JANOG58 Meeting

マルチベンダーバックボーンで実現するDDoS対策 ～RFC Internet-DraftのBGP Flowspec Redirect-to-IP 導入への挑戦～

2026年7月17日

ビッグローブ株式会社

津山・阿部・中野

好きが、未来を変えていく。

会社紹介

商号	ビッグローブ株式会社(英文商号:BIGLOBE Inc.)
代表者	代表取締役社長 大谷 誠之
事業内容	インターネット等のネットワークを利用した情報サービスの提供および、 これに付帯または関連する一切の業務
本社所在地	東京都千代田区飯田橋三丁目10番10号
沿革	1986年　パソコン通信「PC-VAN」を開始 1995年　インターネット接続サービス「mesh」を開始 コンテンツ販売ポータル「Cyber Plaza」を開始 1996年　総合インターネットサービス「BIGLOBE」を開始 2006年　NECから分社し、NECビッグローブ株式会社設立 2014年　ビッグローブ株式会社に社名変更 2017年　KDDIグループへ
AS番号	2518

BIGLOBE光

BIGLOBE mobile

自己紹介

津山 訓司
プロダクト技術本部
セキュリティ基盤のマネージャー

セキュリティサービスを担当
新DDoS対策基盤の全体設計、
ExaBGP開発を担当

阿部 孝一
プロダクト技術本部
ネットワークエンジニア

BIGLOBEバックボーンの
構築・運用を担当
Flowspecの検証を担当

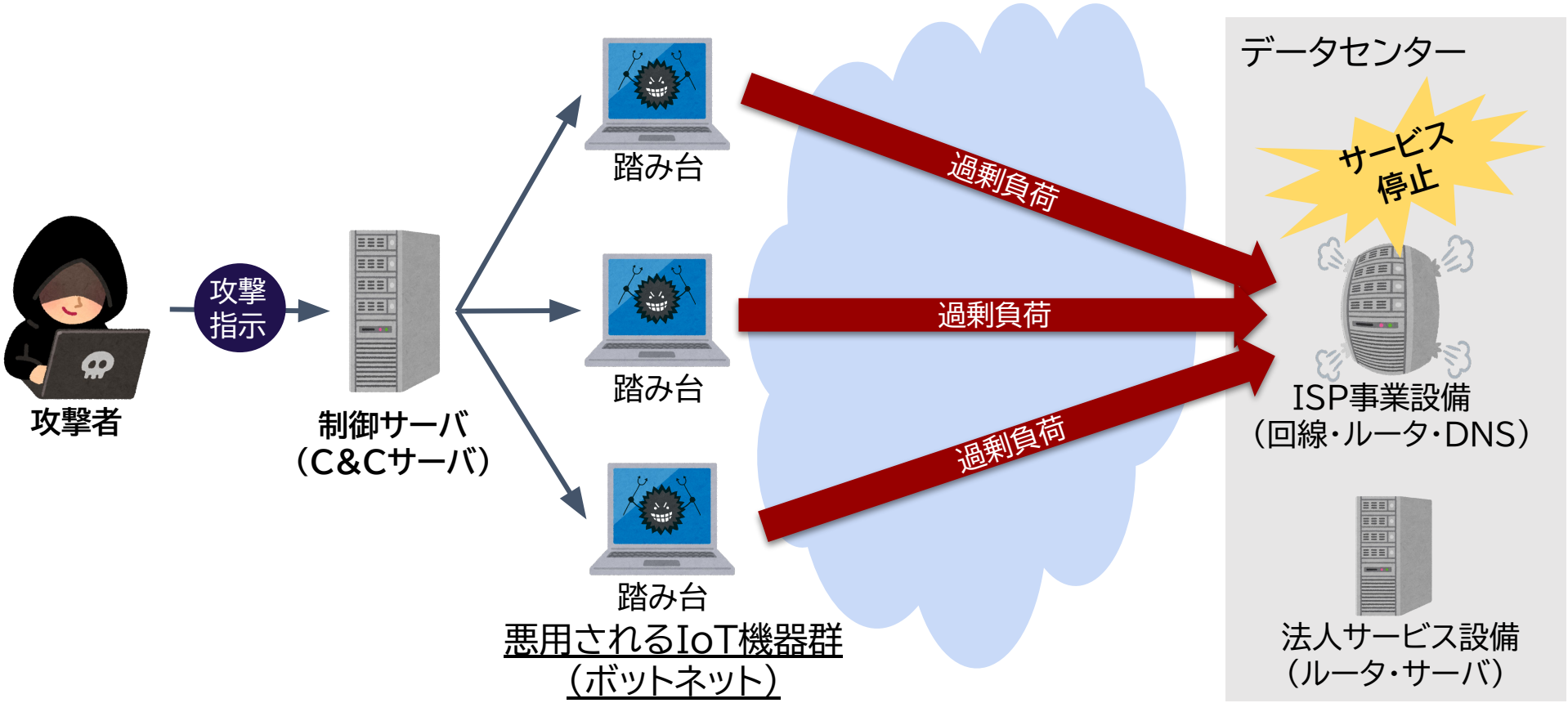
中野 龍
プロダクト技術本部
リードプロフェッショナル

BIGLOBEバックボーンの
設計・構築を担当
Flowspecの設計を担当

DDoS対策リニューアルの背景

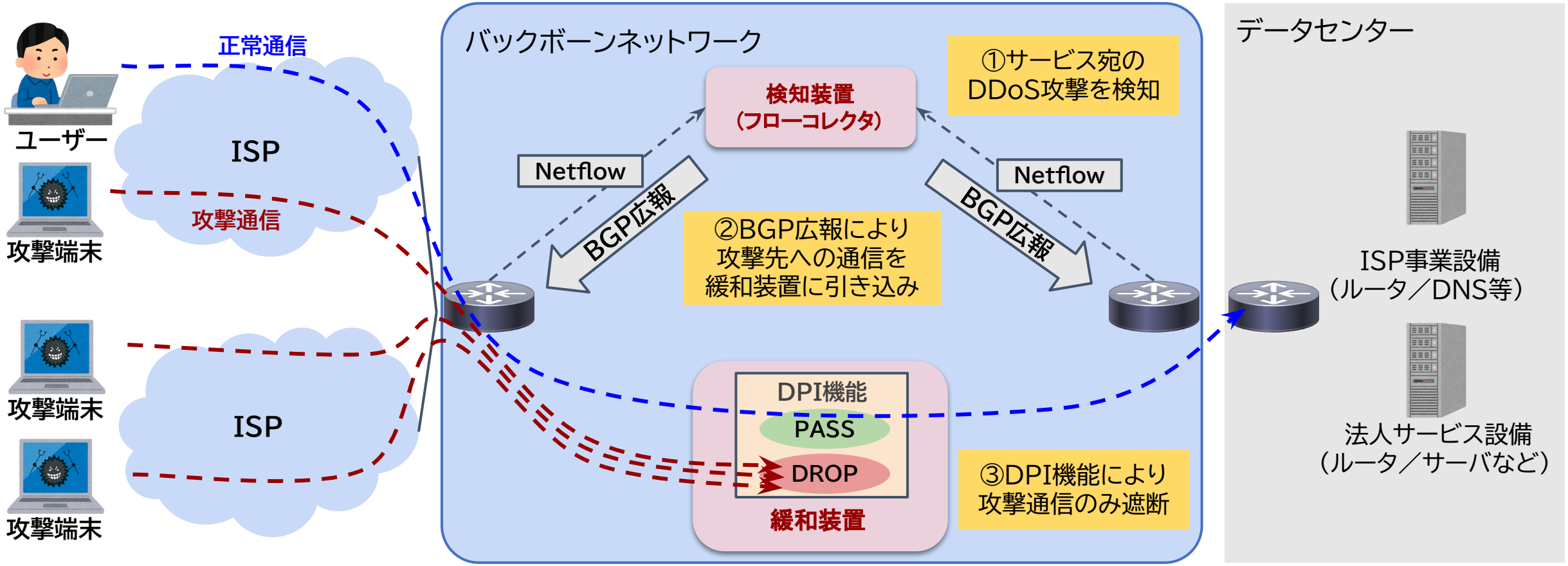
DDoS攻撃とは

- 大量の端末から、攻撃対象のサーバやネットワークに対して大量通信を送信し、膨大な負荷をかけてサービス停止を引き起こすサイバー攻撃
- 攻撃通信と正常通信を**見分けることが困難**なため、攻撃を防ぐためには**専用の仕組みが必要**



BIGLOBEのDDoS対策（BGPオフランプ）

- DDoS対策設備をデータセンターに構築し、以下のフローでDDoS攻撃を緩和。
  ① 攻撃検知 → ルータからフロー情報（Netflow）を収集し、DDoS攻撃を検知。
  ② 引き込み → BGP広報により、攻撃先宛の通信を緩和装置に引き込み。
  ③ 緩和処置 → DPI機能でDDoS攻撃を判別・遮断し、正常通信のみを通過。



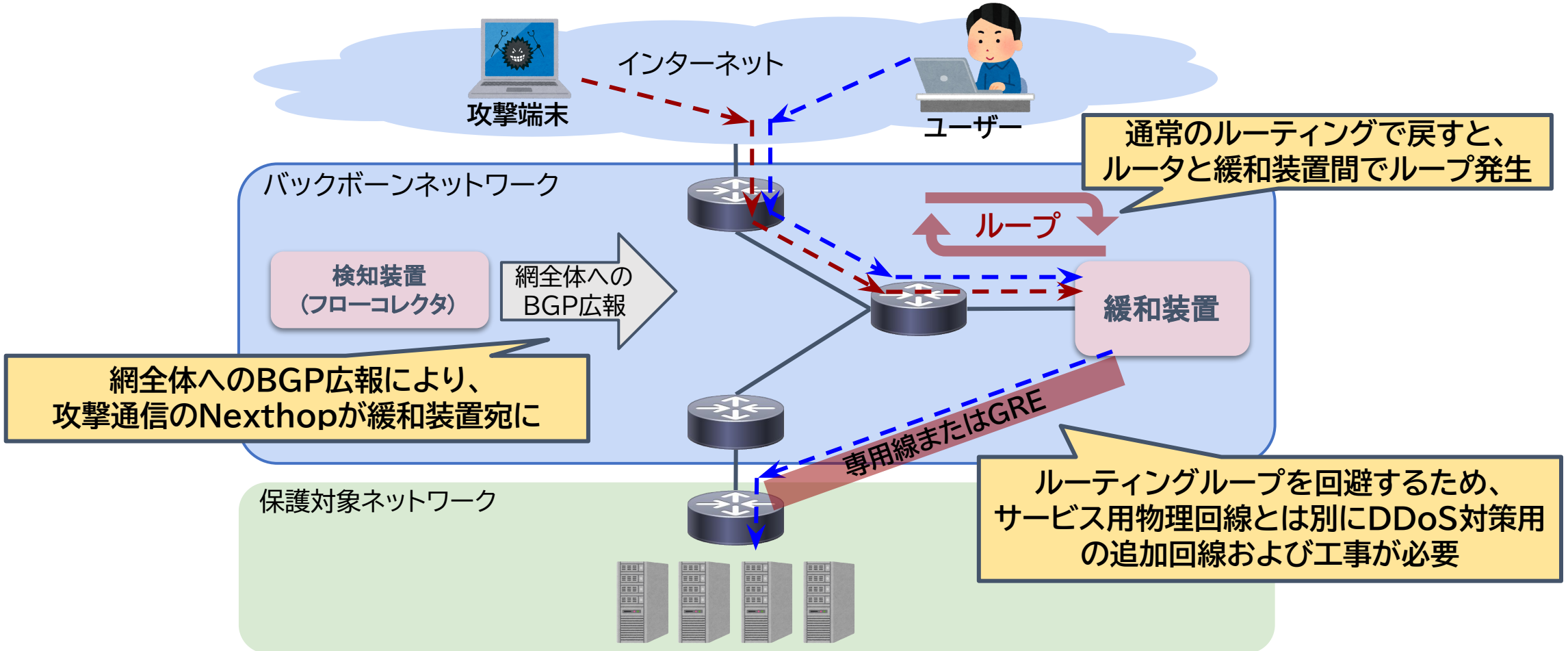
BIGLOBEのDDoS対策の課題

BIGLOBEでは以下の課題を契機に、2025年度にDDoS対策基盤をリニューアル。
本発表は、③「範囲」の課題をバックボーンネットワークで解決した事例紹介。

① 量	• **攻撃の大規模化** 2024年後半からISPユーザフレッツ網への100Gbps超の攻撃が急増し、DDoS緩和キャパシティを大幅に増強する必要が生じた
② 精度	• **攻撃の複雑化** 攻撃パターンの多様化に伴い、ユーザの正常通信と攻撃通信を正確に判別し、より精度良く攻撃を検知する必要性が高まった
③ 範囲	• **保護範囲の限定** DDoS攻撃から保護する設備（回線・ルータ・サーバ）を、技術的な制約で必要最低限の設備に限定せざるを得なかった

