グローバル テーブルから VRF テーブルへの IP プレフィクスのインポートに対する BGP サポート

グローバル テーブルから VRF テーブルへの IP プレフィクスのインポートに対する BGP サポート機能により、インポート ルート マップを使用して、IPv4 ユニキャスト プレフィクスをグローバル ルーティング テーブルから Virtual Private Network（VPN; バーチャル プライベート ネットワーク）routing/forwarding（VRF; VPN ルーティング/転送）インスタンス テーブルにインポートする機能が追加されます。

このモジュール内の機能情報の検索

ご使用の Cisco IOS ソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。最新の機能情報および警告については、ご使用のプラットフォームおよびソフトウェア リリースのリリースノートを参照してください。このモジュール内に記載されている特定の機能のリンクにアクセスする場合、および各機能がサポートされているリリースのリストを参照する場合は、「グローバル テーブルから VRF テーブルへの IP プレフィクス インポートに対する BGP サポートの機能情報」（P.14）を参照してください。

プラットフォームと、Cisco IOS および Catalyst OS ソフトウェア イメージに関するサポート情報の検索

プラットフォームのサポートと、Cisco IOS および Catalyst OS 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、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

マニュアルの内容

グローバル テーブルから VRF テーブルへの IP プレフィクス インポートに対する BGP サポートの前提条件

- Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）ピアリング セッションが確立されている必要があります。
- （分散プラットフォーム用の）CEF または dCEF が、参加しているすべてのルータでイネーブルになっている必要があります。

グローバル テーブルから VRF テーブルへの IP プレフィクス インポートに対する BGP サポートの制限事項

- この機能で VRF にインポートできるのは、IPv4 ユニキャストおよびマルチキャストのプレフィクスだけです。
- グローバル ルーティング テーブルから IPv4 プレフィクスをインポートするために、ルータごとに最大 5 つの VRF インスタンスを作成できます。
- この機能を使用して VRF にインポートされた IPv4 プレフィクスは、VPNv4 VRF にインポートできません。

グローバル テーブルから VRF テーブルへの IP プレフィクスのインポートに対する BGP サポートに関する情報

IPv4 プレフィクスから VRF へのインポート

グローバル テーブルから VRF テーブルへの IP プレフィクスのインポートに対する BGP サポート機能により、インポート ルート マップを使用して、IPv4 ユニキャスト プレフィクスをグローバル ルーティング テーブルからバーチャル プライベート ネットワーク（VPN）ルーティング/転送（VRF）インスタンス テーブルにインポートする機能が追加されます。この機能により VRF インポート マップ設定の機能が拡張され、標準コミュニティに基づいて IPv4 プレフィクスを VRF にインポートできるよ

うになります。IPv4 ユニキャスト プレフィクスおよび IPv4 マルチキャスト プレフィクスの両方がサポートされています。Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）またはルート ターゲット（インポートまたはエクスポート）コンフィギュレーションは不要です。

IP プレフィクスは、標準の Cisco IOS フィルタリング メカニズムでインポート マップの一致基準として定義されます。たとえば、IP アクセス リスト、IP プレフィクス リスト、または IP as-path フィルタを作成して IP プレフィクスまたは IP プレフィクス範囲を定義した後、ルート マップ内で 1 つ以上のプレフィクスに match 句の処理が行われます。ルート マップを通過するプレフィクスは、インポート マップ コンフィギュレーションごとに指定された VRF にインポートされます。

ブラック ホール ルーティング

この機能は、Black Hole Routing（BHR; ブラック ホール ルーティング）をサポートするために設定できます。BHR は、管理者が、トラフィックをデッド インターフェイスや調査用の情報を収集するように設計されたホストにダイナミック ルーティングを行い、ネットワークへの攻撃の影響を軽減することによって、不正な送信元からのトラフィックや Denial of Service（DoS; サービス拒絶）攻撃により生成されたトラフィックなどの望ましくないトラフィックをブロックできる方法です。プレフィクスが検索され、許可されていない送信元から届いたパケットが ASIC によってライン レートでブラック ホール化されます。

グローバル トラフィックの分類

この機能を使用すると、物理的な位置またはサービスのクラスに基づいてグローバル IP トラフィックを分類できます。トラフィックは、管理ポリシーに基づいて分類された後、異なる VRF にインポートされます。たとえば、大学のキャンパスでは、ネットワーク トラフィックは、大学ネットワークと寄宿舎ネットワークのトラフィック、学生ネットワークと学部ネットワーク、またはマルチキャスト トラフィック専用のネットワークに分割できます。管理ポリシーに従ってトラフィックが分割された後、ルーティング決定は、ポリシーベース ルーティングを使用した MPLS VPN-VRF 選択機能、または送信元 IP アドレスに基づく MPLS VPN-VRF 選択機能で設定できます。

