



NAT を使用したパフォーマンス ルーティング

パフォーマンスルーティング (PfR) は、ネットワークアドレス変換 (NAT) を使用するネットワークでスタティック ルーティングによりトラフィック クラス ルーティングを制御できるようになりました。また、既存の NAT コマンドに新しいキーワードが追加されました。PfR および NAT 機能が同じルータで設定されていて、PfR がスタティック ルーティングを使用してトラフィック クラスのルーティングを制御する場合、アプリケーションによっては、ドロップされるパケットにより操作が失敗することがあります。このパケット ドロップは、スタティック ルーティングが同じルータからの複数のインターネットサービスプロバイダー (ISP) の接続に使用されている状況で、PfR がスタティック ルーティングを使用してトラフィック クラス ルーティングを制御し、1 つ以上の ISP がセキュリティのためにユニキャスト リバース パス転送 (Unicast RPF) フィルタリングを使用する場合に発生します。NAT に対する PfR サポートの Cisco IOS XE での実装が説明されます。

新しいキーワードが設定されている場合、新しい NAT 変換に、PfR がパケットに選択したインターフェイスのソース IP アドレスが提供され、PfR は、この NAT 変換が作成されたときのインターフェイスを介して、既存のフローを強制的にルーティングします。



(注) Cisco IOS XE Release 3.1S および 3.2S では、境界ルータ専用機能がサポートされます。また、PfR 構文は、Cisco IOS XE Release 3.1S で導入されました。Optimized Edge Routing (OER) 構文を使用して Cisco IOS XE Release 2.6.1 を実行している場合、『[Cisco IOS XE Performance Routing Configuration Guide, Release 2](#)』を参照してください。Cisco IOS XE Release 3.3S 以降のリリースでは、マスター コントローラのサポートが追加されました。

- [機能情報の確認, 2 ページ](#)
- [NAT を使用するパフォーマンス ルーティングの前提条件, 2 ページ](#)
- [NAT を使用したパフォーマンス ルーティングの制約事項, 2 ページ](#)
- [NAT を使用したパフォーマンス ルーティングの概要, 3 ページ](#)
- [NAT を使用したパフォーマンス ルーティングの設定方法, 5 ページ](#)

- [NAT を使用したパフォーマンス ルーティングの設定例, 9 ページ](#)
- [その他の関連資料, 10 ページ](#)
- [NAT を使用したパフォーマンス ルーティングの機能情報, 11 ページ](#)

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

NAT を使用するパフォーマンス ルーティングの前提条件

PfR 境界ルータとして使用する Cisco ASR 1000 シリーズ アグリゲーション サービス ルータは、Cisco IOS XE Release 3.1S 以降のリリースを実行している必要があります。

NAT を使用したパフォーマンス ルーティングの制約事項

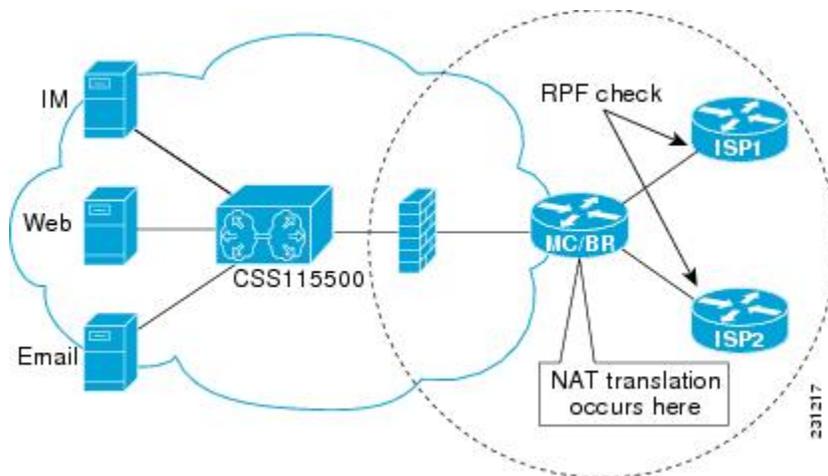
- Cisco IOS XE Release 3.1S 以降のリリースを実行する Cisco ASR 1000 シリーズのアグリゲーション サービス ルータ上では、NAT を使用するネットワーク内で PfR がスタティック ルーティングによってトラフィック クラス ルーティングを制御する機能において、トンネルインターフェイスまたは DMVPN 実装はサポートされません。
- 境界ルータ専用機能は Cisco IOS XE Release 3.1S および 3.2S イメージに含まれます。マスターコントローラ設定は使用できません。Cisco IOS XE Release 3.1S および 3.2S イメージで境界ルータとして使用されている Cisco ASR 1000 シリーズルータと通信するマスターコントローラは、Cisco IOS Release 15.0(1)M またはそれ以降の 15.0M リリースを実行するルータでなければなりません。