ミティゲーション方式により生じる技術制約

- 保護範囲が限定される原因は、引き込み時のBGP広報による特殊なルーティング操作。
- 保護すべきネットワークを緩和装置の保護下に置くには、DDoS緩和装置とルータ間を
  (a)専用線(物理回線) または **(b)GREトンネル(論理回線)** で直結する構成が不可欠。



DDoS保護範囲の課題と対策

広範囲のネットワークにあまねくDDoS対策を展開するには「防御専用の追加回線」と「工事」が必須。
→以下のケースで「導入したいが高すぎる／手間がかかりすぎてできない」

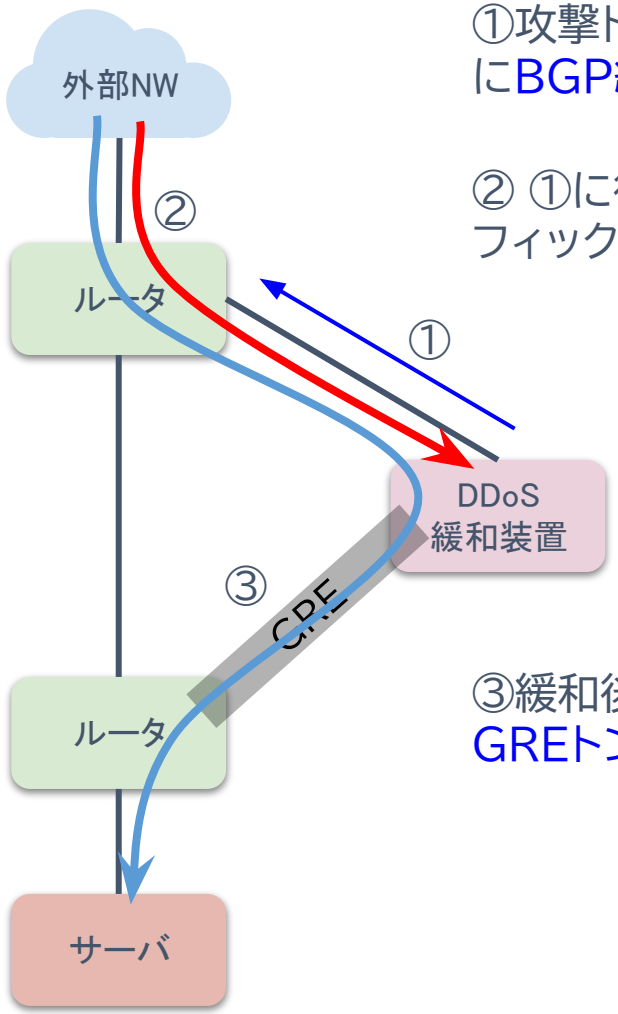
①自社拠点の増設時	（a）DDoS緩和装置から離れた新拠点へ都度専用線を引くのは、コスト・工期の観点から困難。 （b）必然的にGREトンネルを選択せざるを得ないが、運用負荷が増大する。
②トランジット顧客へのDDoS対策サービスの提供	（a）地理的に分散したトランジット顧客に対し、個別に専用線を用意するのはコスト・工期の観点から困難。 （b）顧客側ルータがGRE未対応の場合や、カプセル化に伴うCPU負荷に耐えられない懸念がある。

Flowspec Redirect-to-IPの導入により、回線そのまま、即時に防御

DDoSミティゲーションの主な方式

DDoSミティゲーションの主な方式(1)

BGP広報 + GRE戻し



①攻撃トラフィックを引き込むためにBGP経路の広報(/32等)

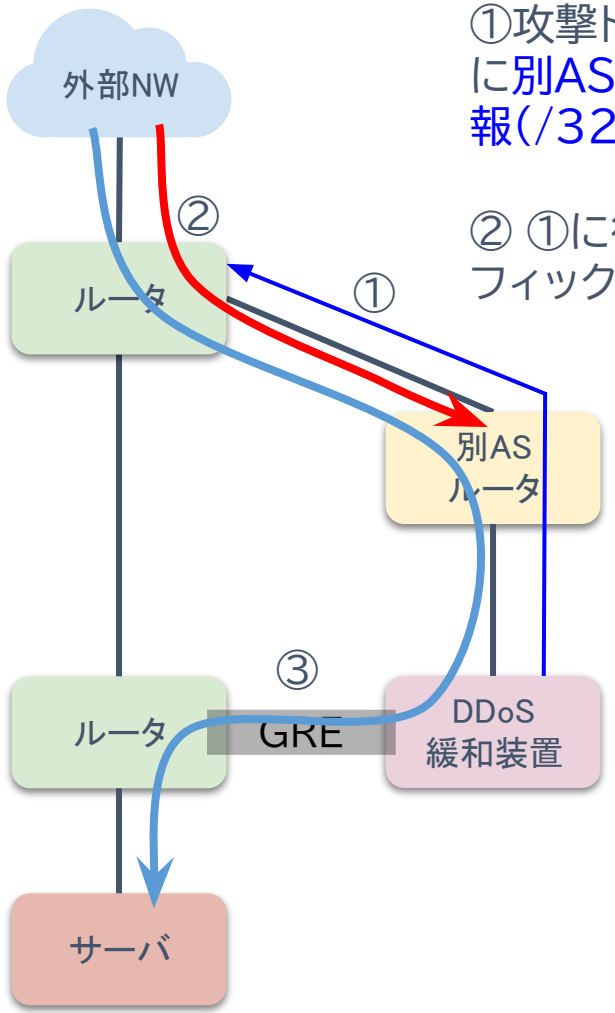
② ①に従いDDoS緩和装置にトラフィックを転送

③緩和後の正規トラフィックはGREトンネルで戻す

正規トラフィック

攻撃トラフィック

BGP広報 + 別AS処理 + GRE戻し



①攻撃トラフィックを引き込むために別ASを経由してBGP経路の広報(/32等)

② ①に従いDDoS緩和装置にトラフィックを転送

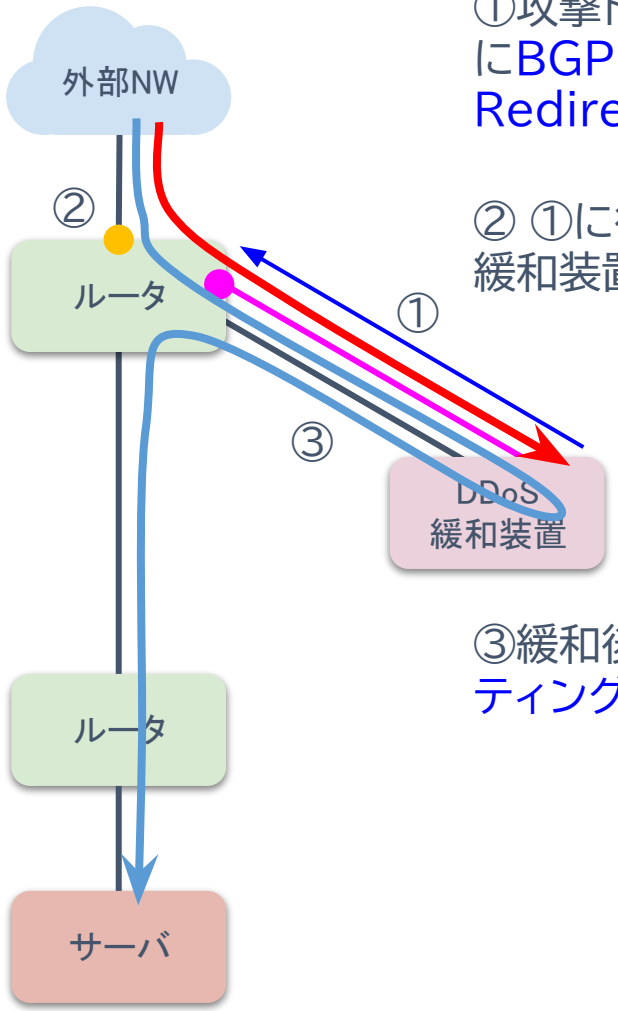
③緩和後の正規トラフィックはGREトンネルで戻す

正規トラフィック

攻撃トラフィック

DDoSミティゲーションの主な方式(2)

BGP Flowspec Redirect-to-VRF



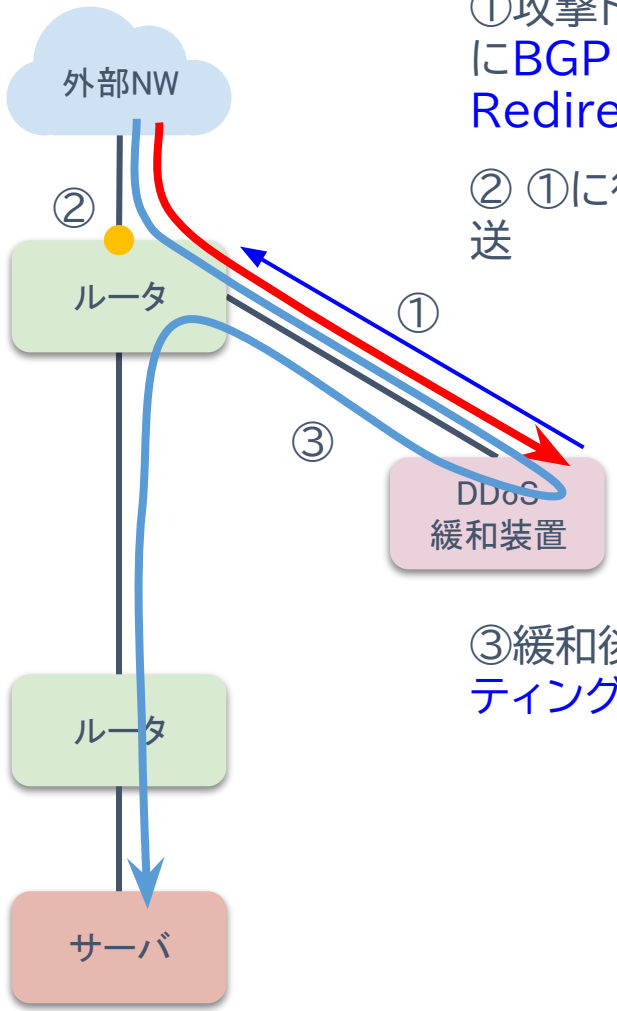
①攻撃トラフィックを引き込むためにBGP Flowspec Redirect-to-VRFの経路を広報

② ①に従いVRF経由にて、DDoS緩和装置に転送

③緩和後の正規トラフィックはルーティングテーブルに従い戻す

- VRF
- Flowspec有効IF
- 正規トラフィック
- 攻撃トラフィック

BGP Flowspec Redirect-to-IP



①攻撃トラフィックを引き込むためにBGP Flowspec Redirect-to-IPの経路を広報

② ①に従いDDoS緩和装置に転送

③緩和後の正規トラフィックはルーティングテーブルに従い戻す

- Flowspec有効IF
- 正規トラフィック
- 攻撃トラフィック

DDoSミティゲーション方式の比較

検討の結果、「BGP Flowspec Redirect-to-IP」を採用

方式	BGP広報 + GRE戻し	BGP広報 + 別AS処理 + GRE戻し	BGP Flowspec Redirect-to-VRF	BGP Flowspec Redirect-to-IP
トラフィック引き込み方法	DDoS検知装置、緩和装置よりIPv4 /32, IPv6 /128等の経路をBGPにて広報	DDoS検知装置、緩和装置よりIPv4 /32, IPv6 /128等の経路をBGPにて広報	DDoS検知装置、緩和装置よりBGP Flowspec Redirect-to-VRFの経路を広報	DDoS検知装置、緩和装置よりBGP Flowspec Redirect-to-IPの経路を広報
正規トラフィックの戻し方法	GREトンネルや専用回線を用意して戻す	GREトンネルや専用回線を用意して戻す	ルーティングテーブルに従い戻す	ルーティングテーブルに従い戻す
自ASへのDDoS緩和	対応可能	AS-PATHループとなり難しい	対応可能	対応可能
顧客ASのマルチホームDDoS緩和	対応可能	対応可能	対応可能	対応可能
BIGLOBEバックボーンへの採用にあたっての課題	GREトンネル/専用回線を多数構築する必要がある	自ASへのDDoS対応ができない GREトンネル/専用回線を多数構築する必要がある	各ルータからDDoS緩和装置へのVRF接続用リンクが必要	他社採用事例が少ない