グローバル テーブルから VRF テーブルへの IP プレフィクスのインポート方法

ここでは、次の作業について説明します。

インポートする IPv4 IP プレフィクスの定義

IPv4 ユニキャストまたは IPv4 マルチキャストのプレフィクスは、標準の Cisco IOS フィルタリング メカニズムを使用して、インポート ルート マップの一致基準として定義されます。この作業では、IP アクセス リストおよび IP プレフィクス リストを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]
4. **ip prefix-list** *prefix-list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*]

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	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** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**] **例：** `Router(config)# access-list 50 permit 10.1.1.0 0.0.0.255`	アクセス リストを作成して、VRF テーブルにインポートする IP プレフィクスの範囲を定義します。 • この例では、50 の番号が付けられた標準アクセス リストを作成しています。このフィルタは、10.1.1.0/24 サブネット内の IP アドレスを持つホストからのトラフィックを許可します。
ステップ 4	**ip prefix-list** *prefix-list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*] **例：** `Router(config)# ip prefix-list COLORADO permit 10.24.240.0/22`	プレフィクス リストを作成して、VRF テーブルにインポートする IP プレフィクスの範囲を定義します。 • この例では、COLORADO という名前の IP プレフィクス リストを作成しています。このフィルタは、10.24.240.0/22 サブネット内の IP アドレスを持つホストからのトラフィックを許可します。

VRF およびインポート ルート マップの作成

インポートに対して定義された IP プレフィクスは、その後、ルート マップ内で match 句の処理が行われます。ルート マップを通過する IP プレフィクスは、VRF にインポートされます。グローバル ルーティング テーブルから IPv4 プレフィクスをインポートするために、ルータごとに最大 5 つの VRF を設定できます。デフォルトでは、VRF ごとに 1000 のプレフィクスがインポートされます。各 VRF に対して、1 ～ 2,147,483,647 のプレフィクスを手動で設定できます。プレフィクス インポートの制限を手動で設定する場合は、注意してください。ルータが過剰な量のプレフィクスをインポートするように設定すると、正常なルータの正常な動作が中断する場合があります。

MPLS コンフィギュレーションもルート ターゲット（インポートまたはエクスポート）コンフィギュレーションも必要ありません。

インポート アクション

インポート アクションは、新しいルーティング アップデートが受信されたとき、またはルートが除去されたときにトリガーされます。最初の BGP アップデート期間中は、BGP がコンバージェンスをより迅速に実行できるように、インポート アクションが延期されます。BGP がコンバージェンスを実行すると、インクリメンタル BGP アップデートがただちに評価されて、認定されたプレフィクスが受信と同時にインポートされます。

新しい syslog メッセージ

この機能によって、次の syslog メッセージが追加されています。このメッセージは、ユーザ定義の制限よりも多くのプレフィクスがインポートで使用できる場合に表示されます。

```
00:00:33: %BGP-3-AFIMPORT_EXCEED: IPv4 Multicast prefixes imported to multicast vrf exceed
the limit 2
```