NAT を使用したパフォーマンス ルーティングの概要

PfR および NAT

Cisco IOS PfR および NAT 機能が同じルータで設定され、PfR がスタティック ルーティングを使用してトラフィック クラスのルーティングを制御する場合、アプリケーションによっては、ドロップされるパケットにより操作が失敗することがあります。このパケット ドロップは、スタティック ルーティングが同じルータからの複数のインターネット サービス プロバイダー (ISP) の接続に使用されている状況で、PfR がスタティック ルーティングを使用してトラフィック クラスルーティングを制御し、1つ以上の ISP がセキュリティのためにユニキャスト リバース パス転送 (Unicast RPF) フィルタリングを使用する場合に発生します。プライベート IP アドレスからパブリック IP アドレスへの NAT 変換が実行された後で PfR によりトラフィック クラスの発信パケットルートの出口インターフェイスが変更されると、ユニキャスト RPF を実行する入力ルータでパケットがドロップされます。パケットが転送されると、入力ルータ (たとえば、ISP ルータ) のユニキャスト RPF フィルタリングは、NAT により割り当てられるソース IP アドレスプールとは異なるソース IP アドレスを示し、パケットがドロップされます。たとえば、次の図は、NAT を使用した場合の PfR の動作を示しています。

図 1 : NAT を使用した PfR



NAT 変換は、内部ネットワークに接続されているルータで発生します。このルータには、境界ルータまたはマスターコントローラと境界ルータの組み合わせを使用できます。PfR が、ルートを変更してトラフィック クラスパフォーマンスを最適化し、ロードバランシングを実行すると、インターフェイスを介して ISP1 にルーティングされた、上の図の境界ルータからのトラフィックは、トラフィック パフォーマンスが測定され、ポリシーしきい値が適用された後で、インターフェイスを介して ISP2 に再ルーティングされることがあります。RPF チェックは ISP ルータで発生し、ISP2 を介してルーティングされるパケットは、ISP2 の入力ルータでの RPF チェックに失敗します。これは、送信元インターフェイスの IP アドレスが変更されたためです。



(注) 境界ルータ専用機能は Cisco IOS XE Release 2.6、3.1S および 3.2S イメージに含まれます。マスター コントローラ設定は使用できません。境界ルータとして使用する Cisco ASR 1000 シリーズルータと通信するマスター コントローラは、Cisco IOS Release 15.0(1)M またはそれ以降の 15.0M リリースを実行するルータでなければなりません。上の図では、ルータは境界ルータです。マスター コントローラと境界ルータの組み合わせではありません。

このソリューションには、**ip nat inside source** コマンドに対して追加された新しい **oer** キーワードを使用した最小限の設定の変更が含まれています。**oer** キーワードを設定すると、新しい NAT 変換では、パケットに対して PfR が選択したインターフェイスの発信元 IP アドレスが指定され、PfR は NAT 変換が作成されたインターフェイスを介して既存のフローがルーティングされるように強制します。たとえば、PfR は、上の図で ISP1 の InterfaceA と ISP2 の InterfaceB の 2 つのインターフェイスがある境界ルータでトラフィックを管理するように設定されます。PfR は、最初に、Web トラフィックを表すトラフィック クラスを制御するように設定されます。このトラフィックの NAT 変換は、InterfaceA に設定されているパケットのソース IP アドレスにすでに存在します。PfR は、トラフィック パフォーマンスを測定して、InterfaceB が現在トラフィック フローに最適な出口であると判断しますが、既存のフローを変更しません。次に、PfR が E メールトラフィックを表すトラフィック クラスを学習および測定するように設定され、E メールトラフィックが開始されると、NAT 変換が InterfaceB で発生します。PfR スタティック ルーティング NAT ソリューションは、シングルボックス ソリューションであるため、NAT を使用し PfR で管理される複数のルータでのインターフェイスの設定はサポートされていません。NAT、および Cisco IOS ソフトウェアを実行しない PIX ファイアウォールなどのデバイスを使用したネットワーク設定はサポートされていません。

ネットワーク アドレス変換 (NAT)

NAT では、未登録の IP アドレスを使用するプライベート IP インターネットワークがインターネットに接続できます。NAT は、ルータ (通常、2 つのネットワークを接続) で機能し、パケットが別のネットワークに転送される前に、内部ネットワークのプライベート (グローバルに一意ではない) アドレスを有効なアドレスに変換します。NAT は、ネットワーク全体の 1 つだけのアドレスを外部にアドバタイズするように設定できます。この機能により、そのアドレスの後ろに内部ネットワーク全体を効果的に隠すことで、セキュリティが強化されます。