BGP Flowspec Redirect-to-IPの動作イメージ

BGP Flowspecとは

RFC 8955/RFC 8956で規定されている、特定のトラフィックに対する制御ルールをネットワーク内のBGPルーター群に動的に伝達するためのもの。
主にDDoS攻撃対策を目的として開発されたが、特定のトラフィックを識別して制御（帯域制限、リダイレクト、マーキングなど）するために幅広く活用されている技術。

フィルタリング条件

- 宛先Prefix
- 送信元Prefix
- IPプロトコル
- ポート番号
- 宛先ポート番号
- 送信元ポート番号
- ICMPタイプ
- ICMPコード
- TCPフラッグ
- パケット長
- DSCP値
- フラグメント

アクション

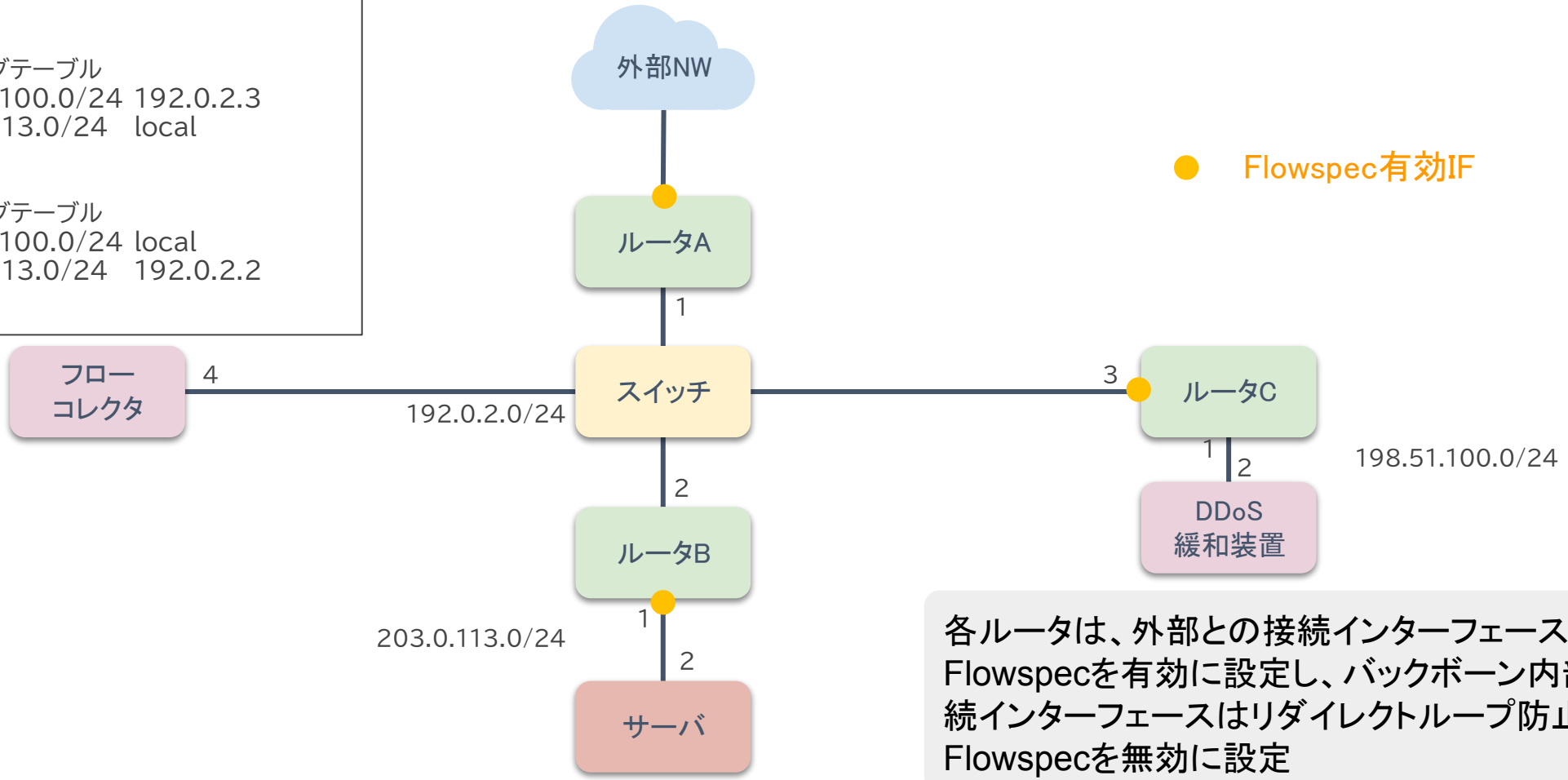
- バイト/秒単位でのトラフィック量制限
  （0を指定すると破棄）
- パケット/秒単位でのトラフィック量制限
- トラフィックアクション
  （後続のFlowspecの評価可否やサンプリング・ロギングの指定）
- VRFへのリダイレクト
- マーキング（DSCP値の上書き）
- **別のIPアドレスにリダイレクト（Redirect-to-IP）**

BGP Flowspec Redirect-to-IPの動作イメージ(1)

●ルータAのルーティングテーブル
BGP　198.51.100.0/24　192.0.2.3
BGP　203.0.113.0/24　192.0.2.2

●ルータBのルーティングテーブル
BGP　198.51.100.0/24　192.0.2.3
BGP　203.0.113.0/24　local

●ルータCのルーティングテーブル
BGP　198.51.100.0/24　local
BGP　203.0.113.0/24　192.0.2.2



Flowspec有効IF

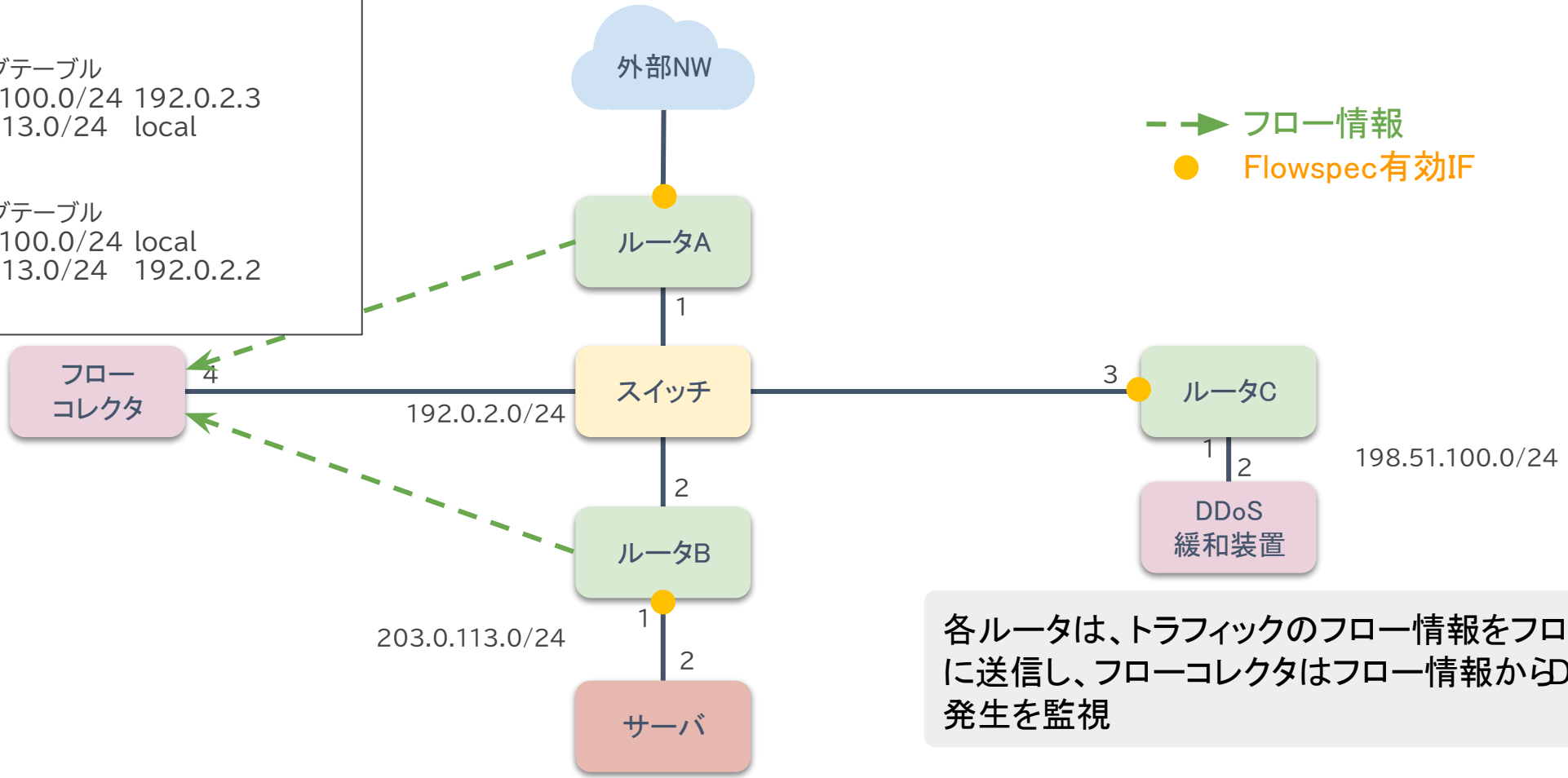
各ルータは、外部との接続インターフェースにおいてFlowspecを有効に設定し、バックボーン内部との接続インターフェースはリダイレクトループ防止のためFlowspecを無効に設定

BGP Flowspec Redirect-to-IPの動作イメージ(2)

●ルータAのルーティングテーブル
BGP　198.51.100.0/24　192.0.2.3
BGP　203.0.113.0/24　192.0.2.2

●ルータBのルーティングテーブル
BGP　198.51.100.0/24　192.0.2.3
BGP　203.0.113.0/24　local

●ルータCのルーティングテーブル
BGP　198.51.100.0/24　local
BGP　203.0.113.0/24　192.0.2.2



フロー情報
Flowspec有効IF

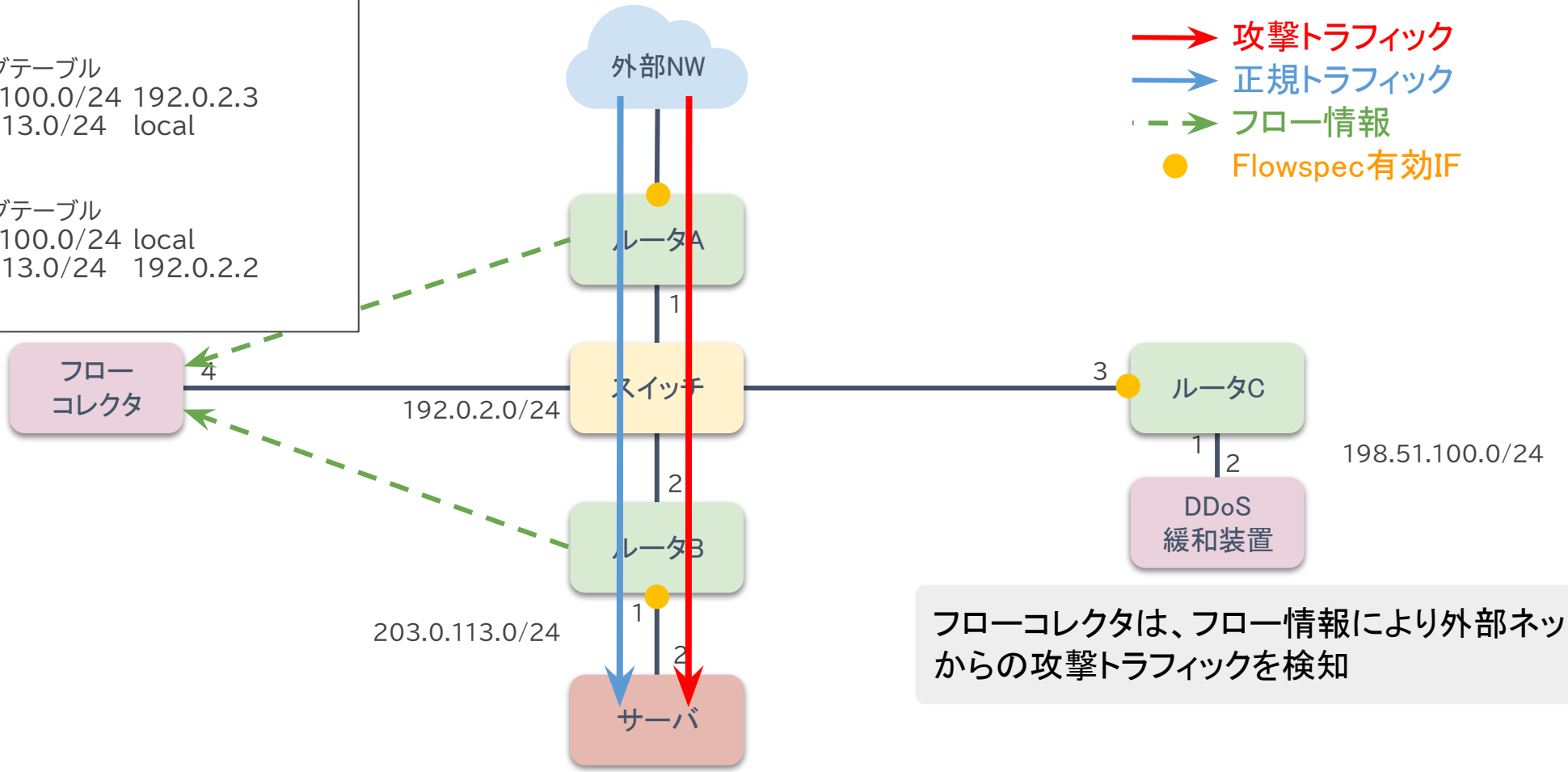
各ルータは、トラフィックのフロー情報をフローコレクタに送信し、フローコレクタはフロー情報からDDoSの発生を監視