プレフィクス制限を増やすか、またはインポート ルート マップ フィルタを微調整すると、候補ルートの数を削減できます。

制約事項

- この機能で VRF にインポートできるのは、IPv4 ユニキャストおよびマルチキャストのプレフィクスだけです。
- グローバル ルーティング テーブルから IPv4 プレフィクスをインポートするために、ルータごとに最大 5 つの VRF インスタンスを作成できます。
- この機能を使用して VRF にインポートされた IPv4 プレフィクスは、VPNv4 VRF にインポートできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **import ipv4** {**unicast** | **multicast**} [*prefix-limit*] **map** *route-map*
6. **exit**
7. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
8. **match ip address** {*acl-number* [*acl-number* | *acl-name*] | *acl-name* [*acl-name* | *acl-number*] | **prefix-list** *prefix-list-name* [*prefix-list-name*]}
9. **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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	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	**ip vrf** *vrf-name* **例：** `Router(config)# ip vrf GREEN`	VRF ルーティング テーブルを作成し、VRF の名前（またはタグ）を指定します。 • **ip vrf** *vrf-name* コマンドは VRF ルーティング テーブルおよび CEF テーブルを作成し、その両方のテーブルに、*vrf-name* 引数を使用して名前が付けられます。この両方のテーブルには、デフォルトのルート識別子の値が関連付けられています。
ステップ 4	**rd** *route-distinguisher* **例：** `Router(config-vrf)# rd 100:10`	VRF インスタンスのためのルーティング テーブルおよびフォワーディング テーブルを作成します。 • ルート識別子の引数を設定するには、2 つの形式があります。例で示されているような as-number:network number（ASN:nn）の形式、または IP address:network number（IP-address:nn）の形式で設定できます。
ステップ 5	**import ipv4** {**unicast** | **multicast**} *[prefix-limit]* **map** *route-map* **例：** `Router(config-vrf)# import ipv4 unicast 1000 map UNICAST`	インポート マップを作成し、グローバル ルーティング テーブルから IPv4 プレフィクスを VRF テーブルにインポートします。 • ユニキャスト プレフィクスまたはマルチキャスト プレフィクスを指定します。 • デフォルトでは、最大 1000 のプレフィクスがインポートされます。1 ～ 2,147,483,647 のプレフィクスの制限を指定するには、*prefix-limit* 引数を使用します。 • インポートするプレフィクスを定義するルート マップは、**map** キーワードの入力後に指定されます。 • この例では、UNICAST という名前のルート マップを通過する最大 1000 のユニキャスト プレフィクスをインポートするインポート マップを作成しています。
ステップ 6	**exit** **例：** `Router(config-vrf)# exit`	VRF 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 モードを開始します。

	コマンドまたはアクション	目的
ステップ 7	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **例：** `Router(config)# route-map UNICAST permit 10`	ルートを、あるルーティング プロトコルから別のルーティング プロトコルに再配布する条件を定義したり、ポリシー ルーティングをイネーブルにしたりします。 • ルート マップ名は、ステップ 5 で指定されたルート マップと一致する必要があります。 • この例では、UNICAST という名前のルート マップを作成しています。
ステップ 8	**match ip address** {*acl-number* [*acl-number* | *acl-name*] | *acl-name* [*acl-name* | *acl-number*] | **prefix-list** *prefix-list-name* [*prefix-list-name*]} **例：** `Router(config-route-map)# match ip address 50`	標準アクセス リストまたは拡張アクセス リストで宛先ネットワーク番号のアドレスが許可されているルートを配布し、一致したパケットのポリシー ルーティングを行います。 • IP アクセス リストと IP プレフィクス リストの両方がサポートされています。 • この例では、標準アクセス リスト 50 を使用して一致基準を定義するようにルート マップを定義しています。
ステップ 9	**end** **例：** `Router(config-route-map)# end`	現在のルート マップ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

入力インターフェイスのフィルタリング

この機能は、グローバルに、またはインターフェイス単位で設定できます。性能を最大限に高めるために、この機能を入力インターフェイスだけに適用することを推奨します。

ユニキャスト Reverse Path Forwarding（ユニキャスト RPF）

ユニキャスト Reverse Path Forwarding（ユニキャスト RPF）は任意に設定できます。ユニキャスト RPF は、送信元アドレスが Forwarding Information Base（FIB; 転送情報ベース）内にあることを確認するために使用されます。**ip verify unicast vrf** コマンドはインターフェイス コンフィギュレーション モードで設定され、各 VRF でイネーブルにされます。このコマンドには、ユニキャスト RPF 確認の後にトラフィックが転送されるかドロップされるかを判断するために使用される **permit** キーワードおよび **deny** キーワードがあります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip policy route-map** *map-tag*
5. **ip verify unicast vrf** *vrf-name* {**deny** | **permit**}
6. **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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	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	**interface** *type number* [*name-tag*] **例：** `Router(config)# interface Ethernet0/0`	インターフェイスを設定し、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 4	**ip policy route-map** *map-tag* **例：** `Router(config-if)# ip policy route-map UNICAST`	インターフェイスでのポリシー ルーティングに使用するルート マップを識別します。 • 設定例では、UNICAST という名前のルート マップをインターフェイスに接続しています。
ステップ 5	**ip verify unicast vrf** *vrf-name* {**deny** | **permit**} **例：** `Router(config-if)# ip verify unicast vrf GREEN permit`	（任意）指定された VRF のユニキャスト Reverse Path Forwarding の確認をイネーブルにします。 • この例では、GREEN という名前の VRF の確認をイネーブルにしています。確認を通過したトラフィックは転送されます。
ステップ 6	**end** **例：** `Router(config-if)# end`	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。

グローバル IP プレフィクス インポートの確認

次の作業の手順を実行すると、この機能で設定された VRF に関する情報が表示され、指定された VRF テーブルにグローバル IP プレフィクスがインポートされていることを確認できます。

