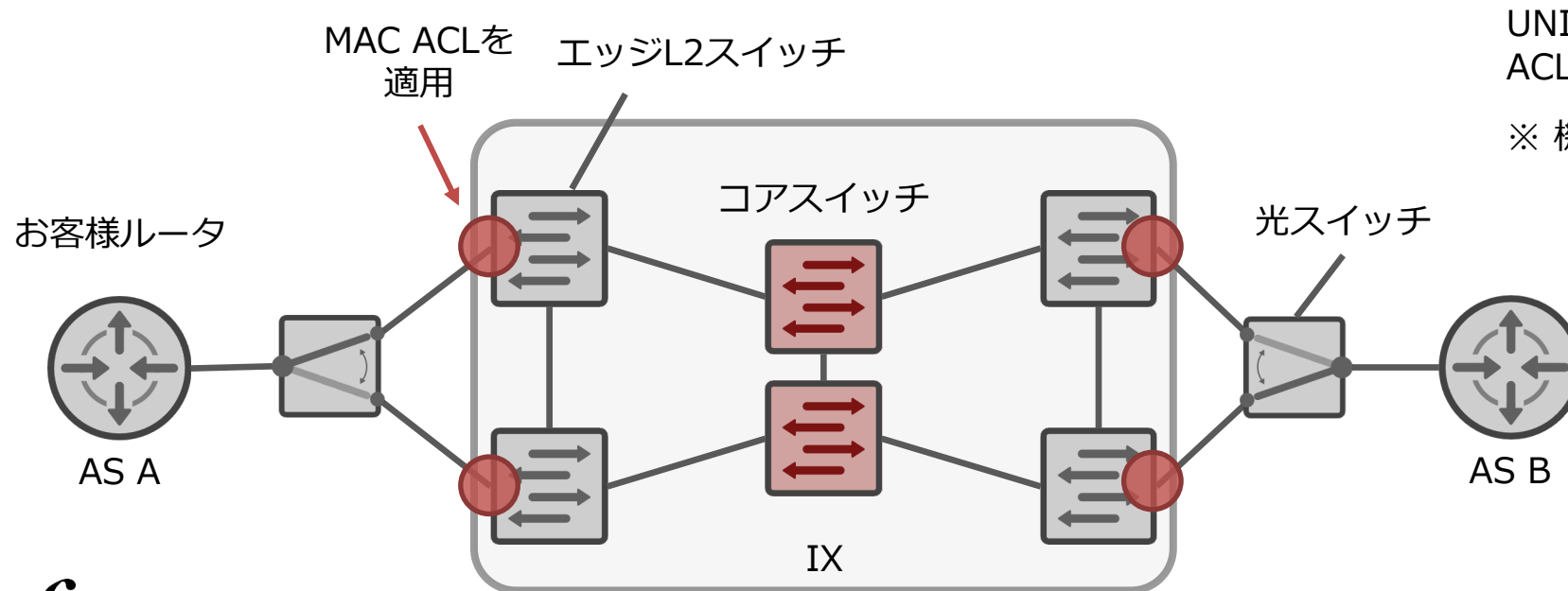


回答期限：2023/3/xx (アーカイブ配信終了の頃まで)
以降のコメントはメールやSlackにてお願いします

背景・RTBHについて

JPNAPのネットワーク構成

- IXはL2接続性のみを提供
 - お客様ルータはエッジL2スイッチに接続
 - コアスイッチを介し、同じIXに接続しているお客様同士の相互接続を実現
- お客様向けポート(UNI)で、MACアドレスでのフィルタリング(MAC ACL)を適用

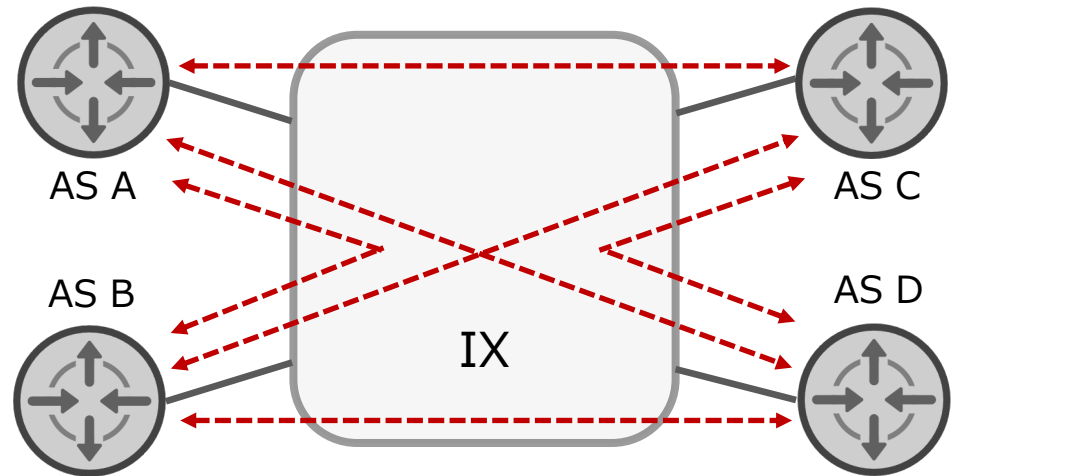


ルートサーバ

■ ルートサーバ (Route Server, RS)

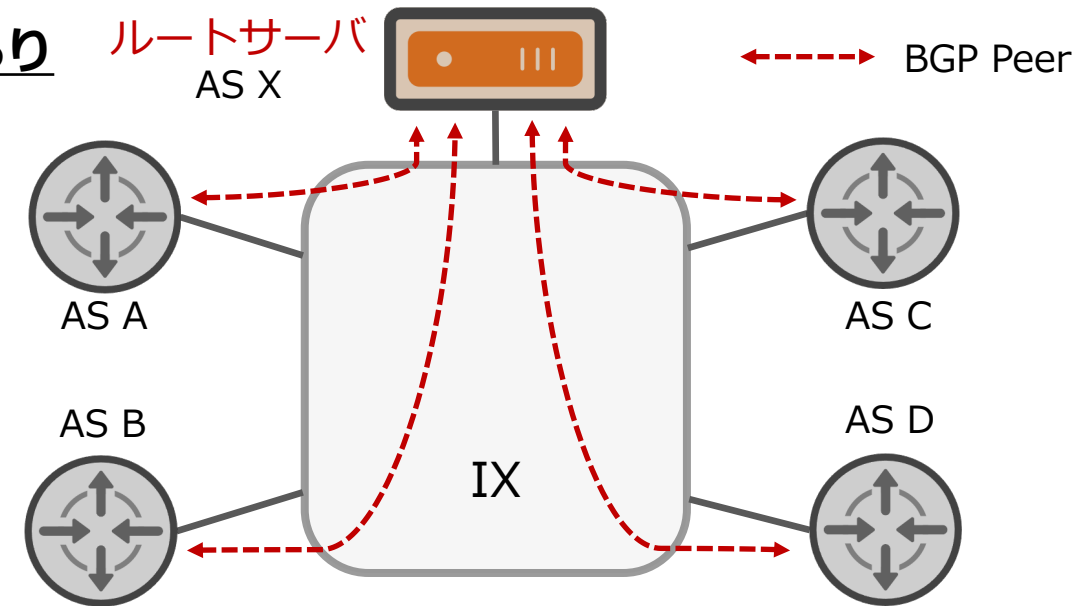
- IX上でのBGPによる経路交換を効率化する
- RSとピアすることで、他の全てのRSピアと自動的に経路を交換できる (マルチラテラル・ピアリング)

RSなし



- トラフィックを交換したいASと直接ピアして経路を交換 (バイラテラル・ピアリング)
- 経路制御の自由度は高い

RSあり



- 実トラフィックはRSを経由しない (= Control Planeのみ提供)
- Path Attribute (AS_PATH, MED等) を透過的に扱う
- 経路制御はRSが提供する機能に依存 (BGP Communityによる制御)