NAT は、エンタープライズエッジでも使用され、内部ユーザのインターネットへのアクセスを許可し、メールサーバなど内部デバイスへのインターネット アクセスを許可します。

NAT の詳細については、『Cisco IOS IP Addressing Services Configuration Guide』の「Configuring NAT for IP Address Conservation」の章を参照してください。

内部グローバルアドレスのオーバーロード

ルータで多くのローカルアドレスに 1 つのグローバルアドレスを使用できるようにすることで、内部グローバルアドレス プールのアドレスを節約できます。このオーバーロードが設定されている場合、ルータは、より高いレベルのプロトコルから十分な情報 (たとえば、TCP または UDP

ポート番号) を保持して、グローバルアドレスを正しいローカルアドレスに戻します。複数のローカルアドレスが1つのグローバルアドレスにマッピングされる場合、各内部ホストの TCP または UDP ポート番号によりローカルアドレスが区別されます。

NAT を使用したパフォーマンス ルーティングの設定方法

NAT を使用するネットワークでスタティックルーティングによりトラフィックを制御するように PfR を設定する

NAT を使用するネットワークでスタティックルーティングによりトラフィックを制御するように PfR を設定するには、次のタスクを実行します。このタスクを行うと、内部ユーザによりインターネットへのアクセスを許可しつつ、PfR がトラフィック クラスを最適化できるようになります。

Cisco IOS PfR および NAT 機能が同じルータで設定され、PfR がスタティック ルーティングを使用してトラフィック クラスのルーティングを制御する場合、アプリケーションによっては、ドロップされるパケットにより操作が失敗することがあります。このパケット ドロップは、スタティック ルーティングが同じルータからの複数のインターネット サービス プロバイダー (ISP) の接続に使用されている状況で、PfR がスタティック ルーティングを使用してトラフィック クラスルーティングを制御し、1つ以上の ISP がセキュリティのためにユニキャスト リバース パス転送 (Unicast RPF) フィルタリングを使用する場合に発生します。

この作業では、**oer** キーワードを **ip nat inside source** コマンドに使用します。**oer** キーワードを設定すると、新しい NAT 変換では、パケットに対して PfR が選択したインターフェイスの発信元 IP アドレスが指定され、PfR は NAT 変換が作成されたインターフェイスを介して既存のフローがルーティングされるように強制します。このタスクでは、1つの IP アドレスを使用していますが、IP アドレス プールを設定することもできます。IP アドレス プールの設定例については、設定例に関する項を参照してください。



(注) この設定は、マスター コントローラ上で実施します。境界ルータ専用機能は Cisco IOS XE Release 3.1S 以降のリリースに含まれます。マスター コントローラ設定は使用できません。境界ルータとして使用する Cisco ASR 1000 シリーズルータと通信するマスター コントローラは、Cisco IOS Release 15.0(1)M またはそれ以降の 15.0M リリースを実行するルータでなければなりません。



(注) PfR スタティック ルーティング NAT ソリューションは、シングルボックス ソリューションであるため、NAT を使用し PfR で管理される複数のルータでのインターフェイスの設定はサポートされていません。

NAT の詳細については、『CiscoIOS IP Addressing Services Configuration Guide』の「[Configuring NAT for IP Address Conservation](#)」の章を参照してください。

NAT を使用するネットワークでスタティック ルーティングによりトラフィックを制御するように PIR を設定する

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**permit** | **deny**} *ip-addressmask*
4. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
5. **match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name*}
6. **match interface** *interface-type interface-number* [...*interface-type interface-number*]
7. **exit**
8. 必要に応じて、ステップ 4～7 を繰り返し、その他のルート マップを設定します。
9. **ip nat inside source** {**list** {*access-list-number* | *access-list-name*} | **route-map** *map-name*} {**interface** *type number* | **pool** *name*} [**mapping-id** *map-id* | **overload** | **reversible** | **vrf** *vrf-name*][**oer**]
10. **interface** *type number*
11. **ip address** *ip-address mask*
12. **ip nat inside**
13. **exit**
14. **interface** *type number*
15. **ip address** *ip-address mask*
16. **ip nat outside**
17. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： <pre>Router> enable</pre>	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"> • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： <pre>Router# configure terminal</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	access-list <i>access-list-number</i> { permit deny } <i>ip-addressmask</i> 例： <pre>Router(config)# access-list 1 permit 10.1.0.0 0.0.255.255</pre>	変換する IP アドレスを許可する標準のアクセスリストを定義します。 <ul style="list-style-type: none"> • アクセスリストは、変換されるアドレスだけを許可する必要があります（各アクセスリストの最後には暗黙的な「deny all」があるので注意してください）。アクセスリストでアドレスを許可しすぎると、予期しない結果になる可能性があります。