BGP Flowspec Redirect-to-IPの動作イメージ(3)

●ルータAのルーティングテーブル
BGP　198.51.100.0/24 192.0.2.3
BGP　203.0.113.0/24　192.0.2.2

●ルータBのルーティングテーブル
BGP　198.51.100.0/24 192.0.2.3
BGP　203.0.113.0/24　local

●ルータCのルーティングテーブル
BGP　198.51.100.0/24 local
BGP　203.0.113.0/24　192.0.2.2



攻撃トラフィック
正規トラフィック
フロー情報
Flowspec有効IF

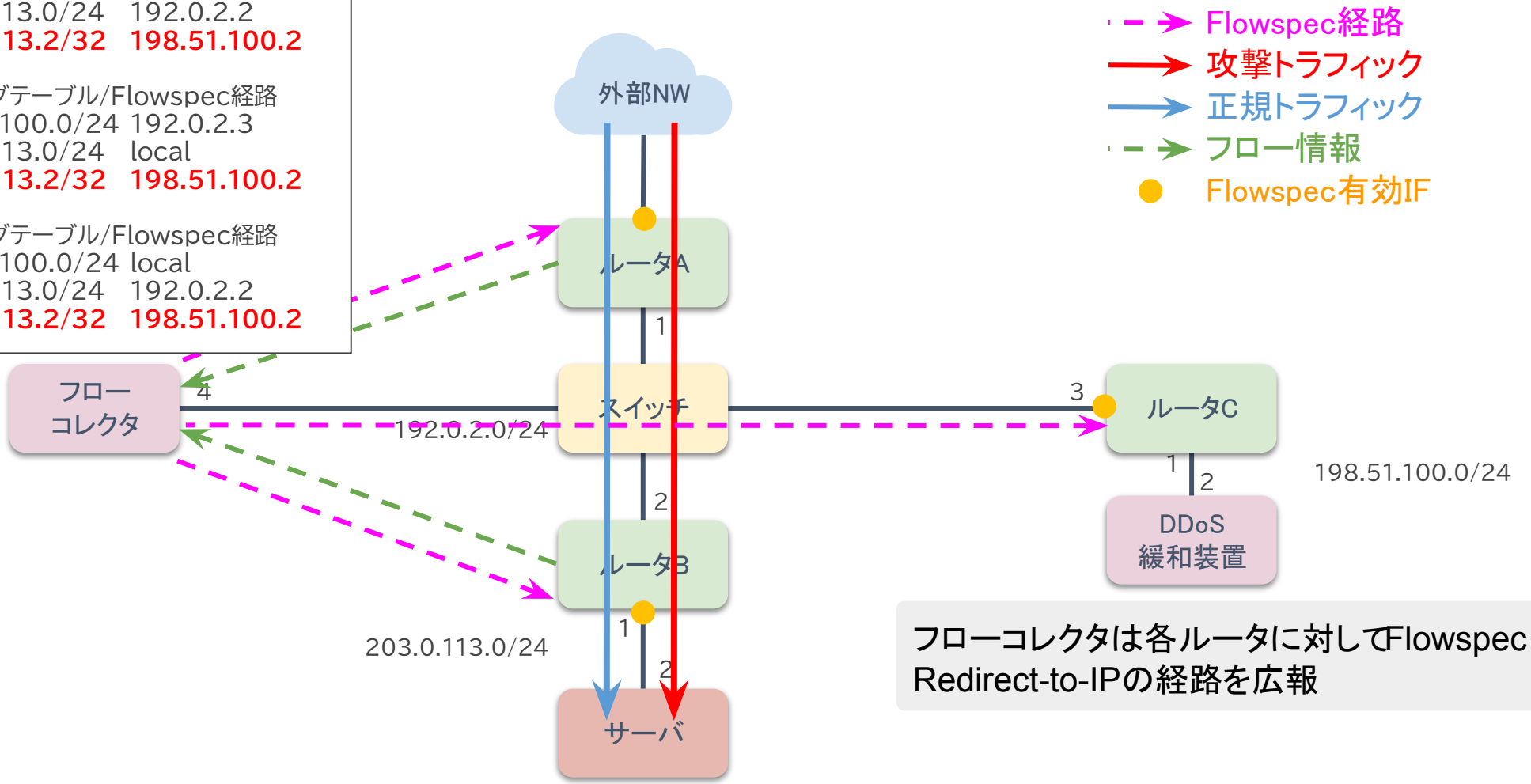
フローコレクタは、フロー情報により外部ネットワークからの攻撃トラフィックを検知

BGP Flowspec Redirect-to-IPの動作イメージ(4)

●ルータAのルーティングテーブル/Flowspec経路
BGP　198.51.100.0/24　192.0.2.3
BGP　203.0.113.0/24　192.0.2.2
Flowspec　203.0.113.2/32　198.51.100.2

●ルータBのルーティングテーブル/Flowspec経路
BGP　198.51.100.0/24　192.0.2.3
BGP　203.0.113.0/24　local
Flowspec　203.0.113.2/32　198.51.100.2

●ルータCのルーティングテーブル/Flowspec経路
BGP　198.51.100.0/24　local
BGP　203.0.113.0/24　192.0.2.2
Flowspec　203.0.113.2/32　198.51.100.2



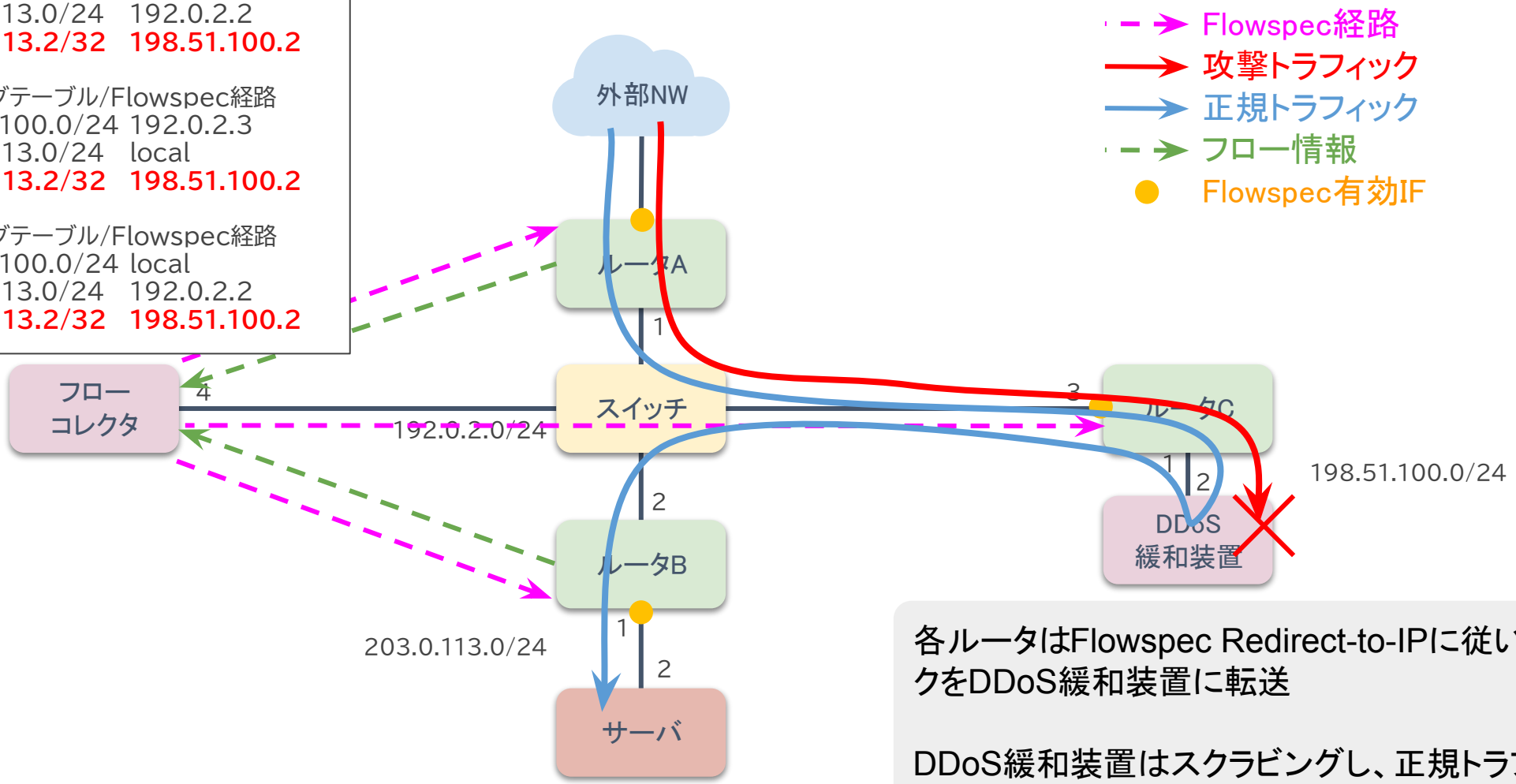
フローコレクタは各ルータに対してFlowspec Redirect-to-IPの経路を広報

BGP Flowspec Redirect-to-IPの動作イメージ(5)

●ルータAのルーティングテーブル/Flowspec経路
BGP　198.51.100.0/24　192.0.2.3
BGP　203.0.113.0/24　192.0.2.2
Flowspec　203.0.113.2/32　198.51.100.2

●ルータBのルーティングテーブル/Flowspec経路
BGP　198.51.100.0/24　192.0.2.3
BGP　203.0.113.0/24　local
Flowspec　203.0.113.2/32　198.51.100.2

●ルータCのルーティングテーブル/Flowspec経路
BGP　198.51.100.0/24　local
BGP　203.0.113.0/24　192.0.2.2
Flowspec　203.0.113.2/32　198.51.100.2