手順の概要

1. **enable**
2. **show ip bgp vpnv4** {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*}
3. **show ip vrf** [**brief** | **detail** | **interfaces** | **id**] [*vrf-name*]

手順の詳細

ステップ 1　enable

特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。

```
Router# enable
```

ステップ 2 **show ip bgp vpnv4** {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*}

VPN アドレス情報を BGP テーブルから表示します。出力には、インポート ルート マップ、トラフィック タイプ（ユニキャストまたはマルチキャスト）、デフォルトまたはユーザ定義のプレフィクス インポート制限、インポートされた実際のプレフィクスの数、および個別のインポート プレフィクス エントリが表示されます。

```
Router# show ip bgp vpnv4 all

BGP table version is 15, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf academic)
Import Map: ACADEMIC, Address-Family: IPv4 Unicast, Pfx Count/Limit: 6/1000
*> 10.50.1.0/24     172.17.2.2                             0 2 3 ?
*> 10.50.2.0/24     172.17.2.2                             0 2 3 ?
*> 10.50.3.0/24     172.17.2.2                             0 2 3 ?
*> 10.60.1.0/24     172.17.2.2                             0 2 3 ?
*> 10.60.2.0/24     172.17.2.2                             0 2 3 ?
*> 10.60.3.0/24     172.17.2.2                             0 2 3 ?
Route Distinguisher: 200:1 (default for vrf residence)
Import Map: RESIDENCE, Address-Family: IPv4 Unicast, Pfx Count/Limit: 3/1000
*> 10.30.1.0/24     172.17.2.2                  0          0 2 i
*> 10.30.2.0/24     172.17.2.2                  0          0 2 i
*> 10.30.3.0/24     172.17.2.2                  0          0 2 i
Route Distinguisher: 300:1 (default for vrf BLACKHOLE)
Import Map: BLACKHOLE, Address-Family: IPv4 Unicast, Pfx Count/Limit: 3/1000
*> 10.40.1.0/24     172.17.2.2                  0          0 2 i
*> 10.40.2.0/24     172.17.2.2                  0          0 2 i
*> 10.40.3.0/24     172.17.2.2                  0          0 2 i
Route Distinguisher: 400:1 (default for vrf multicast)
Import Map: MCAST, Address-Family: IPv4 Multicast, Pfx Count/Limit: 2/2
*> 10.70.1.0/24     172.17.2.2                  0          0 2 i
*> 10.70.2.0/24     172.17.2.2                  0          0 2 i
```

ステップ 3 **show ip vrf** [**brief** | **detail** | **interfaces** | **id**] [*vrf-name*]

定義された VRF、および関連付けられたインターフェイスを表示します。出力には、インポート ルート マップ、トラフィック タイプ（ユニキャストまたはマルチキャスト）、およびデフォルトまたはユーザ定義のプレフィクス インポート リミットが表示されています。次の例では、UNICAST という名前のインポート ルート マップが IPv4 ユニキャスト プレフィクスをインポートしており、プレフィクス インポート リミットが 1000 であることを示します。

```
Router# show ip vrf detail

VRF academic; default RD 100:10; default VPNID <not set>
VRF Table ID = 1
  No interfaces
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:10
  Import VPN route-target communities
    RT:100:10
  Import route-map for ipv4 unicast: UNICAST (prefix limit: 1000)

  No export route-map
```

グローバル テーブルから VRF テーブルへの IP プレフィクス インポートに対する BGP サポートの設定例

ここでは、次の設定例について説明します。

グローバル IP プレフィクス インポートの設定：例

次に、IP プレフィクス リストとルート マップを使用して、ユニキャスト プレフィクスを、*green* という名前の VRF にインポートする例を示します。

この例は、グローバル コンフィギュレーション モードで開始します。

```
!
ip prefix-list COLORADO seq 5 permit 10.131.64.0/19
ip prefix-list COLORADO seq 10 permit 172.31.2.0/30
ip prefix-list COLORADO seq 15 permit 172.31.1.1/32
!
ip vrf green
 rd 200:1
 import ipv4 unicast map UNICAST
 route-target export 200:10
 route-target import 200:10
!
 exit
!
route-map UNICAST permit 10
 match ip address prefix-list COLORADO
!
 exit
```

グローバル IP プレフィクス インポートの確認：例

show ip vrf コマンドまたは **show ip bgp vpnv4** コマンドを使用すると、プレフィクスがグローバル ルーティング テーブルから VRF テーブルにインポートされていることを確認できます。