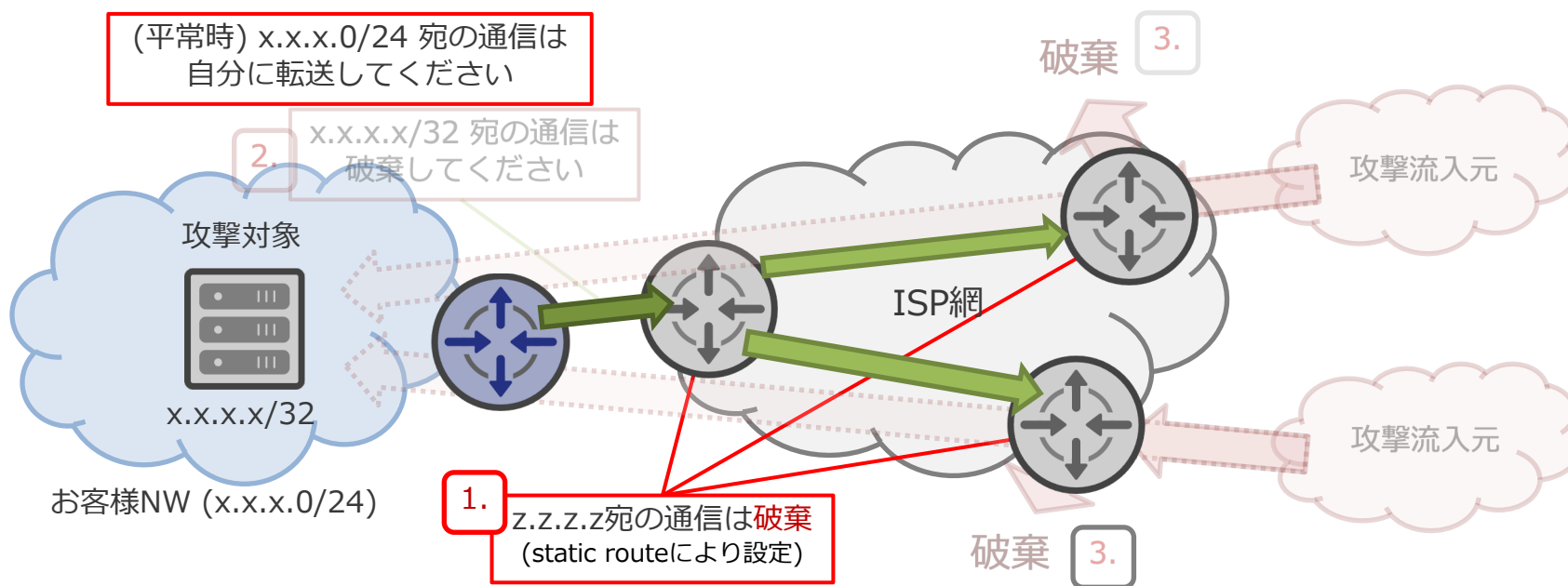
RTBH (Remote Triggered Black Hole) とは

- BGPの経路広告により、遠隔 (Remote) で不要なパケットの破棄 (Black Holing) を行う仕組み
- 主にISPやIXでのDDoS攻撃の対策に使われる

RTBHの仕組み (1/3)

1. ISP網内のルータに破棄用の経路 (null route) を設定しておく
2. 攻撃対象のIP prefixに対して、Blackhole用のBGP communityを付与して広告
3. 該当IP prefix向けの通信を破棄

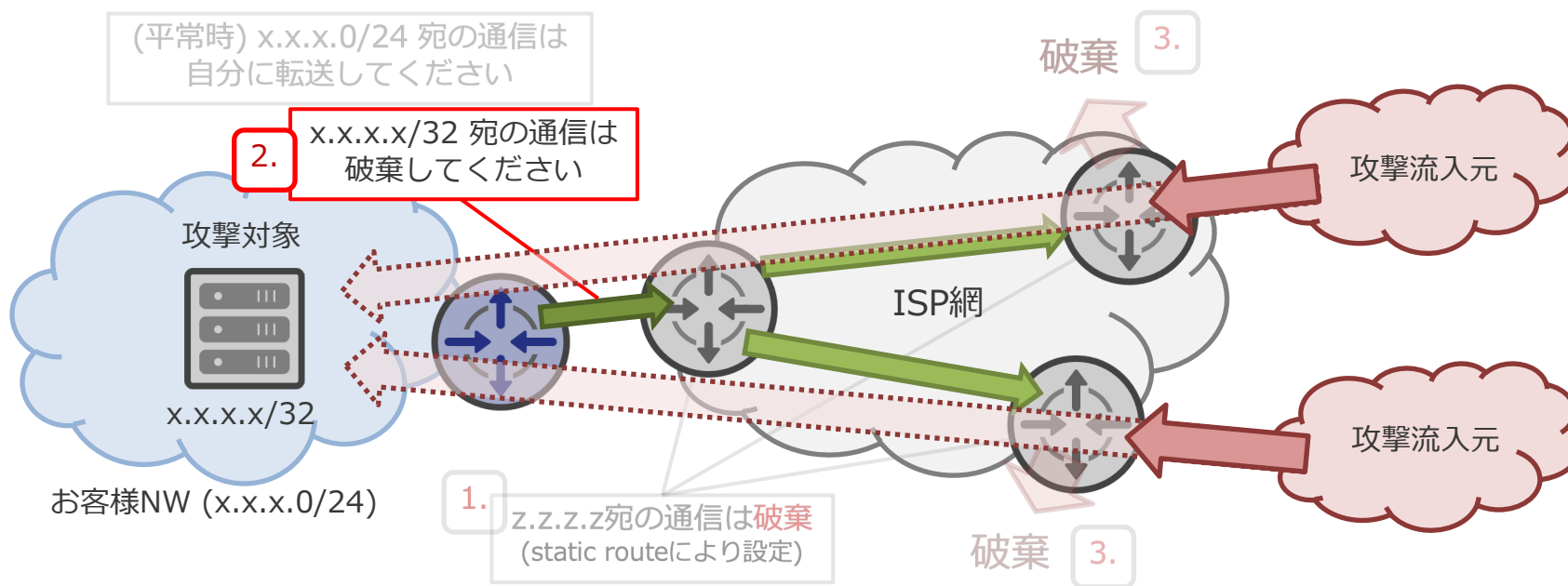
ISPでのRTBH構成例



RTBHの仕組み (2/3)

1. ISP網内のルータに破棄用の経路 (null route) を設定しておく
2. 攻撃対象のIP prefixに対して、Blackhole用のBGP communityを付与して広告
3. 該当IP prefix向けの通信を破棄

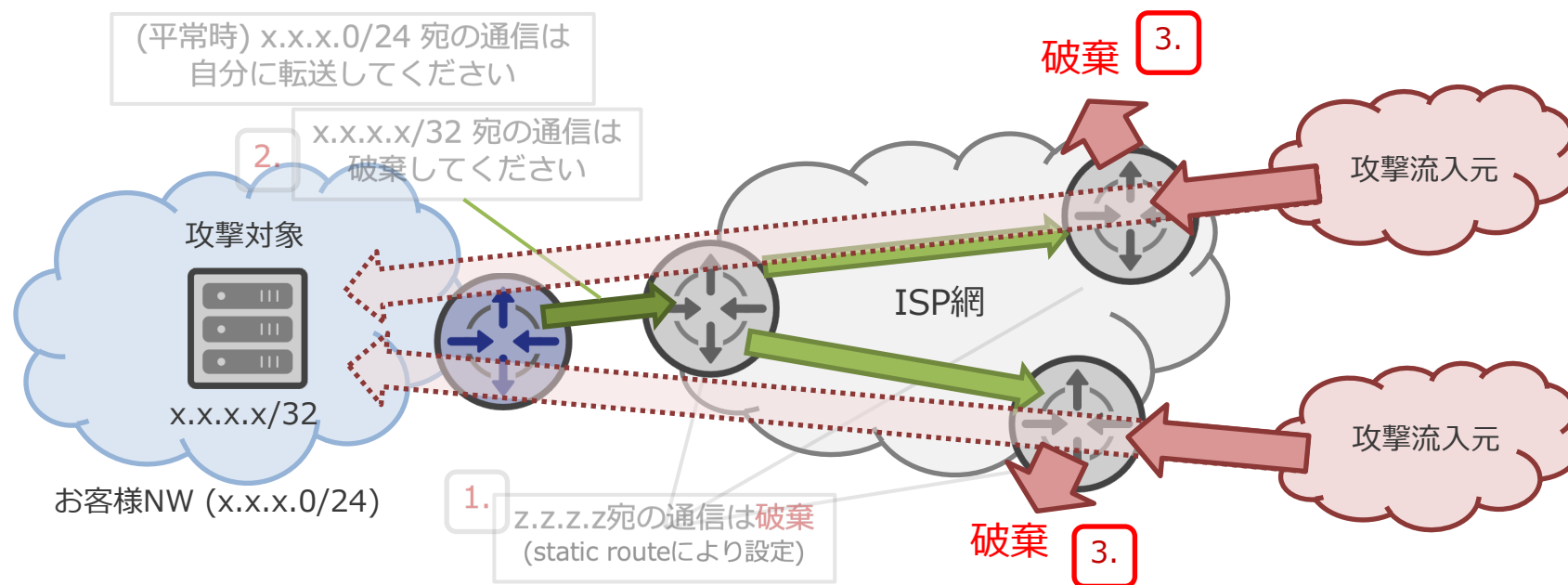
ISPでのRTBH構成例



RTBHの仕組み (3/3)