	コマンドまたはアクション	目的
ステップ 4	route-map <i>map-tag</i> [permit deny] <i>[sequence-number]</i> 例： <pre>Router(config)# route-map isp-1 permit 10</pre>	ルート マップ コンフィギュレーション モードを開始して、ルート マップを設定します。 <ul style="list-style-type: none"> 例では、BGP という名前のルート マップを作成します。
ステップ 5	match ip address { access-list <i>access-list-name</i> prefix-list <i>prefix-list-name</i> } 例： <pre>Router(config-route-map)# match ip address access-list 1</pre>	NAT により変換されるトラフィックを識別するアクセス リストまたはプレフィックス リスト match 句エントリをルート マップに作成します。 <ul style="list-style-type: none"> 例では、ステップ 3 で作成した、一致基準として 10.1.0.0/24 プレフィックスを指定するアクセス リストを参照します。
ステップ 6	match interface <i>interface-type</i> <i>interface-number</i> [... <i>interface-type</i> <i>interface-number</i>] 例： <pre>Router(config-route-map)# match interface GigabitEthernet 0/0/2</pre>	ルート マップに match 句を作成して、指定されたいずれかのインターフェイスに一致するルート を分散します。 <ul style="list-style-type: none"> 例では、match 句を作成して、ステップ 5 の match 句をシリアルインターフェイス 1/0 経由で通過するルートを配布します。
ステップ 7	exit 例： <pre>Router(config-route-map)# exit</pre>	ルート マップ インターフェイス コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	必要に応じて、ステップ 4～7 を繰り返し、その他のルート マップを設定します。	--
ステップ 9	ip nat inside source { list { <i>access-list-number</i> <i>access-list-name</i> } route-map <i>map-name</i> } { interface <i>type number</i> pool <i>name</i> } [mapping-id <i>map-id</i> overload reversible vrf <i>vrf-name</i>][oer] 例： <pre>Router(config)# ip nat inside source interface GigabitEthernet 1/0/0 overload oer</pre>	インターフェイスを指定して、オーバーロードでのダイナミックな送信元変換を確立します。 <ul style="list-style-type: none"> インターフェイスを指定するには、interface キーワードと、type および number 引数を使用します。 oer キーワードを使用し、PFR が NAT を使用して動作し、スタティック ルーティングでトラフィック クラスを制御するようにします。

NAT を使用するネットワークでスタティック ルーティングによりトラフィックを制御するように PIR を設定する

	コマンドまたはアクション	目的
ステップ 10	interface <i>type number</i> 例 : <pre>Router(config)# interface GigabitEthernet 1/0/0</pre>	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	ip address <i>ip-address mask</i> 例 : <pre>Router(config-if)# ip address 10.114.11.8 255.255.255.0</pre>	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 12	ip nat inside 例 : <pre>Router(config-if)# ip nat inside</pre>	内部と接続されることを示すマークをインターフェイスに付けます。
ステップ 13	exit 例 : <pre>Router(config-if)# exit</pre>	インターフェイス コンフィギュレーション モードを終了して、コンフィギュレーション モードに戻ります。
ステップ 14	interface <i>type number</i> 例 : <pre>Router(config)# interface GigabitEthernet 1/1/0</pre>	別のインターフェイスを指定して、インターフェイス コンフィギュレーション モードに戻ります。
ステップ 15	ip address <i>ip-address mask</i> 例 : <pre>Router(config-if)# ip address 172.17.233.208 255.255.255.0</pre>	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 16	ip nat outside 例 : <pre>Router(config-if)# ip nat outside</pre>	外部と接続されることを示すマークをインターフェイスに付けます。
ステップ 17	end 例 : <pre>Router(config-if)# end</pre>	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

NAT を使用したパフォーマンス ルーティングの設定例

ネットワーク内で NAT を使用してスタティック ルーティングでトラフィックを制御する PfR の設定例

次に、NAT を使用するネットワークで PfR がスタティック ルーティングによりトラフィックを制御できるようにマスター コントローラを設定する例を示します。この例では、NAT 変換の IP アドレスのプールを使用する方法を示します。



- (注) この設定は、マスター コントローラ上で実施します。境界ルータ専用機能は Cisco IOS XE Release 3.1S 以降のリリースに含まれます。マスター コントローラ設定は使用できません。境界ルータとして使用する Cisco ASR 1000 シリーズルータと通信するマスター コントローラは、Cisco IOS Release 15.0(1)M またはそれ以降の 15.0M リリースを実行するルータでなければなりません。