次の例は **show ip vrf** コマンドの出力であり、UNICAST という名前のインポート ルート マップが IPv4 ユニキャストをインポートしており、プレフィクス インポート リミットが 1000 であることを示します。

```
Router# show ip vrf detail

VRF green; default RD 200:1; default VPNID <not set>
  Interfaces:
    Se2/0
VRF Table ID = 1
  Export VPN route-target communities
    RT:200:10
  Import VPN route-target communities
    RT:200:10
  Import route-map for ipv4 unicast: UNICAST (prefix limit: 1000)
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
```

```
VRF red; default RD 200:2; default VPNID <not set>
  Interfaces:
    Se3/0
VRF Table ID = 2
  Export VPN route-target communities
    RT:200:20
  Import VPN route-target communities
    RT:200:20
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
```

次の例は **show ip bgp vpnv4** コマンドの出力であり、インポート ルート マップ名、プレフィクス インポート制限、インポートされたプレフィクスの実際の数、および個別のインポート エントリを示します。

```
Router# show ip bgp vpnv4 all

BGP table version is 18, local router ID is 10.131.127.252
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 200:1 (default for vrf green)
Import Map: UNICAST, Address-Family: IPv4 Unicast, Pfx Count/Limit: 1/1000
*>i10.131.64.0/19   10.131.95.252            0    100      0 i
*> 172.16.1.1/32    172.16.2.1               0         32768 i
*> 172.16.2.0/30    0.0.0.0                  0         32768 i
*>i172.31.1.1/32    10.131.95.252            0    100      0 i
*>i172.31.2.0/30    10.131.95.252            0    100      0 i
Route Distinguisher: 200:2 (default for vrf red)
*> 172.16.1.1/32    172.16.2.1               0         32768 i
*> 172.16.2.0/30    0.0.0.0                  0         32768 i
*>i172.31.1.1/32    10.131.95.252            0    100      0 i
*>i172.31.2.0/30    10.131.95.252            0    100      0 i
```

参考資料

次の項では、グローバル テーブルから VRF テーブルへの IP プレフィクスのインポートに対する BGP サポート機能に関連する参照資料について説明します。

関連資料

関連項目	参照先
BGP コマンド：コマンド構文の詳細、デフォルト、コマンド モード、コマンド履歴、使用上の注意事項、および例	『*Cisco IOS IP Routing: BGP Command Reference*』
BGP 機能のロードマップと、機能およびコンフィギュレーション モジュールへのリンク	『BGP Features Roadmap』
MPLS レイヤ 3 VPN の設定作業	『Configuring MPLS Layer 3 VPNs』
ポリシーベース ルーティングを使用した VRF 選択	『Directing MPLS VPN Traffic Using Policy-Based Routing』
送信元 IP アドレスに基づく VRF の選択	『MPLS VPN— VRF Selection Based on Source IP Address』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能で変更された既存規格のサポートはありません。	—

MIB

MIB	MIB リンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存の MIB のサポートはありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能による新規または変更された RFC のサポートはありません。また、この機能による既存の RFC サポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/en/US/support/index.html

コマンド リファレンス

このモジュールに記載されている 1 つ以上の機能で、次のコマンドが追加または変更されています。これらのコマンドについては、http://www.cisco.com/en/US/docs/ios/iproute_bgp/command/reference/irg_book.html の『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。すべての Cisco IOS コマンドについては、http://tools.cisco.com/Support/CLILookup にアクセスしてコマンド検索ツールを使用するか、『*Cisco IOS Master Commands List*』を参照してください。

- **debug ip bgp import**
- **import ipv4**
- **ip verify unicast vrf**

グローバル テーブルから VRF テーブルへの IP プレフィクス インポートに対する BGP サポートの機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースでは、一部のコマンドが使用できない場合があります。特定のコマンドのリリース情報については、コマンド リファレンス マニュアル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 を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS と Catalyst OS のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　グローバル テーブルから VRF テーブルへの IP プレフィクス インポートに対する BGP サポートの機能情報

機能名	リリース	機能情報
グローバル テーブルから VRF テーブルへの IP プレフィクスのインポートに対する BGP サポート	12.0(29)S 12.2(25)S 12.2(27)SBC 12.2(33)SRA 12.2(33)SXH 12.3(14)T 15.0(1)S	グローバル テーブルから VRF テーブルへの IP プレフィクスのインポートに対する BGP サポート機能により、インポート ルート マップを使用して、IPv4 ユニキャスト プレフィクスをグローバル ルーティング テーブルからバーチャル プライベート ネットワーク（VPN）ルーティング/転送（VRF）インスタンス テーブルにインポートする機能が追加されます。 この機能によって、**debug ip bgp import**、**import ipv4**、**ip verify unicast vrf** の各コマンドが追加または変更されています。