1. ISP網内のルータに破棄用の経路 (null route) を設定しておく
2. 攻撃対象のIP prefixに対して、Blackhole用のBGP communityを付与して広告
3. 該当IP prefix向けの通信を破棄

ISPでのRTBH構成例



RTBHの特徴

■ 利点

- 通信事業者側との連絡を介さず、お客様側の設定変更のみで適用が可能
 - ◆ 迅速に対処ができる
- 攻撃トラフィックがお客様のネットワークに流入する前に破棄が期待できる
 - ◆ お客様の上流の帯域を圧迫しない

■ 注意点

- 攻撃通信と正常通信の識別はできないため、指定した経路への通信が全て破棄される
- お客様側で攻撃が止まったかどうかの検知ができない

RTBH導入のきっかけ - IXでもセキュリティ対策サービスの需要

■ IX利用者の多様化

- コンテンツ事業者など、直接攻撃対象になりうるお客様も増加
- ここ1-2年でRTBHに対応しているか？という問い合わせも複数件あり
 - ◆ 特に中国系のお客様が気にされている傾向がある

■ JPNAPでの過去1年間の実例

- ロシア系ISPの一時的な輻輳を観測

■ DDoS攻撃からのより確実な防御には、IX上での対処もできることが望ましい

IX上でのRTBH導入課題

一般的なnull0
フィルタが使用できない

IXはあくまでL2サービスであるため、**別の手法で実装が必要**

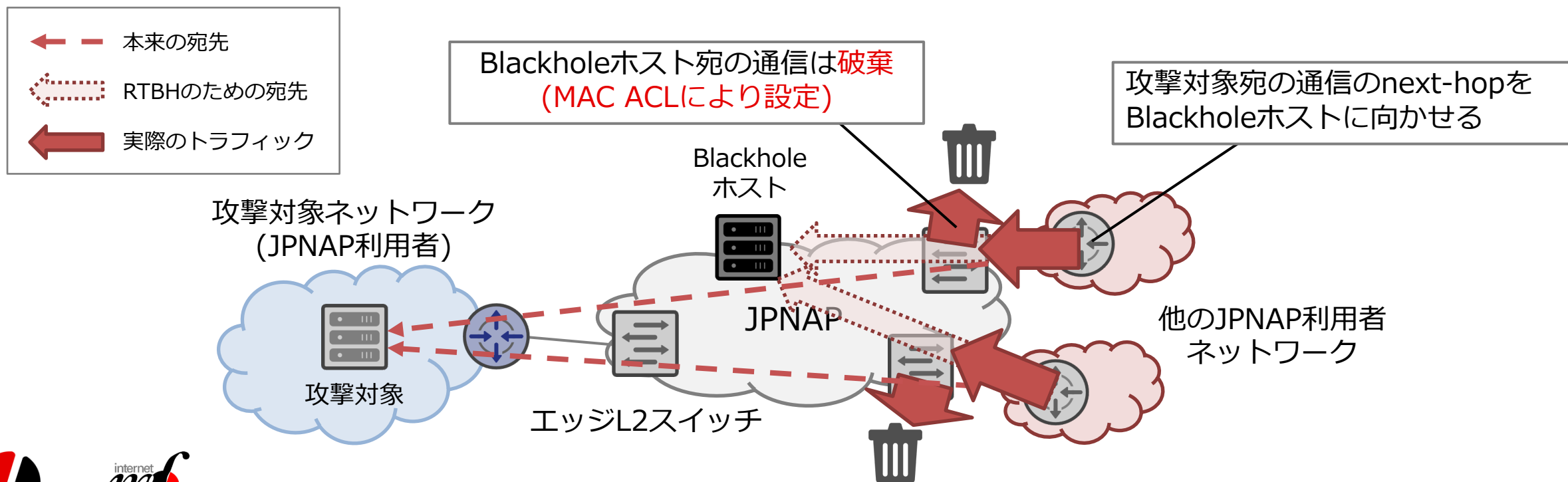
RTBH経路の受け入れ先が
お客様のルータになる

そのホストアドレスの経路を広告させる必要があるが、
一般的には **/32, /128 の経路は受け入れてもらえない**
→ Blackhole community付きの/32 /128の経路は受け入れる
共通認識ができると嬉しい

JPNAPで採用した、RTBHフィルタリングサービスの 実現方式と仕様について

JPNAPでのRTBH実装コンセプト

- お客様向けポートのMAC ACLで、宛先が破棄用ホスト(Blackholeホスト)宛の通信を破棄する設定を入れておく
- お客様ルータ上で、破棄対象通信のnext-hopをBlackholeホストに曲げ、対象通信をMAC ACLにより破棄する



JPNAPでのRTBHの利用パターン

(A) ルートサーバを経由する場合 (こちらがメインの想定)

- i. お客様から、通信を破棄させたい経路に**Blackhole community**を付与して広告
- ii. **ルートサーバ**で、NEXT_HOPをBlackholeホストに書き換えて他のピアに広告
- iii. 他のピアからの対象の通信は、Blackholeホスト宛に送信される
- iv. Blackholeホスト宛の通信を、JPNAP L2スイッチのMAC ACLで破棄

} (B)との差分

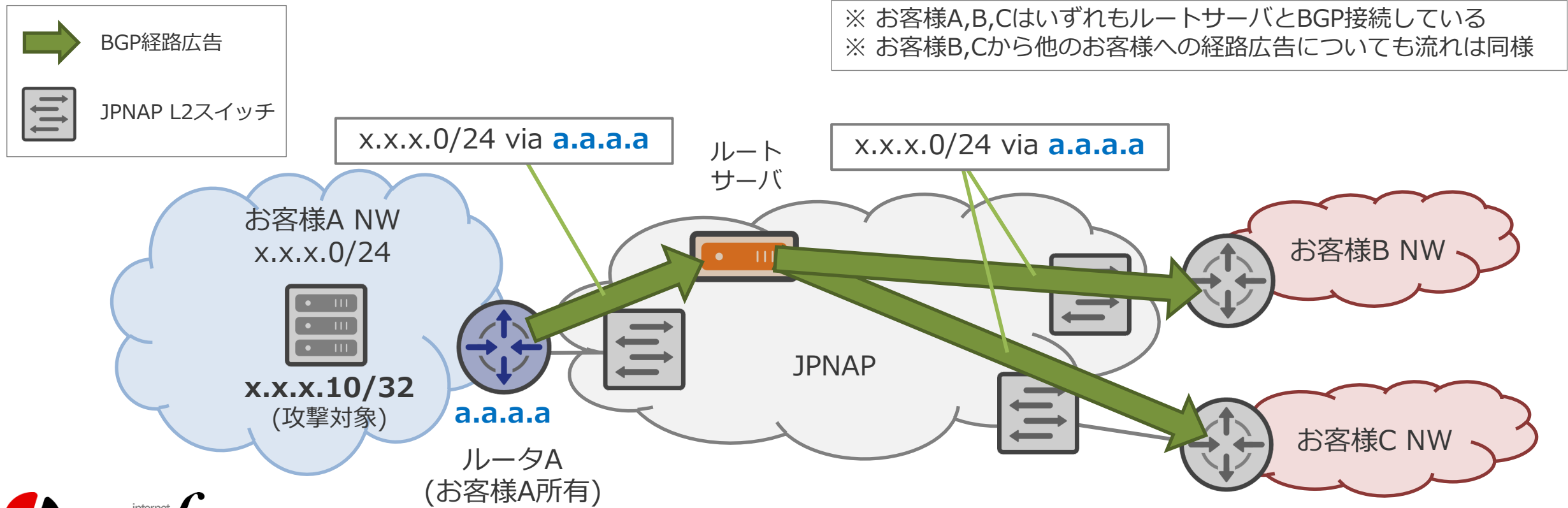
(B) ルートサーバを経由しない場合 (直接ピアリングしている先へのRTBH)