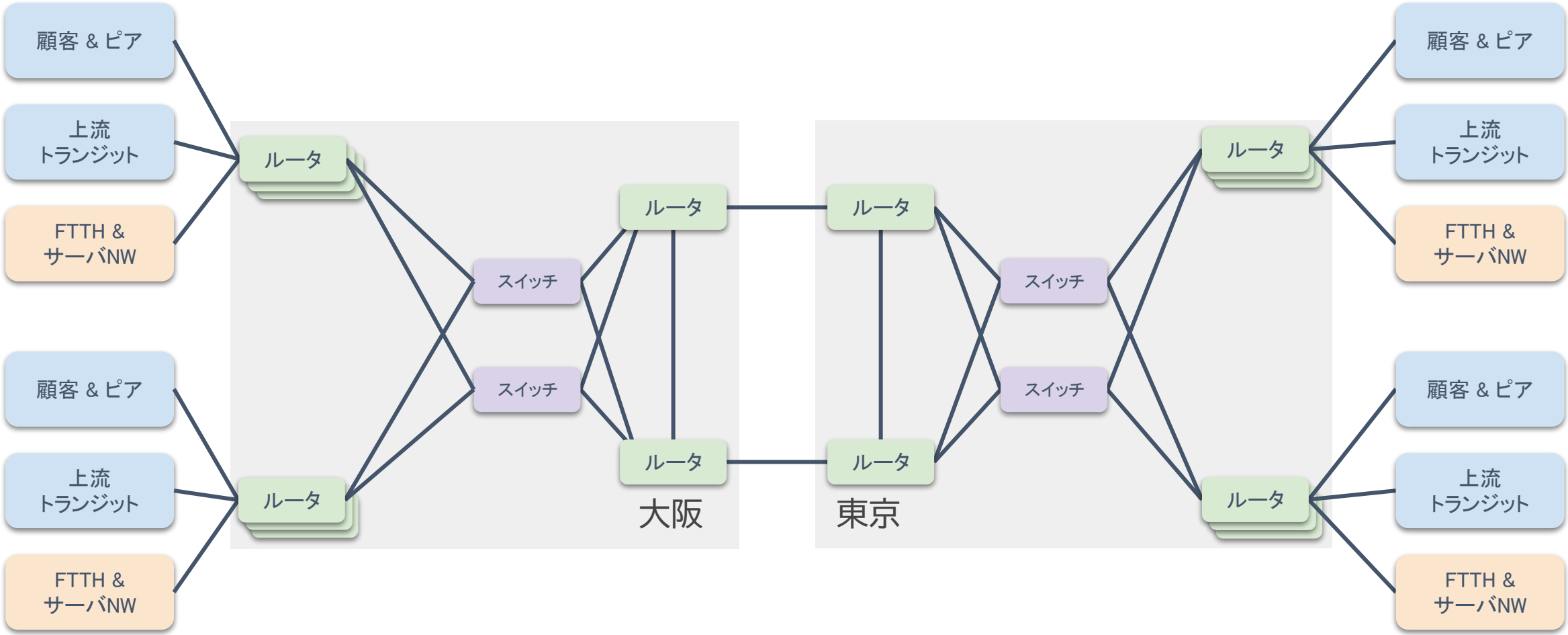
各ルータはFlowspec Redirect-to-IPに従いトラフィックをDDoS緩和装置に転送

DDoS緩和装置はスクラビングし、正規トラフィックだけを本来の宛先に転送

BIGLOBEがRedirect-to-IPを採用した理由

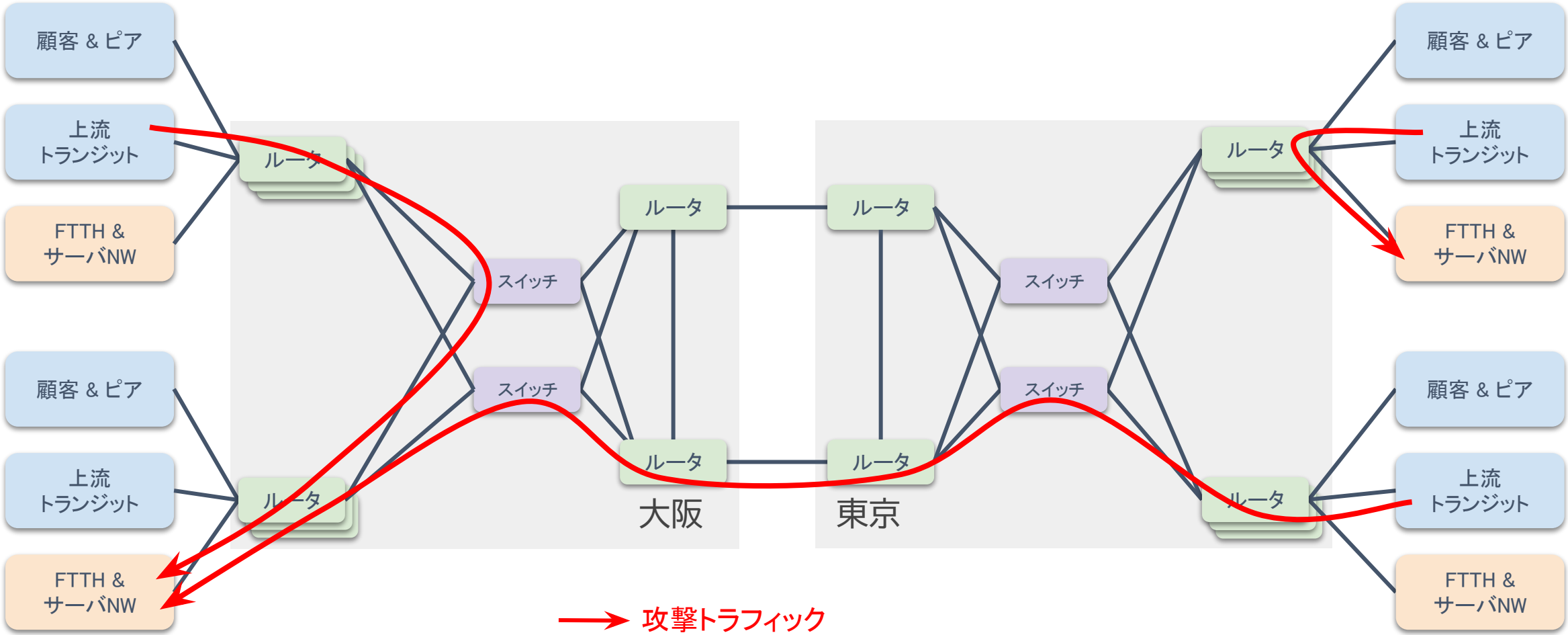
BIGLOBEがRedirect-to-IPを採用した理由(1)

BIGLOBEでは、バックボーンネットワークの各ルータに、「顧客」「ピア」「上流トランジット」「FTTH」「サーバNW」を混在収容している。



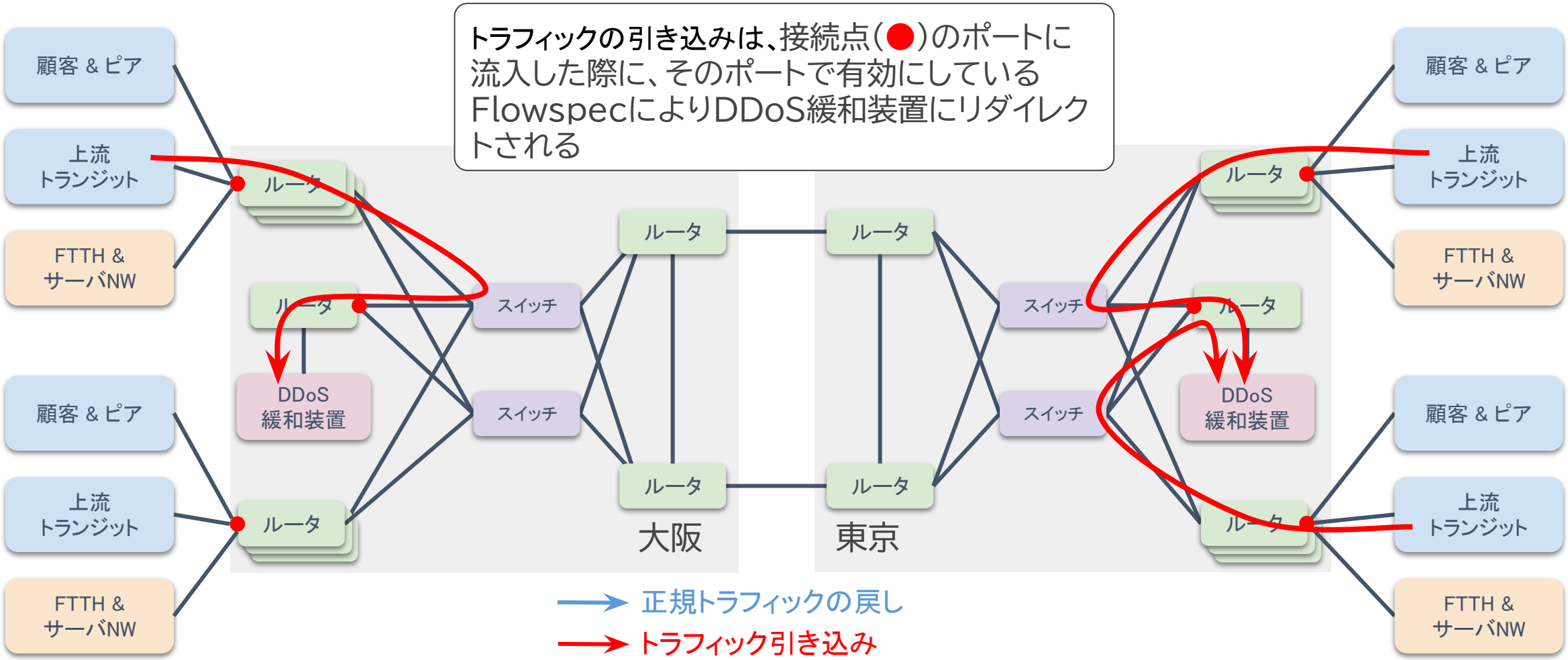
BIGLOBEがRedirect-to-IPを採用した理由(2)

攻撃先の収容ルータは、全ルータが対象で、DDoS緩和装置で緩和後の正規トラフィックの戻し先も全ルータとなり、全てにGREトンネルや専用回線の戻しルートを構成することは難しい。
そのため、戻しトラフィックの考慮が不要となる「Flowspec Redirect-to-IP」を採用。



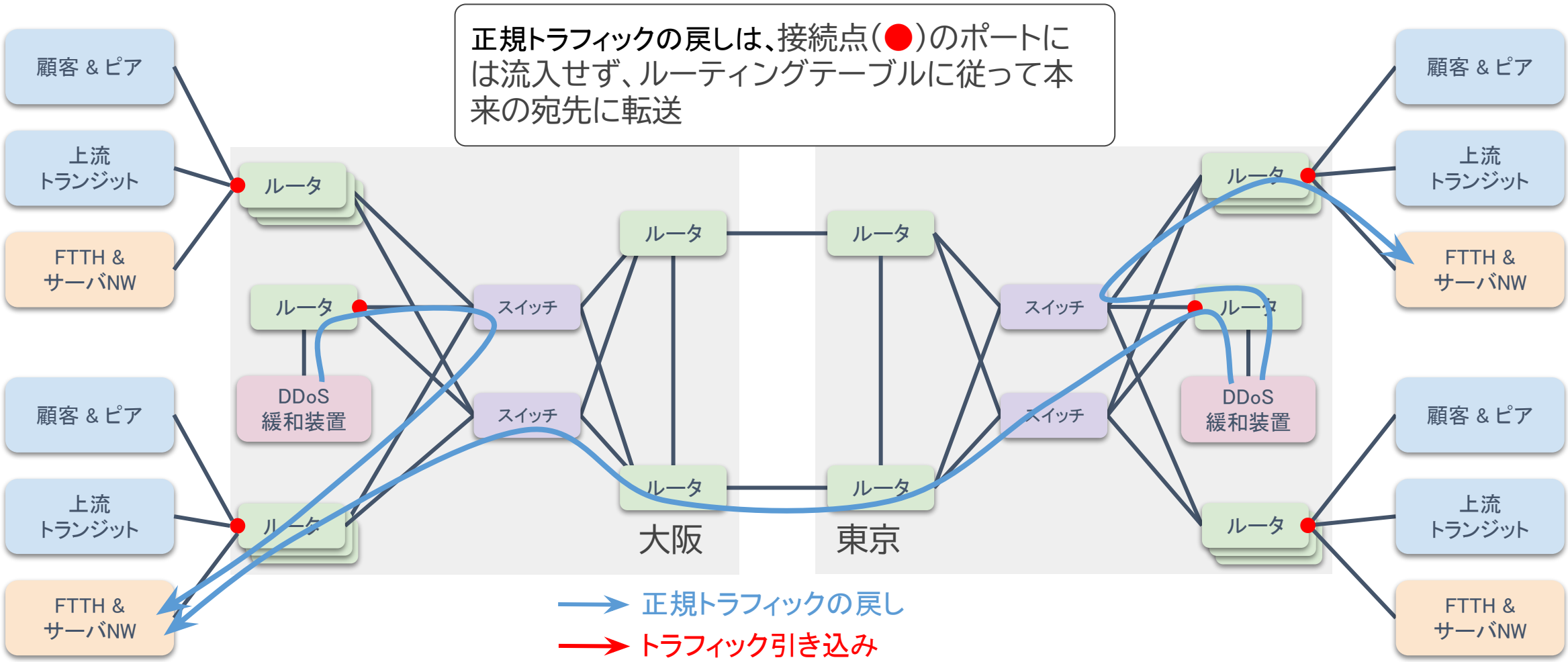
BGP Flowspec Redirect-to-IPの導入後の構成

DDoS緩和装置は東京・大阪に設置し、BGP AnycastにてDDoS流入から近い装置で緩和処理を実施。
Flowspecの処理は、各ルータの外部との接続点(●)のみで有効にし、リダイレクトループの発生を防ぐ構成を実現。