この例では、境界ルータは 2 つの異なる ISP を介してインターネットに接続されています。次の設定では、PfR は、内部ユーザのインターネットへのアクセスを許可しつつ、トラフィック クラスを最適化できます。この例では、NAT を使用して変換されるトラフィック クラスは、アクセス リストおよびルート マップを使用して指定されます。次に、NAT 変換のための IP アドレス プールの使用を設定し、**oer** キーワードを **ip nat inside source** コマンドに追加し、NAT が変換した発信元アドレスであるインターフェイスを介して通過する既存のトラフィック クラスを PfR が維持するように設定します。新しい NAT 変換には、PfR がパケットに選択したインターフェイスの IP アドレスを指定できます。



- (注) PfR スタティック ルーティング NAT ソリューションは、シングルボックス ソリューションであるため、NAT を使用し PfR で管理される複数のルータでのインターフェイスの設定はサポートされていません。

次の例は、Cisco IOS Release 15.0(1)M またはそれ以降の 15.0M リリースを実行するルータに設定できる稼働中のマスター コントローラで設定する必要があります。

```
Router(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Router(config)# route-map isp-2 permit 10BGP permit 10
Router(config-route-map)# match ip address access-list 1
Router(config-route-map)# match interface serial 2/0
Router(config-route-map)# exit
Router(config)# ip nat pool ISP2 209.165.201.1 209.165.201.30 prefix-length 27
Router(config)# ip nat inside source route-map isp-2 pool ISP2 oer
Router(config)# interface FastEthernet 3/0
Router(config-if)# ip address 10.1.11.8 255.255.255.0
Router(config-if)# ip nat inside
```

```

Router(config-if)# exit

Router(config)# interface serial 1/0
Router(config-if)# ip address 192.168.3.1 255.255.255.0
Router(config-if)# ip nat outside
Router(config-if)# exit

Router(config)# interface serial 2/0
Router(config-if)# ip address 172.17.233.208 255.255.255.0
Router(config-if)# ip nat outside
Router(config-if)# end

```

次の例は、Cisco IOS XE Release 3.3S 以降のリリースを実行する Cisco ASR 1000 シリーズ ルータで設定できます。

```

Router(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Router(config)# route-map isp-2 permit 10BGP permit 10
Router(config-route-map)# match ip address access-list 1
Router(config-route-map)# match interface GigabitEthernet 0/0/2
Router(config-route-map)# exit
Router(config)# ip nat pool ISP2 209.165.201.1 209.165.201.30 prefix-length 27
Router(config)# ip nat inside source route-map isp-2 pool ISP2 oer
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.1.11.8 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)# exit

Router(config)# interface GigabitEthernet 0/0/1
Router(config-if)# ip address 192.168.3.1 255.255.255.0
Router(config-if)# ip nat outside
Router(config-if)# exit

Router(config)# interface GigabitEthernet 0/0/2
Router(config-if)# ip address 172.17.233.208 255.255.255.0
Router(config-if)# ip nat outside
Router(config-if)# end

```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco PfR コマンド (コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト、使用上の注意事項、および例)	『Cisco IOS Performance Routing Command Reference』
ベーシック PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール
パフォーマンスルーティングの運用フェーズを理解するために必要な概念	「パフォーマンス ルーティングの理解」モジュール
アドバンスド PfR の設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール

関連項目	マニュアル タイトル
IP SLA の概要	『 <i>IP SLAs Configuration Guide</i> 』
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホーム ページ	PfR:Home

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンラインリソースを提供しています。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

NAT を使用したパフォーマンス ルーティングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

表 1: NAT を使用したパフォーマンス ルーティングの機能情報

機能名	リリース	機能情報
NAT およびスタティック ルーティングのサポート ¹	Cisco IOS XE Release 2.6.1、 Cisco IOS XE Release 3.1S、 Cisco IOS XE Release 3.3S	<p>NAT を使用するネットワークでスタティック ルーティングを使用してトラフィック クラス ルーティングを制御するように PfR を許可できます。</p> <p>この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。</p> <p>PfR 構文は、Cisco IOS XE Release 3.1S で導入されました。</p> <p>(注) Cisco IOS XE Release 3.3S では、マスターコントローラのサポートが導入されました。</p> <p>この機能により、次のコマンドが変更されました。 ip nat inside source。</p>

¹ これはマイナーな拡張です。マイナーな拡張は、通常 Feature Navigator に記載されません。