- i. **お客様**から、通信を破棄させたい経路のNEXT_HOPをBlackholeホストにして広告
- ii. 他のピアからの対象の通信は、Blackholeホスト宛に送信される
- iii. Blackholeホスト宛の通信を、JPNAP L2スイッチのMAC ACLで破棄

} (A) ii. と
実質同等

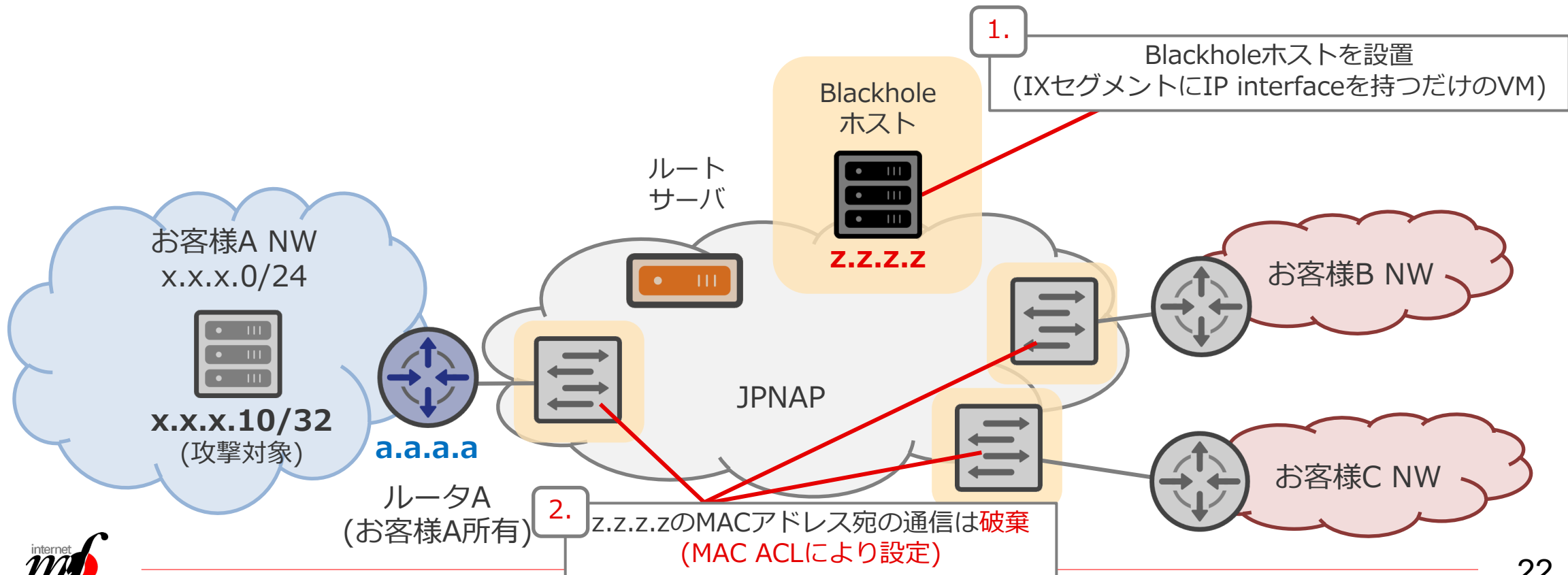
(A) ルートサーバを経由する場合 (前提)

- ルートサーバ経由の平常時の経路広告について
 - お客様Aのルータから、ルートサーバ宛に経路を広告
 - ルートサーバは、他のお客様B,Cのルータにも原則同じ経路を広告



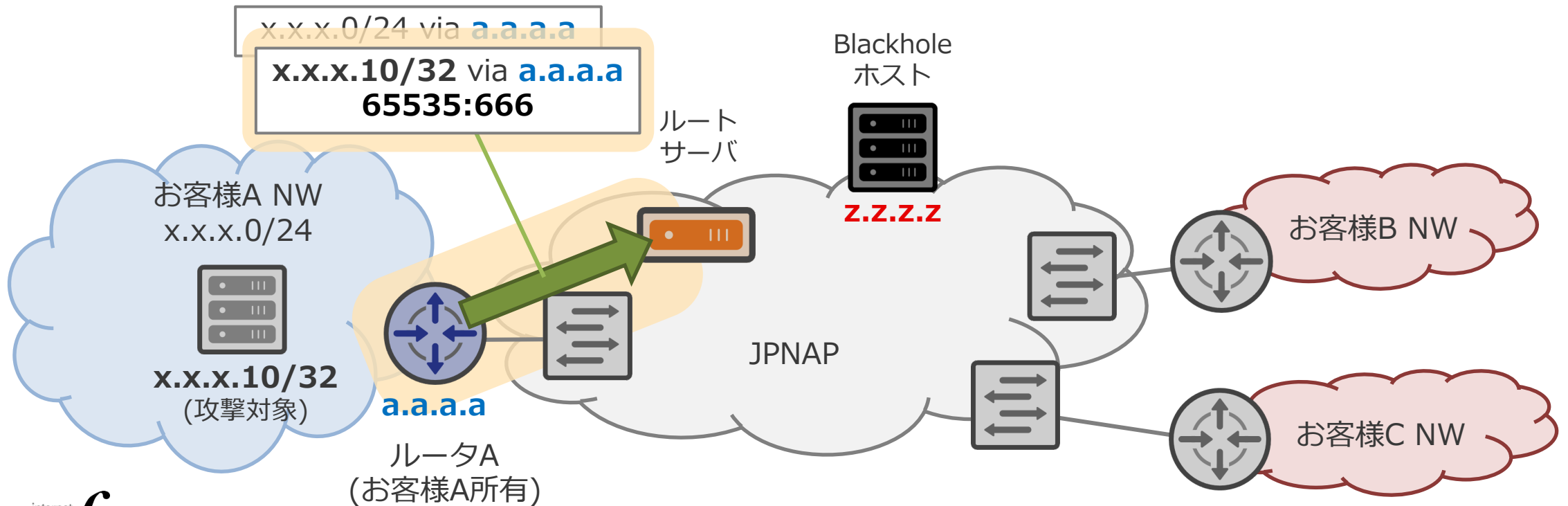
(A) ルートサーバを経由する場合 (1/4)

1. 事前準備として、JPNAP網上に通信破棄先として **Blackholeホスト** を設置
2. JPNAP L2スイッチのお客様ポートの **MACアドレスベースACL (MAC ACL)** に Blackholeホスト宛通信を破棄するルールを設定しておく



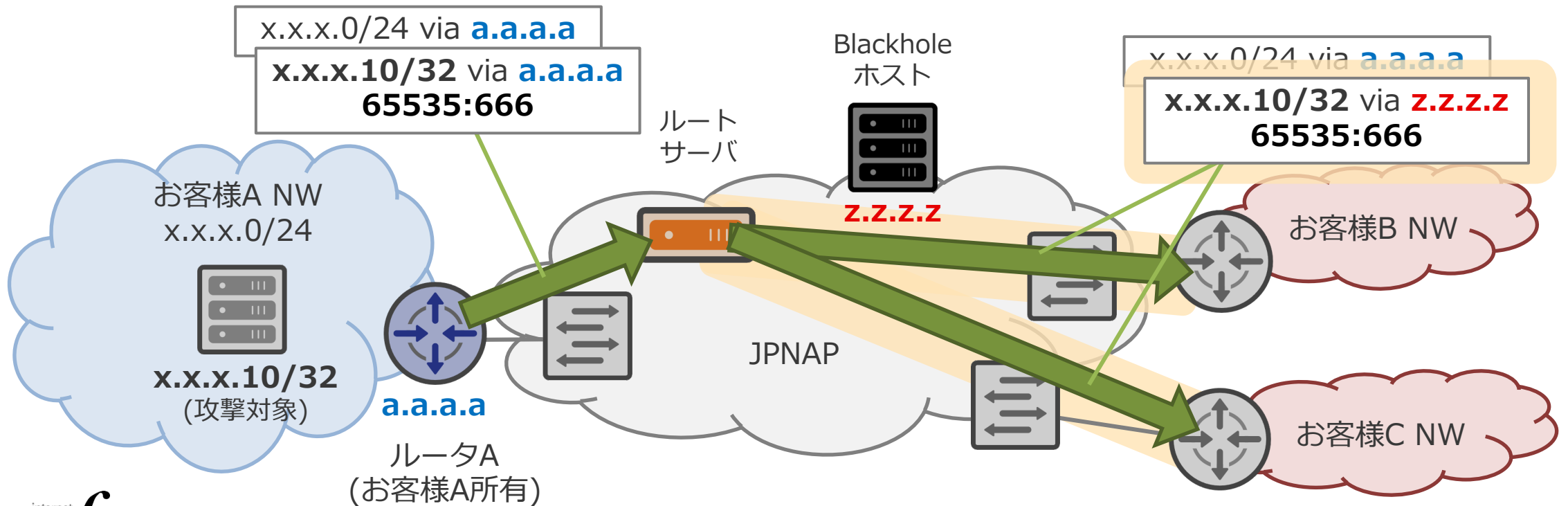
(A) ルートサーバを経由する場合 (2/4)