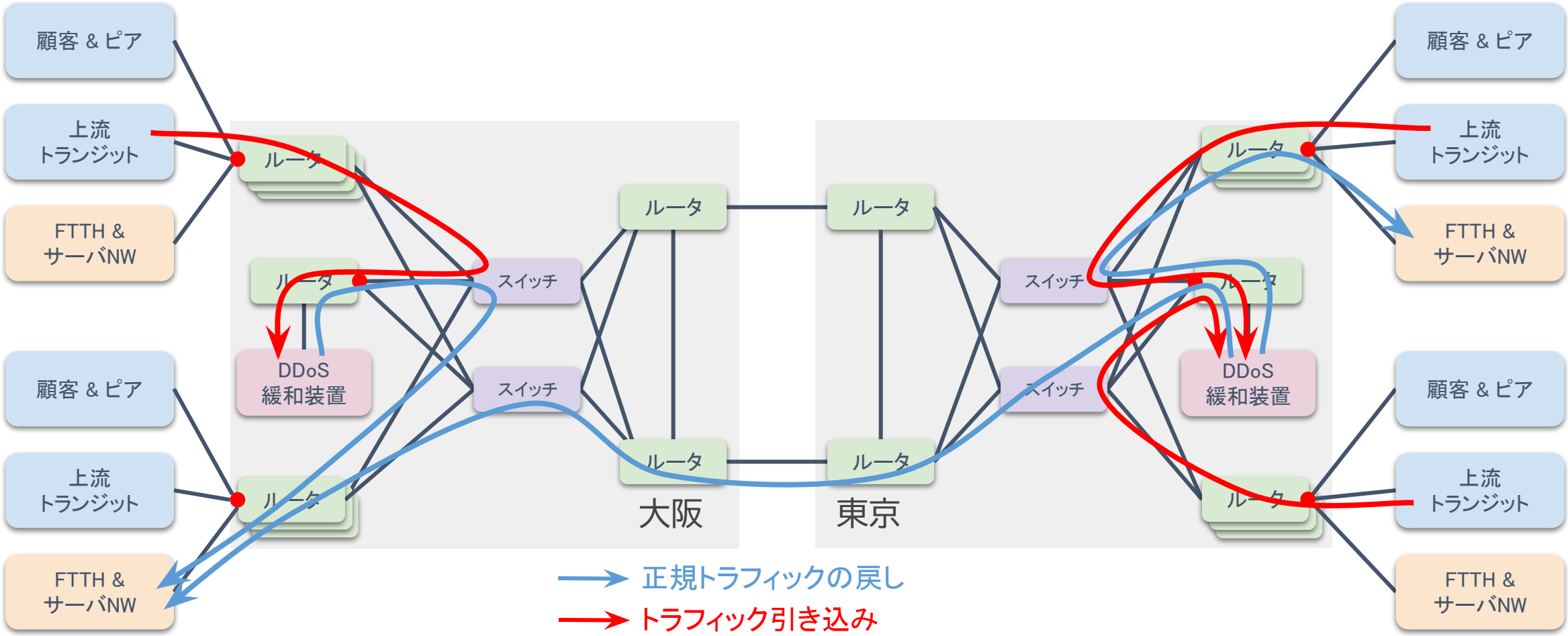
BGP Flowspec Redirect-to-IPの導入後の構成

DDoS緩和装置は東京・大阪に設置し、BGP AnycastにてDDoS流入から近い装置で緩和処理を実施。
Flowspecの処理は、各ルータの外部との接続点(●)のみで有効にし、リダイレクトループの発生を防ぐ構成を実現。



BGP Flowspec Redirect-to-IPの導入後の構成

DDoS緩和装置は東京・大阪に設置し、BGP AnycastにてDDoS流入から近い装置で緩和処理を実施。
Flowspecの処理は、各ルータの外部との接続点(●)のみで有効にし、リダイレクトループの発生を防ぐ構成を実現。



BGP Flowspec Redirect-to-IPのRFCドラフトの非互換性の課題

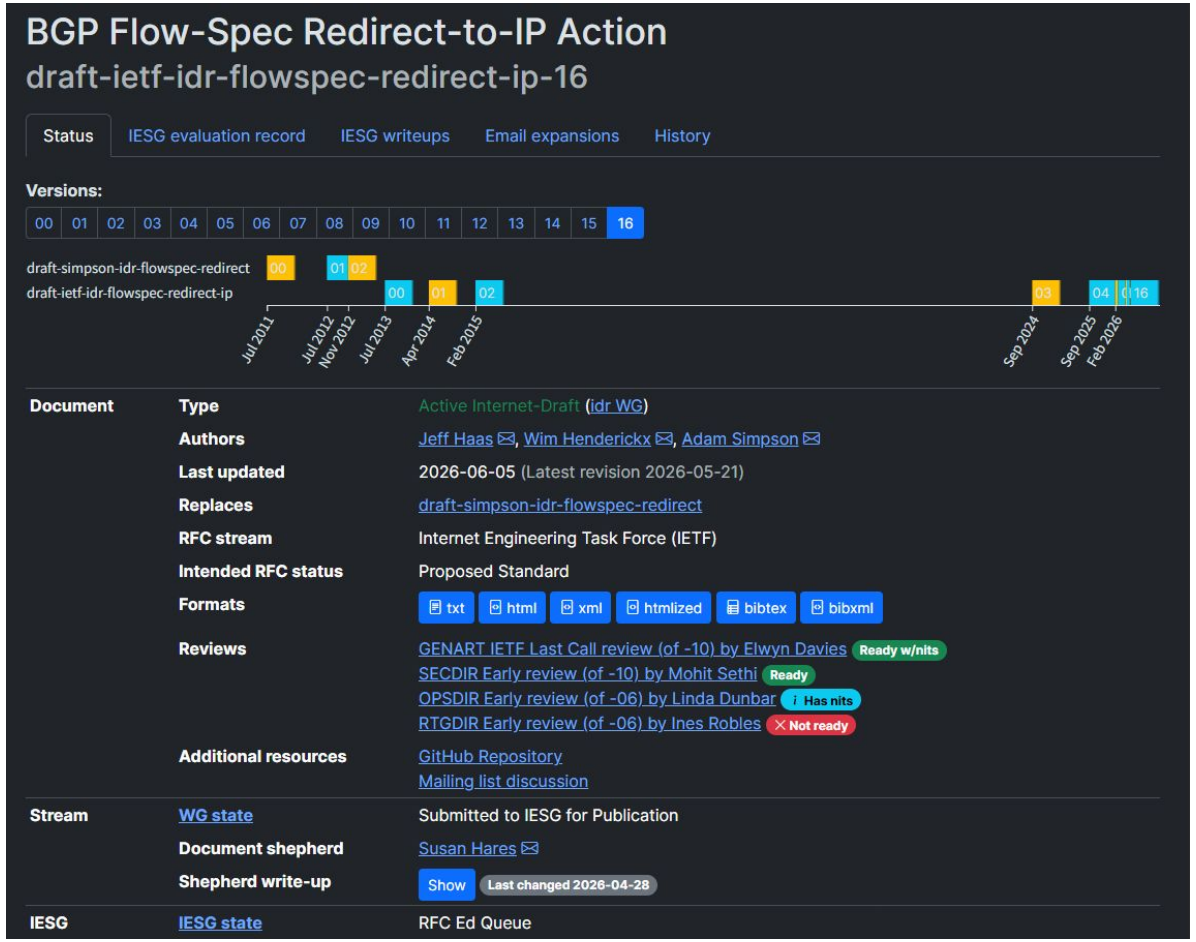
非互換性に気づいたキッカケ

1. DDoSミティゲーション方式の確定後、設計とPoC（概念実証）を並行して実施

2. PoC（概念実証）の内容
   a. A社ルータにてRedirect-to-IP経路を生成し、B社ルータにて正常動作を確認
   b. B社ルータにてRedirect-to-IP経路を生成し、A社ルータにて正常動作を確認
   c. C社ルータにRedirect-to-IPの処理機能が実装されていることを確認
   d. a, b, cの結果より、実現可能と判断

3. PoC（概念実証）の結果を受けて、評価環境にて実機検証
   a. B社ルータにてRedirect-to-IP経路を生成し、C社ルータで動作確認すると、BGP Extended Communityが認識されず、正しく処理されないことを確認
   b. 調べた結果、B社とC社のルータに実装の違いがあることを確認・・・

BGP Flowspec Redirect-to-IPのRFC Internet-Draftの状況



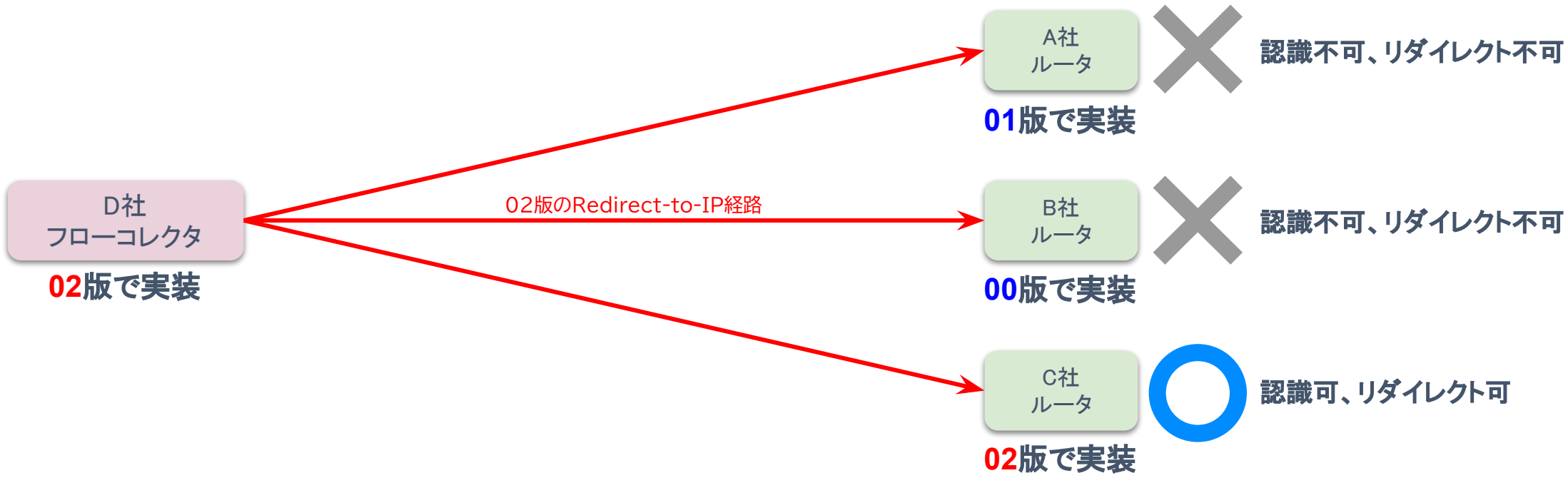
https://datatracker.ietf.org/doc/draft-ietf-idr-flowspec-redirect-ip/

BGP Flowspec Redirect-to-IPは、最初のドラフトが2011年7月に公開され、現在もInternet-Draftの状態（最新のドラフトは2026年5月の16版）

BIGLOBEが採用しているルータベンダー毎に実装バージョンが異なり、そのバージョン間（00/01版と02版）には互換性がない状態となっていた

A社	**IPv4/IPv6ともに以下の実装** draft-ietf-idr-flowspec-redirect-ip-01
B社	**IPv4は以下から選択可能** draft-ietf-idr-flowspec-redirect-ip-00 draft-ietf-idr-flowspec-redirect-ip-02 **IPv6は以下の実装** draft-ietf-idr-flowspec-redirect-ip-00
C社	**IPv4/IPv6ともに以下の実装** draft-ietf-idr-flowspec-redirect-ip-02