- お客様側でDDoS攻撃検知時に、受信を止めたい経路 (/32 or /128) に対して、**Blackhole用BGP community** (ここでは **65535:666** とする) を付与して、ルートサーバに経路広告



(A) ルートサーバを経由する場合 (3/4)

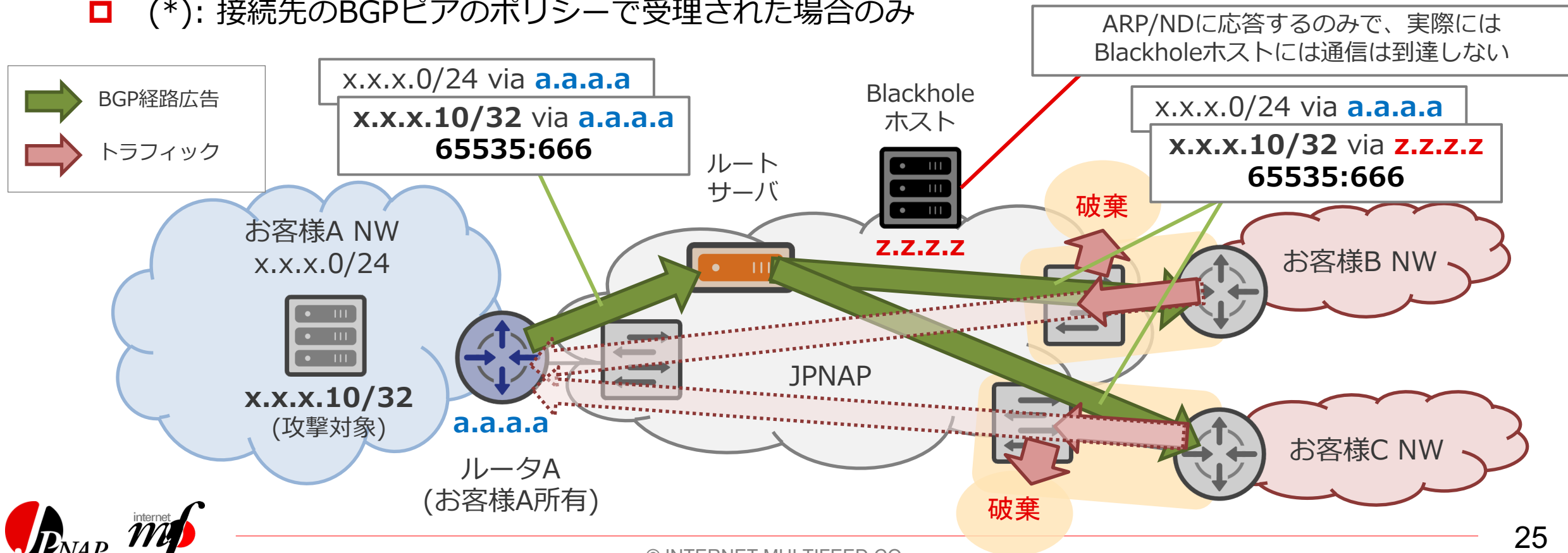
4. ルートサーバで、攻撃対象への通信の宛先 (NEXT_HOP) を Blackholeホストに上書きした経路を他のBGPピアに広報する



(A) ルートサーバを経由する場合 (4/4)

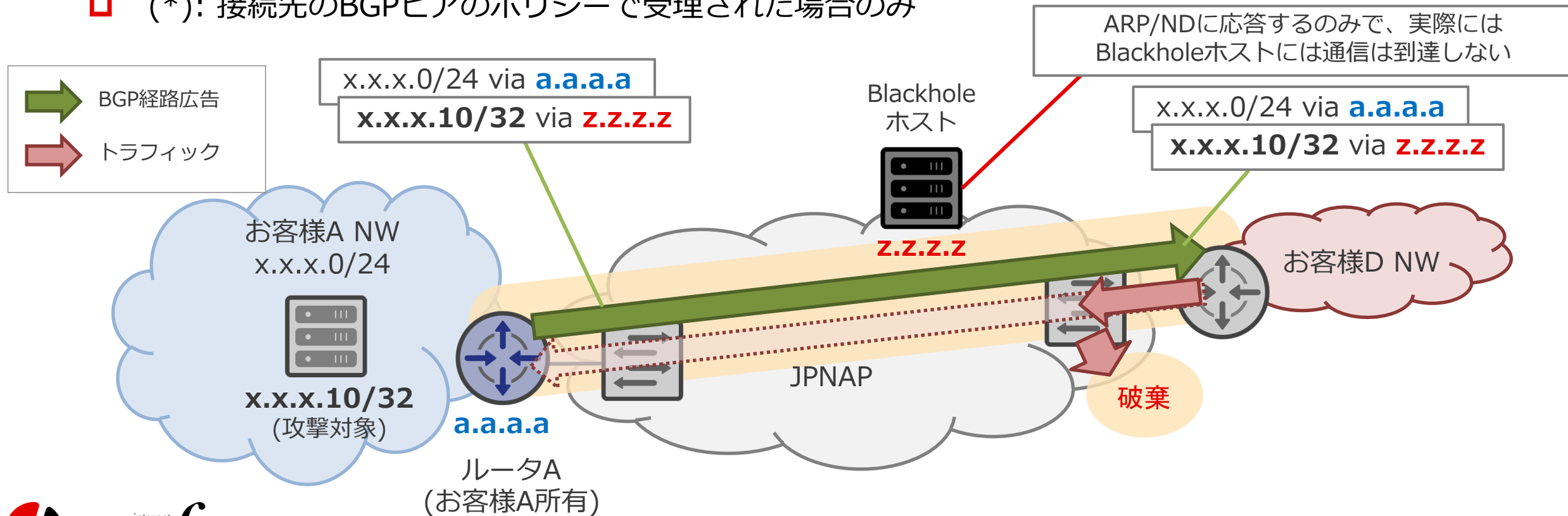
- 5. 平常時の経路の一部がRTBH用経路に上書きされ (longest matchによる)、攻撃対象宛の通信はBlackholeホスト宛として送信される(*) が、
2. のJPNAP L2スイッチ上のMAC ACLにより、破棄される

□ (*): 接続先のBGPピアのポリシーで受理された場合のみ



(B) ルートサーバを経由しない場合

- お客様側でDDoS攻撃検知時に、next-hopをBlackholeホストにした経路をピアに直接広告する
- 攻撃対象宛の通信はBlackholeホスト宛として送信される(*) が、MAC ACLにより破棄される
 - (*): 接続先のBGPピアのポリシーで受理された場合のみ



設計で悩んだこと

- ルートサーバを経由する/しない場合共通
 - トラフィックの破棄方式は？
 - MAC ACLのポリシー設計どうする？

- ルートサーバを経由する場合のみ
 - ルートサーバの経路フィルタ設計どうする？
 - Blackhole community値は？

設計で悩んだこと

- ルートサーバを経由する/しない場合共通
 - トラフィックの破棄方式は？
 - MAC ACLのポリシー設計どうする？

- ルートサーバを経由する場合のみ
 - ルートサーバの経路フィルタ設計どうする？
 - Blackhole community値は？

トラフィックの破棄方式は？ - 破棄を行う場所

■ トラフィックの破棄はどこで行う？

□ [案1] エッジL2スイッチのMAC ACLで破棄

- ◆ 長所：IX網への不要なトラフィック流入を防げる
- ◆ 短所：破棄通信の内容がわからなくなる (flow収集も不可)、一部Neighbor Solicitationも破棄 (後述)

□ [案2] Blackholeホストに集めてから破棄

- ◆ 長所：破棄対象通信の解析や攻撃が止まったかの確認が可能、[案1]に比べ他の通信への懸念が小さい
- ◆ 短所：攻撃流入元ポート～Blackholeホストまでの途中経路で輻輳の恐れ

トラフィックの破棄方式は？ - Blackholeホストの設置方法

■ [案2] Blackholeホストに集めてから破棄 の場合

□ Blackholeホストの設置位置は？

◆ [案2-A] IXセグメント上のどこか1箇所に設置

- ✓ 長所：運用がラク
- ✓ 短所：攻撃流入元ポート～Blackholeホストまでの経路で輻輳の恐れ

◆ [案2-B] 各エッジ (各データセンターごと相当) に設置

- ✓ 長所：Blackholeホストまでの途中経路の輻輳を抑制できる
- ✓ 短所：構成・運用が複雑になる (例えばBlackholeホスト全台が同じMACアドレスを持つ場合…)



IX上での輻輳回避と運用性のバランスから
前頁の [案1] エッジL2スイッチのMAC ACLで破棄 を採用

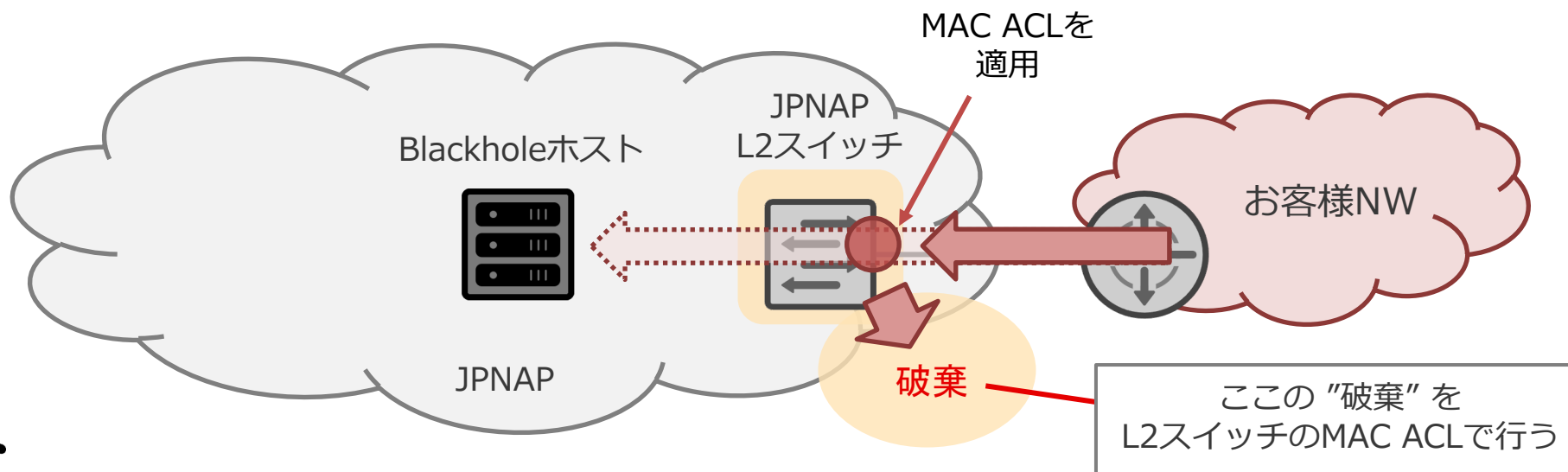
設計で悩んだこと

- ルートサーバを経由する/しない場合共通
 - トラフィックの破棄方式は？
 - MAC ACLのポリシー設計どうする？

- ルートサーバを経由する場合のみ
 - ルートサーバの経路フィルタ設計どうする？
 - Blackhole community値は？

MAC ACLのポリシー設計どうする？ - MAC ACLの採用について

- JPNAPでは、元々お客様向けポートにMAC ACLを適用していた
 - srcが事前設定済みのMACアドレスの通信のみを許可し、意図しない通信がIX上に流れないようにするため
 - → 以前から利用していた機能だったので、導入コストは小さく済んだ
- 不要な通信を極力JPNAP網の入口付近で落とし、網内への流入を防ぐためにも、エッジL2スイッチで実現可能な手法を採りたい
- → MAC ACLでの破棄を採用



MAC ACLのポリシー設計どうする？ - 設計検討

■ Blackholeホスト宛の通信を全てdeny するだけで良い？

□ 下表 #1 行の追加

#	アクション	送信元MACアドレス	宛先MACアドレス	通信タイプ
1	deny	any	Blackholeホスト	any
2	permit	お客様機器	any	any
...	(以降、その他の既存ルールが続く。defaultはdeny)			

追加ルール行

既存ルール行

MAC ACLのポリシー設計どうする？ - 設計検討

■ Blackholeホスト宛の通信を全てdeny するだけで良い？

□ → 通信制御のための通信 (ARPやND) は通した方が良い

◆ これをしないと、IXセグメントでのBUMトラフィックの増加につながるため

ND: Neighbor Discovery

BUM: Broadcast, Unknown unicast, Multicast

#	アクション	送信元MACアドレス	宛先MACアドレス	通信タイプ
1	deny	any	Blackholeホスト	any
2	permit	お客様機器	any	any
...	(以降、その他の既存ルールが続く。defaultはdeny)			

追加ルール行

既存ルール行

MAC ACLのポリシー設計どうする？ - 設計検討 (ARPについて)

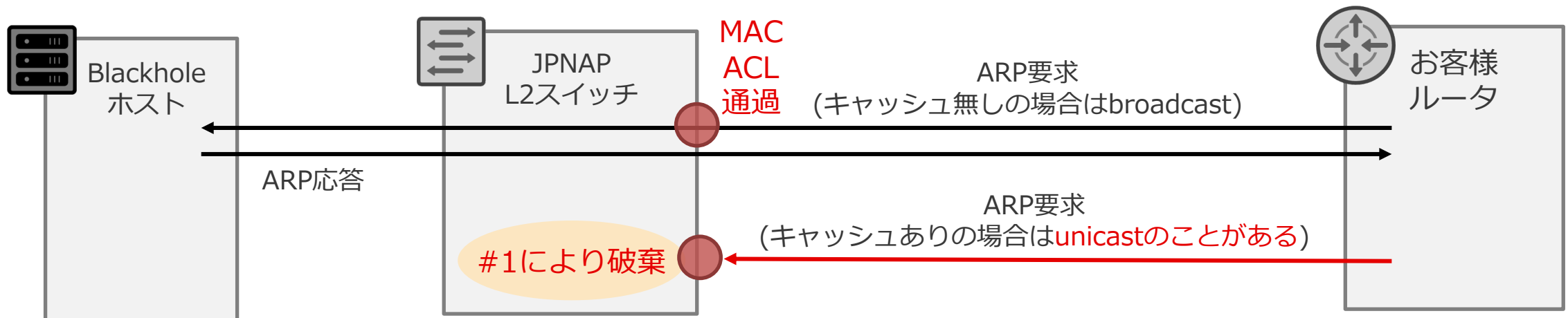
■ お客様ルータ → Blackholeホスト への ARP要求 について

□ お客様ルータが、ARPキャッシュを持っている場合：

- ◆ **機器の設定/実装によっては、unicastのARP要求が送られる** → #1 のルールにマッチしdenyされる
→ 一定時間経過後キャッシュ破棄 → ARPキャッシュ無しの場合が再発生 = **broadcast通信の増加**

#	アクション	送信元MACアドレス	宛先MACアドレス	通信タイプ
1	deny	any	Blackholeホスト	any

追加ルール行



(参考) unicastのARP要求について

■ [RFC826](#)

- “unicast” の表記ではないが、キャッシュの維持を検討する場面において ARP要求は “直接” 送られるとの記載がある

Another alternative is to have a daemon perform the timeouts. After a suitable time, the daemon considers removing an entry. **It first sends** (with a small number of retransmissions if needed) **an address resolution packet with opcode REQUEST directly to the Ethernet address in the table.** If a REPLY is not seen in a short amount of time, the entry is deleted. **The request is sent directly** so as not to bother every station on the Ethernet. Just forgetting entries will likely cause useful information to be forgotten, which must be regained.