ドラフトバージョンの違いによる挙動

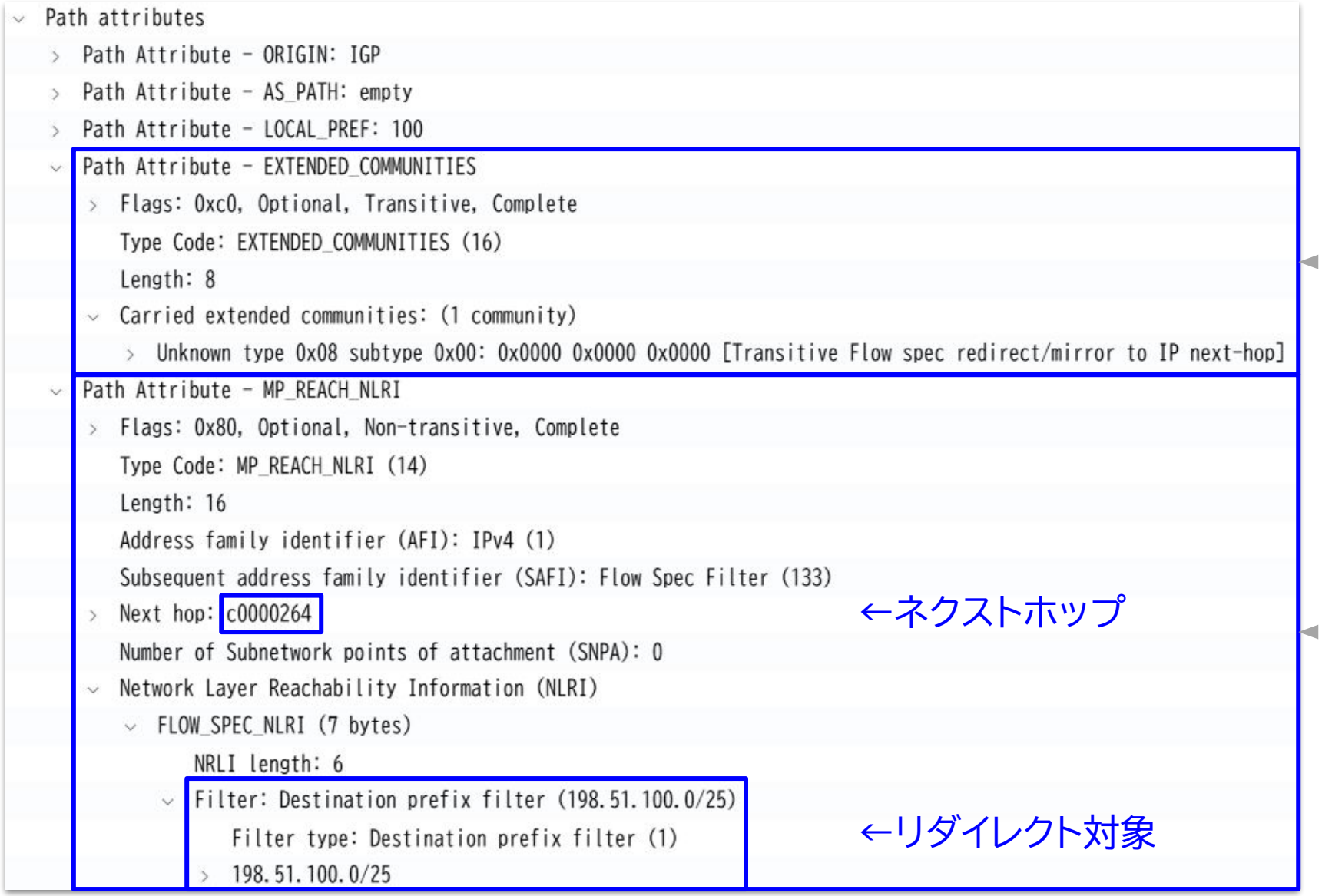


D社フローコレクタは、draft-ietf-idr-flowspec-redirect-ip-02で実装され、02版のRedirect-to-IPの経路広報のみ可能

A/B社ルータは、draft-ietf-idr-flowspec-redirect-ip-00/01にて実装されているため、02版のRedirect-to-IPの経路を受け取っても認識されず、リダイレクト処理が実行されない

C社ルータは、draft-ietf-idr-flowspec-redirect-ip-02にて実装されているため、02版のRedirect-to-IPの経路を受け取った場合は、リダイレクト処理が実行される

draft-ietf-idr-flowspec-redirect-ip-00/01のフォーマット



Extended Community

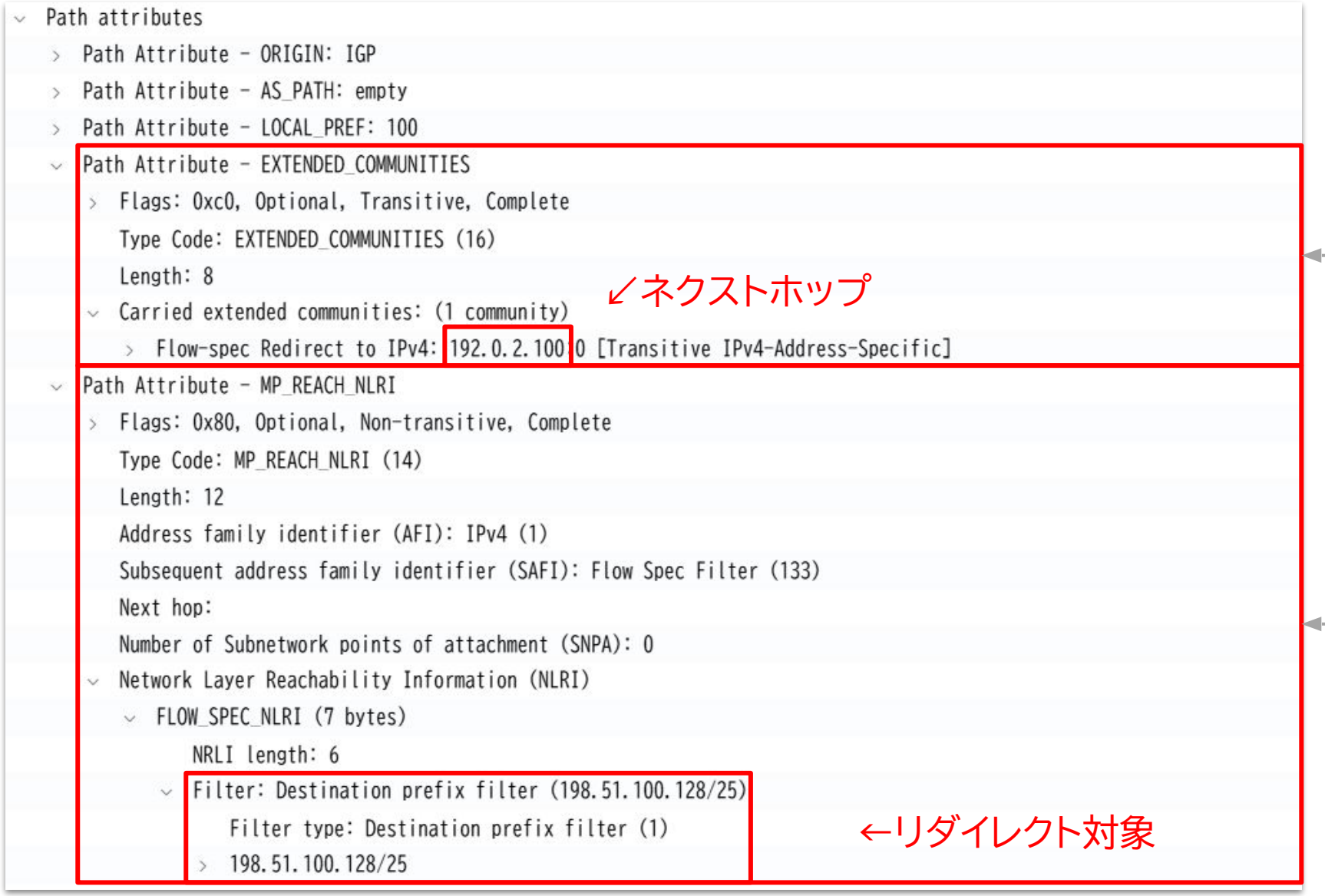
タイプは0x08、サブタイプは0x00

MP_REACH_NLRI

リダイレクト先のNext hopは、MP_REACH_NLRI内のNext hopに格納

リダイレクト対象の情報は、MP_REACH_NLRI内のNLRIに格納

draft-ietf-idr-flowspec-redirect-ip-02以降のフォーマット



Extended Community

タイプは0x01、サブタイプは0x0c

リダイレクト先のNext hopは、
Extended Community内にIPv4 Address Specificとして格納

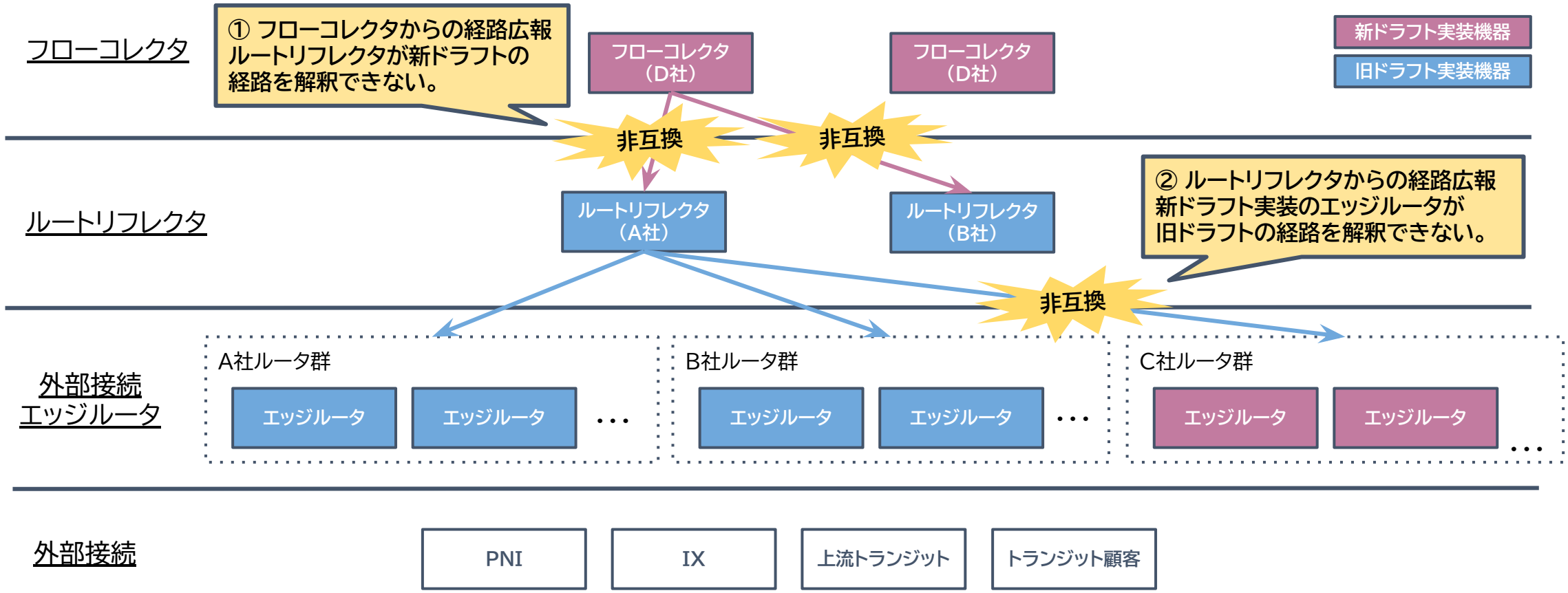
MP_REACH_NLRI

リダイレクト対象の情報は、
MP_REACH_NLRI内のNLRIに格納

ドラフトバージョンの非互換性への対応

ドラフトバージョン非互換による課題

バックボーンネットワーク内でのDDoS攻撃対策において、緩和装置へ通信を引き込むためのFlowspec経路伝搬が、プロトコル非互換により2箇所で遮断されてしまう。
どのように経路伝搬を実現させるか？