MAC ACLのポリシー設計どうする？ - 設計検討 (NDについて)

■ お客様ルータ → Blackholeホスト への Neighbor Solicitation (NS) について

□ お客様ルータが、NDキャッシュを持っている場合：

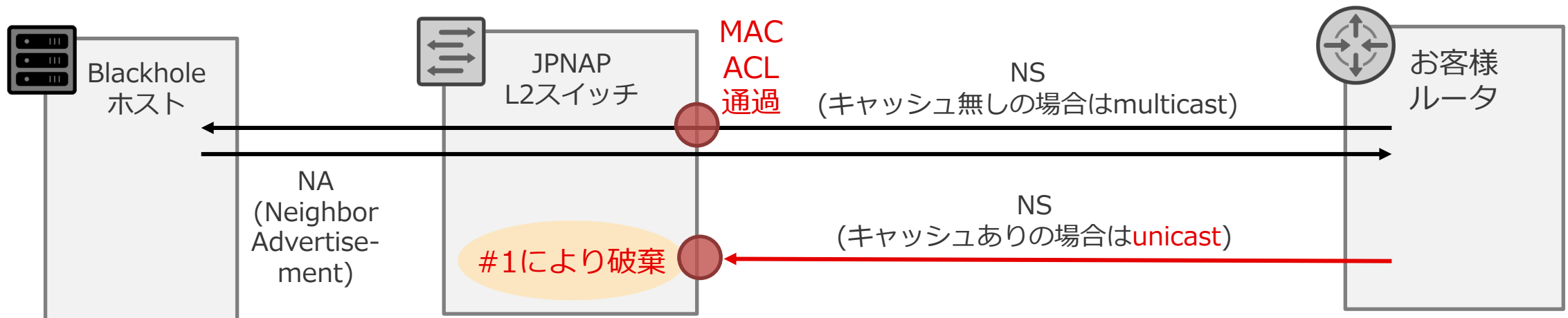
◆ **PROBE状態ではunicastでNSが送られる** ([RFC4861 \(7.3.3\)](#))

→ #1 のルールにマッチしdenyされる → 一定時間経過後キャッシュ破棄

→ NDキャッシュ無しの場合が再発生 = **multicast通信の増加**

#	アクション	送信元MACアドレス	宛先MACアドレス	通信タイプ
1	deny	any	Blackholeホスト	any

} 追加ルール行



(参考) unicastのNeighbor Solicitationについて

■ [RFC4861 \(7.3.3\)](#)

- PROBE状態ではunicastで送られるとの記載がある

Upon entering the PROBE state, a node sends a **unicast Neighbor Solicitation message** to the neighbor using the cached link-layer address. While in the PROBE state, a node retransmits Neighbor Solicitation messages every RetransTimer milliseconds until reachability confirmation is obtained. Probes are retransmitted even if no additional packets are sent to the neighbor. If no response is received after waiting RetransTimer milliseconds after sending the MAX_UNICAST_SOLICIT solicitations, retransmissions cease and the entry SHOULD be deleted. Subsequent traffic to that neighbor will recreate the entry and perform address resolution again.

MAC ACLのポリシー設計どうする？ - 最終的な設計

■ 最終的に採用したMAC ACLポリシー

#	アクション	送信元MACアドレス	宛先MACアドレス	通信タイプ	
1	permit	any	Blackholeホスト	ARP	今回の追加ルール行
2	deny	any	Blackholeホスト	any	
3	permit	お客様機器	any	any	既存ルール行
...	(以降、その他の既存ルールが続く。defaultはdeny)				

■ NDは？

- NDは EtherType: IPv6 であり、NDか否かをL2ヘッダ上では区別できない
- IP ACL(L3)でNDを通すことについては、JPNAPで利用中の装置では、IP ACL(L3)より先にMAC ACL(L2)が適用されるため不可能
- → アドレス解決はリトライで担保されるため、現時点ではmulticast通信の増加を許容する形とした

設計で悩んだこと

- ルートサーバを経由する/しない場合共通
 - トラフィックの破棄方式は？
 - MAC ACLのポリシー設計どうする？
- ルートサーバを経由する場合のみ
 - ルートサーバの経路フィルタ設計どうする？
 - ◆ prefix長が /32, /128 の経路のみの受け入れで良い？
 - ◆ RPKI ROVは無効でも良い？
 - ◆ NEXT_HOPがBlackholeホストの経路にも対応すべき？
 - Blackhole community値は？

経路フィルタ設計どうする？ - prefix長 /32, /128 のみの受け入れで良い？

■ インターネットで流通する経路のprefix長は、一般的に

□ **IPv4: 最長 /24 まで、IPv6: 最長 /48 まで** (ref. RFC7454)

■ RTBH/Blackholing用の経路について

□ RFC7999 や RFC5635 に「可能な限り具体的な /32 または /128 であるべき」の旨の記載あり

◆ 他IX/ISPは、/32, /128 のみacceptする場合・短い経路もacceptする場合の双方あった


How does the Blackholing service work?

→ **Default case – Blackholing is not used**

- Customers advertise their IP prefix(es) with the next-hop IP of their advertising router. DE-CIX Route Servers accept the following prefix lengths:
 - IPv4: /8 ≤ prefix length ≤ /24
 - IPv6: /19 ≤ prefix length ≤ /48

→ **Blackholing case: To protect against a massive DDoS attack**

- Customers advertise their IP prefix(es) tagged with the BGP BLACKHOLE Community (65535:666). Accepted prefix lengths are:
 - IPv4: /8 ≤ prefix length ≤ /32 (if and only if BLACKHOLE is set)
 - IPv6: /19 ≤ prefix length ≤ /128 (if and only if BLACKHOLE is set)
- Prefix validation (RIR filtering) is applied as usual, to prevent unauthorized Blackholing

 **DE CIX**
Where networks meet www.de-cix.net

Accepted prefixes

	IPv4	IPv6
Standard	8 < x < 24	19 < x < 48
Blackholing	8 < x < 32	19 < x < 128

The BGP community supported by HKIX MLPA route servers

1	4635:666	Trigger participant routers to discard (null) route for a specific address. HKIX route servers will ONLY accept /32s with BGP community tagged for RTBH filtering and forward the network prefixes to participant routers.
---	----------	---

DE-CIX: <https://www.de-cix.net/Resources/Persistent/4/d/5/f/4d5f5d57cb3a466d34ea4d640961353f309ca6b3/DE-CIX%20Blackholing%20service.pdf>
France-IX: <https://www.franceix.net/en/english-services/infrastructure-en/blackholing-english>
HKIX: <https://www.hkix.net/hkix/anti-ddos.htm>

経路フィルタ設計どうする？ - prefix長 /32, /128 のみの受け入れで良い？

- JPNAPのルートサーバでは、RTBH用の経路について以下のprefix長のみacceptすることとした
 - **IPv4: /32、IPv6: /128**
 - ◆ お客様側で事前登録(IRR等)された経路のprefix範囲内に限る
- RFCの推奨に従った形だが、利便性を考えると短い経路も許容する方が良い？
 - 複数IPに対してRTBHを利用したいケースがどのくらいあるか？
 - IX事業者視点だけでは、コンテンツサービスの運用事情がわかりきらない部分も…

経路フィルタ設計どうする？ - RPKI ROVは無効でも良い？

- JPNAPのルートサーバではRPKI ROVを基本的に有効にしているが、Blackhole communityが付与されている経路のみ、ROVを無効にした

ROV: Route Origin Validation
RPKIで行う経路検証のこと

- 基本的にどの経路に対してもRPKI ROVを有効にしたいが...

ROA: Route Origin Authorization
RPKIでの経路情報
(AS番号、IP prefixとその最大長)

- /32, /128のみ受け入れるポリシーにしたため、ROAのmax lengthに引っかかりInvalidになるのが目に見えている
- ROAのmax lengthを32, 128にするのは無理がある
 - ◆ RFCでもmax lengthは小さく設定するのが推奨
- Euro-IXのコミュニティでも過去に議論があったが、有効/無効にすべきと双方の意見もあり

経路フィルタ設計どうする？ - NEXT_HOPがBlackholeホストの経路にも対応すべき？

- 現状NEXT_HOP = peer IPの経路のみしかacceptしない仕様になっている
- ルートサーバ経由でないBGPピアとも合わせて設定を変えられるように、NEXT_HOPが変更された経路を受け入れてほしいという声も
 - Blackhole communityが付与された経路に限り、NEXT_HOPがBlackholeホストに変更された経路を受け入れるポリシーに変更していきたいと考えている

設計で悩んだこと

- ルートサーバを経由する/しない場合共通
 - トラフィックの破棄方式は？
 - MAC ACLのポリシー設計どうする？

- ルートサーバを経由する場合のみ
 - ルートサーバの経路フィルタ設計どうする？
 - Blackhole community値は？

Blackhole community値は？

- IANAのBGP Well-known Communities(*)として **65535:666** が定義されている
 - RFC7999でも言及あり
- **<自AS番号>:666** の採用もある
- 各IX/ISPの例：

IX/ISP	Blackhole community	source
France-IX	65535:666	https://www.franceix.net/en/english-services/infrastructure-en/blackholing-english
DE-CIX	65535:666	https://www.de-cix.net/en/resources/service-information/blackholing-guide
Equinix IX	65535:666	https://docs.equinix.com/ja/Content/Interconnection/IX/IX-rtbh-host-info.htm
HKIX	4635:666	https://www.hkix.net/hkix/anti-ddos.htm
GIN	2914:666 (Selective RTBHあり)	https://www.gin.ntt.net/support-center/policies-procedures/routing/
Arelion	65535:666, 1299:666 (Selective RTBHあり)	https://www.arelion.com/our-network/bgp-routing/bgp-communities

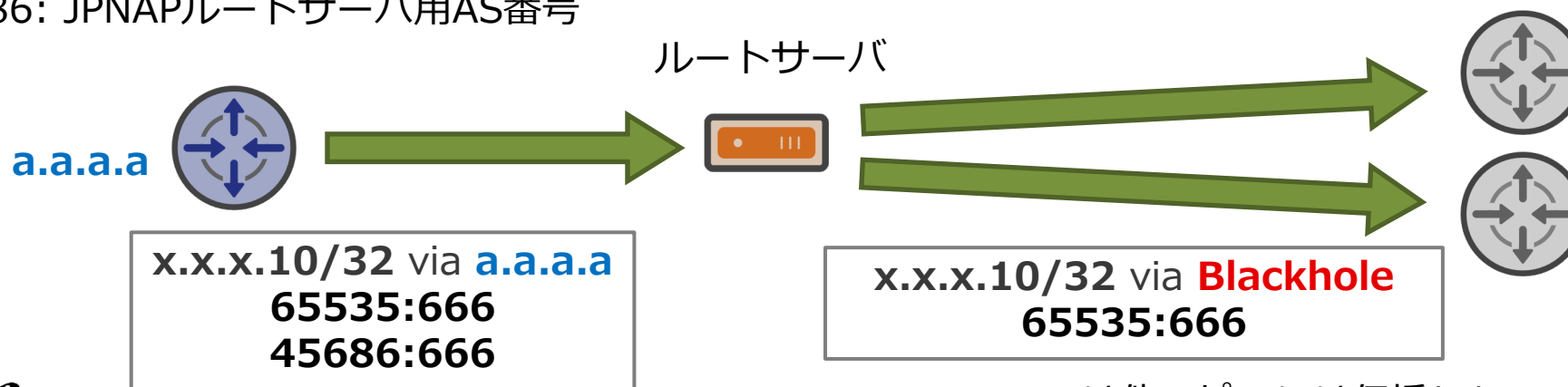
(*) IANA - Border Gateway Protocol (BGP) Well-known Communities: <https://www.iana.org/assignments/bgp-well-known-communities/bgp-well-known-communities.xhtml>

Blackhole community値は？

- 最終的に両パターンの2つを定義 (併用可)
 - お客様側での目的に応じた使い分けを可能にするため

Blackhole community	ルートサーバでの処理の違い	意図
65535:666	RSからexport時にcommunityをstripしない	一般的に広く使われている値を受け入れるため定義
45686:666	RSからexport時にcommunityをstripする	JPNAP上でのRTBHの利用であるということが明示的にわかるように、自AS番号の値も定義

※ 45686: JPNAPルートサーバ用AS番号



45686:666 は他のピアには伝播しない

(参考) 開発体制・導入までのスケジュール

■ 開発体制

- JPNAP ルートサーバ担当 3名 → 2名 (途中で人事異動)
 - ◆ NW機器側の設計検討・相談や、メンテナンスは他のメンバーも含む

■ スケジュール

~2022/3	設計検討・情報収集
2022/4~9	サービス仕様検討 詳細設計・動作検証・試験 (ルートサーバ、L2スイッチ等) Blackholeホスト構築
2022/9	L2スイッチメンテナンス ルートサーバメンテナンス
2022/9/28	サービス提供開始

まとめ

■ JPNAPでRTBHを導入した

- 攻撃流入元ルータ上でnext-hopをBlackholeホストに向け、MAC ACLで通信破棄
- IXのRTBHについては手探りで実装した部分も多い
 - ◆ 仕様変更の余地もまだあるので、IXコミュニティ全体でより良い方向に持っていけたら幸いです
 - ✓ ご意見・議論へのご参加お待ちしております

■ 引き続き検討すべき事項も残る

- IX接続では /32, /128 のBlackhole community付きの経路は受け入れるという文化の形成・共通認識ができると嬉しい
- IXのRTBH、IXのセキュリティサービスは、どうあるべき？

議論したいポイント

議論したいポイント

- それぞれの視点から、率直な感想・忌憚なきご意見をお聞きしたい

- 回答フォームからもぜひ (<https://forms.office.com/r/kBsRaTYkqw>)

回答期限:2023/3/xx (アーカイブ配信終了の頃まで)
以降のコメントはメールやSlackにてお願いします

フォーム QRコード



- 利用者視点

- ◆ 利用に際しての懸念や、もっとこうなっていて欲しいという要望など
- ◆ ルートサーバに求める仕様は？

- サービス提供者視点

- ◆ この仕組みがより効果的に働く環境をどう作っていくか
 - ✓ お客様に地道に /32, /128 のRTBH用経路の受け入れを依頼？

- その他

議論したいポイント詳細 (1/3)

■ 本方式でのRTBHについて、利用者視点での率直な感触をお伺いしたい

- /32, /128 の受け入れはやはり抵抗がある？
 - ◆ 所定のBGP communityが付いているなど、目印があればまだ受け入れやすい？
- RTBHの利用に際し、ルートサーバに求める仕様は？
 - ◆ RTBHの経路に対してはRPKI ROVを実施しないことへの懸念等
 - ✓ IRRベースの経路フィルターのprefixに含まれる場合のみRTBH経路としてacceptする
 - ◆ NEXT_HOPがBlackholeホストの経路もRTBH用経路としてacceptされたほうが良い？
 - ✓ BGP設定ポリシーやconfig設計上の都合などあれば
 - ◆ 65535:666 は他でも使う？ 見分けがついたほうが良い or 同じ値が良い？

議論したいポイント詳細 (2/3)

- 本方式でのRTBHについて、利用者視点での率直な感触をお伺いしたい (続き)
 - MAC ACLでのBlackhole宛通信の全破棄はやりすぎ？
 - ◆ 一部のNeighbor Solicitationが落ちる他にも、通信影響の懸念はある？
 - RTBH経路を広告するときの想定運用について
 - ◆ いざRTBHを利用したい時に、Blackhole communityを付与して経路広報するハードルは高い？
 - ✓ ポータルサイト上のGUI操作で適用できると嬉しい？
 - » 現状のJPNAPでの構成だと利用者のGUI操作からルートサーバへの反映まで、数十分程度のタイムラグが生じてしまう
 - ◆ RTBHの特性上、攻撃が止まったかどうかの判断がお客様側でできないことについて
 - ✓ IX側でMAC ACLのdenyカウンターを見る程度しか取れる手がないと考えている

議論したいポイント詳細 (3/3)

■ サービス提供者視点で、この仕組みがより効果的に働く環境をどう作っていくか

- お客様に地道に /32, /128 のRTBH用経路の受け入れを依頼？
 - ◆ 広告された経路の受け入れ率を測る術はない
 - ◆ 実際に使ってみないと、どの程度効果が出るのか、本当に止められるのかは読みきれない
 - ◆ 帯域が潤沢な利用者からすると、受け入れるメリットが小さい…
 - ◆ これがIXでは標準的な挙動として浸透すれば、受け入れてもらいやすい…？
- 馴染みのないお客様向けに、RTBHの勉強会などを開催？