新旧ドラフトのFlowspec経路を伝搬させるには・・・

フローコレクタ（製品）側の動作変更は困難なため、それ以外の箇所で新旧ドラフト差分を吸収して解決を図る必要があった。

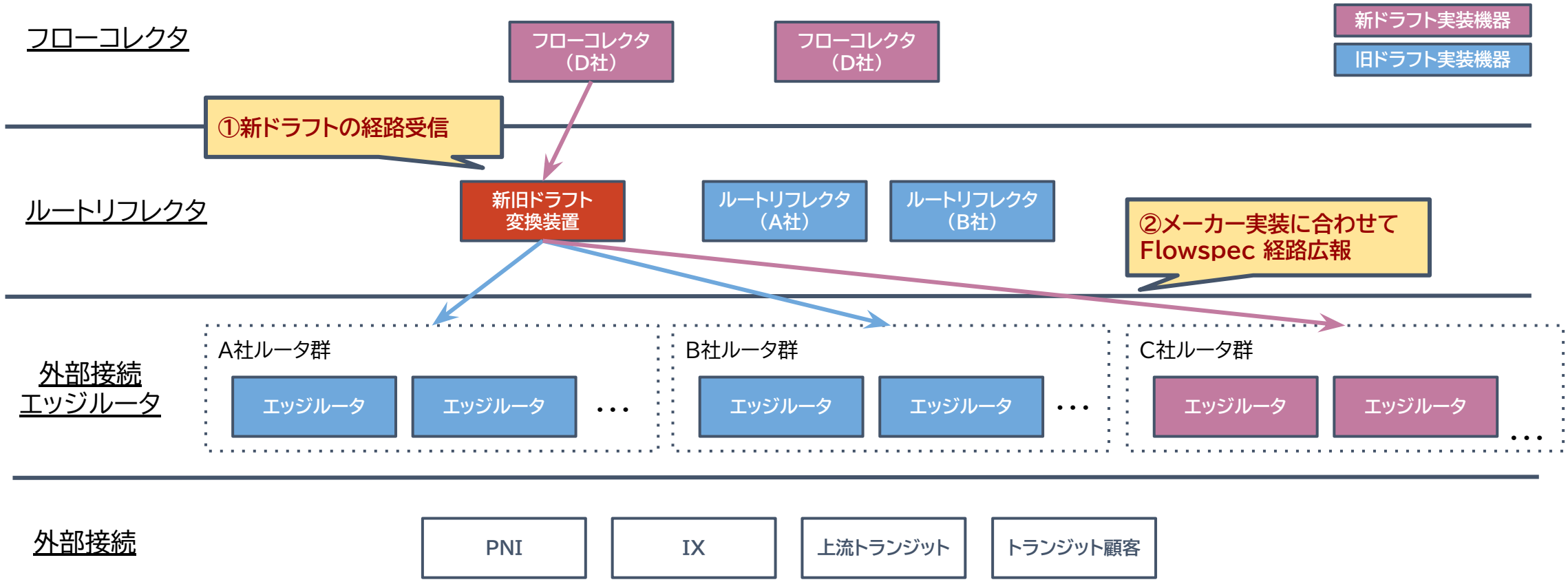
- 解決策① **ルータ機器内**で新旧ドラフト差分を吸収する
  - ルートリフレクタによる、新旧ドラフト両対応のFlowspec経路広報
  - C社ルータ側での、旧ドラフト経路の受信対応

- 解決策② **ルータ機器外部**で新旧ドラフト差分を吸収する
  - **新旧ドラフトを変換できるソフトウェア・製品の導入**

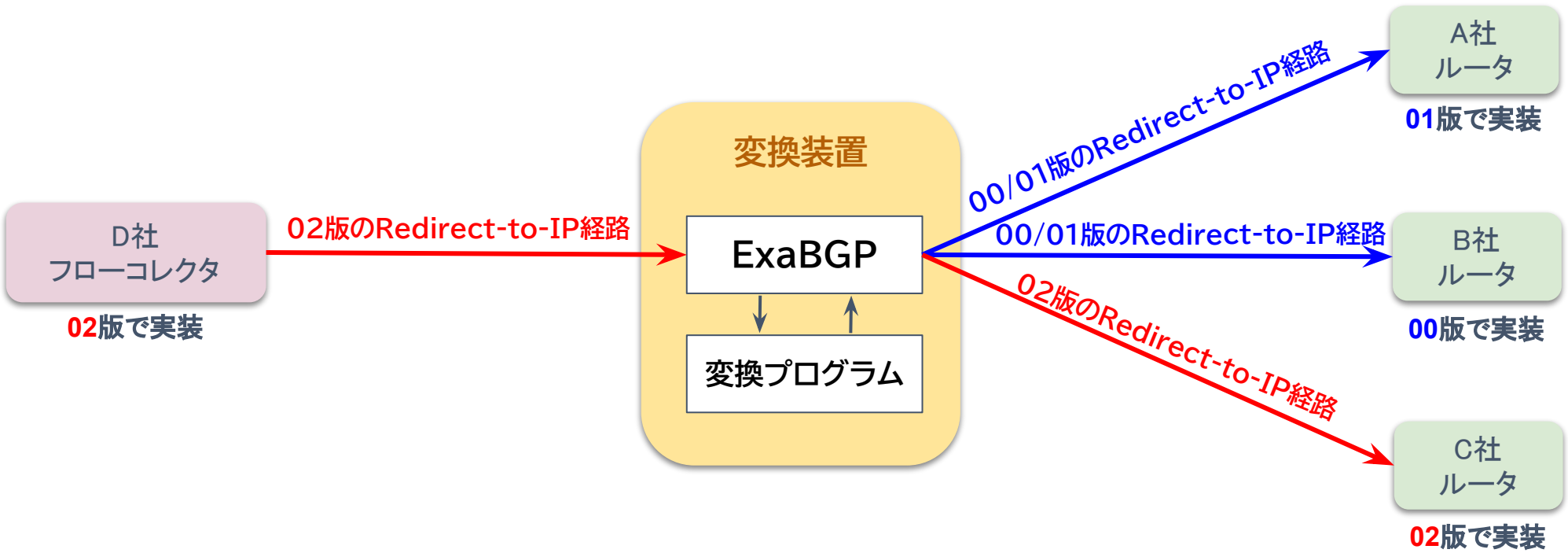
- 解決策③ Redirect-to-IPの採用を諦める
  - RFC標準化済みのRedirect-to-VRFを利用すれば、ルータ間の非互換性は回避可能
  - ただし、バックボーンコア設計の抜本的な変更が必要（ネットワーク全体を1面→2面へ変更）

解決策　新旧ドラフト変換ソフトウェアの導入

新旧ドラフトを変換できる既存製品がないため、自社で独自の変換装置を開発する解決策を採用。
① フローコレクタ（D社）からの新ドラフト経路を受信
② エッジルータ（ABC社）に、メーカー実装に合わせたFlowspec経路を広報



新旧ドラフト変換装置の開発



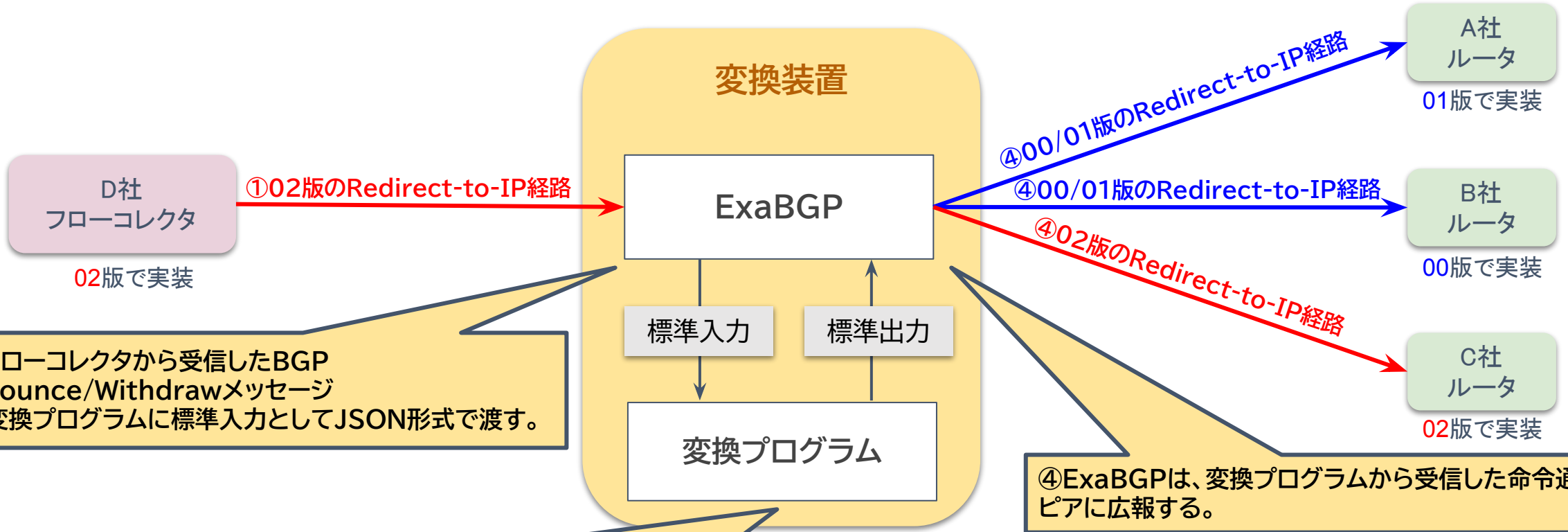
指定したドラフトバージョンのBGP Flowspec Redirect-to-IPの経路を広報する装置をOSSのExaBGPベースに開発

https://github.com/Exa-Networks/exabgp

ExaBGPの外部プログラム(process, run)機能を利用して、フローコレクタから受信したBGP Updateメッセージを
パースし、各ルータに00/01版あるいは02版に変換して広報することで、バージョン間の非互換性を吸収

ExaBGPを用いた非互換性の変換

ExaBGPの新旧ドラフトAPIを利用して、最小限の実装で変換装置を実現。



② フローコレクタから受信したBGP Announce/Withdrawメッセージを、変換プログラムに標準入力としてJSON形式で渡す。

④ExaBGPは、変換プログラムから受信した命令通りにピアに広報する。

③ 変換プログラムの処理内容:
1. 受信したBGPメッセージのExtended Communityより、新ドラフト版であることを判定。
2. 広報対象の全ピアに対して、以下の操作を実施。
  ・各ピアがどのドラフト実装(00/01版 or 02版)のルータかを判定。
  ・ExaBGPの新旧ドラフトAPIを使い分け、標準出力へ広報命令を渡す。

旧ドラフトAPI

```
neighbor x.x.x.x announce flow route destination-ipv4 x.x.x.x/32 redirect x.x.x.x
```

新ドラフトAPI

```
neighbor x.x.x.x announce flow route destination-ipv4 x.x.x.x/32 redirect-to-next-ietf x.x.x.x
```

まとめ

まとめと今後の展望

まとめ

- BIGLOBEではDDoSミティゲーションのために、BGP Flowspec Redirect-to-IPを採用
- マルチベンダーのルータ採用は、品質向上やコストメリットはあるが、なかなか大変
  - 複数ベンダー/複数モデルあると、OSバージョンアップ時や機能追加時には、それなりに時間がかかる
- RFC化前のInternet-Draftには気をつけよう
  - 設計・PoCが終わり、実機検証をする中で気付いたので、スケジュール的に大変だった・・・

今後の展望

- フローコレクタ側で複数ドラフトバージョンに対応した経路の出し分けが可能となり、今後は変換装置が不要となる見込み
- バックボーン全体のFlowspec対応により、Service Chainingや上下双方向のトラフィックリダイレクトを利用した高度な機能展開が可能に
- DDoS対策における、フィルタ/破棄/流量制御 + リダイレクトの組み合わせによる柔軟な制御の実現
- トランジット顧客に対するDDoSトラフィックの吸い込み + 緩和機能の提供

議論のポイント

- DDoSミティゲーション(スクラビングへの引き込み)には様々な方式がありますが、どのような方式で導入されていますか
- BGP Flowspecは10年ほど前によく話題になっていましたが、実際にどのような目的で商用利用されていますか。商用利用にあたって課題になった事はありますか
- マルチベンダーを採用する事によって、品質向上やコスト改善のメリットはありますが、機種数の増大で運用コストの増加に繋がっていると感じていますが、どう改善されていますか
- Internet-Draft段階のRFCの商用導入においては、Standardになるまでに非互換の変更がされる事がありますが、どのように乗り越えていますか

好きが、未来を変えていく。

BIGLOBE