グローバル テーブルから VRF テーブルへの IP プレフィッ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 プレフィッ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 プレフィックスをグローバル ルーティング テーブルから 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。

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。最新の機能情報および警告については、「Bug Search Tool」および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、このモジュー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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

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

- ボーダー ゲートウェイ プロトコル（BGP）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有効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 プレフィックス 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ックスだけです。
- グローバル ルーティング テーブルから IPv4 プレフィッ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 プレフィックスは、VPNv4 VRF にインポートできません。
- グローバル プレフィックスは、この機能で BGP VRF テーブルにインポートできるように、BGP テーブル内にある必要があります。
- この機能を使用して VRF にインポートされた IPv4 プレフィックスは、2 番目の VPNv4 VRF には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 プレフィックスのインポートに対する BGP サポートに関する情報

IPv4 プレフィックスから 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 プレフィッ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 プレフィックスをグローバル 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 プレフィックスを VRF にインポートできるようになります。IPv4 ユニキャスト プレフィックスおよび IPv4 マルチキャスト プレフィックスの両方がサポートされています。マルチプロトコル ラベル スイッチング（MPLS）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 プレフィックスは、標準のシスコ 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 プレフィックス リスト、または IP as-path フィルタを作成して IP プレフィックスまたは IP プレフィックス範囲を定義した後、ルート マップ内で 1 つ以上のプレフィックスに 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ックスは、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

グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポート機能は、ブラック ホール ルーティング（BHR）をサポートするように設定できます。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サービス妨害（DoS）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。プレフィックスが検索され、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

グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポート機能は、実際の位置またはサービス クラスに基づいてグローバル IP トラフィックを分類するために使用できます。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。

ユニキャスト リバース パス フォワーディング

ユニキャスト リバース パス転送（ユニキャスト RPF）は、グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポートを使用して任意で設定できます。ユニキャスト RPF は、送信元アドレスが転送情報ベース（FIB）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 で有効化されます。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。

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

インポートする IPv4 IP プレフィックスの定義

IPv4 ユニキャストまたは IPv4 マルチキャストのプレフィックスは、標準のシスコ 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 プレフィックス 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： `Device> enable`	特権 EXEC モードを有効にします。 • 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： `Device# 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。

	コマンドまたはアクション	目的
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**] 例： `Device(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 プレフィッ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： `Device(config)# ip prefix-list COLORADO permit 10.24.240.0/22`	プレフィックス リストを作成して、VRF テーブルにインポートする IP プレフィックスの範囲を定義します。 • この例では、COLORADO という名前の IP プレフィックス 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 プレフィックスは、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 プレフィックスは、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 プレフィッ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 あたり最大 1000 プレフィックスをインポートできます。この制限は、VRF ごとに 1 ～ 2,147,483,647 プレフィックスの範囲で変更できます。プレフィックス インポート制限を 1000 よりも大きく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ッ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ックスが受信と同時にインポートされます。

次の syslog メッセージが、グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポート機能で導入されました。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ッ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
```

プレフィッ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。

（注）
- 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ックスだけです。
- グローバル ルーティング テーブルから IPv4 プレフィッ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 プレフィックスは、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 モードを有効にします。 • 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： `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

	コマンドまたはアクション	目的
		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`	IPv4 プレフィックスを、指定したルート マップでフィルタ処理して、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します。 • ユニキャスト プレフィックスまたはマルチキャスト プレフィックスを指定します。 • デフォルトでは、最大 1000 のプレフィックスがインポートされます。1 ～ 2,147,483,647 のプレフィックスの制限を指定するには、*prefix-limit* 引数を使用します。 • この例では、通過した最大 1000 のユニキャスト プレフィックスをインポートするルート マップを参照しています。
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。
ステップ 7	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] 例： `Router(config)# route-map UNICAST permit 10`	あるルーティング プロトコルから別のルーティング プロトコルへルートを再配布する条件を定義するか、ポリシー ルーティングをイネーブルにします。 • 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*]}	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

	コマンドまたはアクション	目的
	例： `Router(config-route-map)# match ip address 50`	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 プレフィックス 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

グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポート機能は、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。

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 モードを有効にします。 • 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： `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。

	コマンドまたはアクション	目的
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ポリシー ルーティングに使用するルート マップを特定します。 • この例では、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 プレフィックス インポートの確認

グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポート機能で設定された VRF に関する情報を表示し、指定した VRF テーブルにグローバル IP プレフィックスがインポートされていることを確認するには、次の手順を実行します。

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 モードを有効にします。パスワードを入力します（要求された場合）。

例：

```
Device# 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ックス インポート制限、インポートされた実際のプレフィックスの数、および個別のインポート プレフィックス エントリが表示されます。

例：

```
Device# 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ックス 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 プレフィックスをインポートしており、プレフィックス インポート リミットが 1000 であることを示します。

例：

```
Device# 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 プレフィックス インポートに対する BGP サポートの設定例

例：グローバル テーブルから VRF テーブルへの IP プレフィックスのインポート

次に、IP プレフィックス リストとルート マップを使用して、ユニキャスト プレフィックスを、*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
```

例：VRF テーブルへの IP プレフィックス インポートの確認

show ip vrf コマンドまたは **show ip bgp vpnv4** コマンドを使用すると、プレフィックスがグローバル 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。

次の出力例では、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 プレフィックスをインポートしており、プレフィックス インポート制限が 1000 であることを示します。

```
Device# 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
```

次の出力例は、インポート ルート マップ名、プレフィックス インポート制限、インポートされたプレフィックスの実際の数、および個別のインポート エントリを示します。

```
Device# 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
```

内部 BGP 機能に関する追加情報

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 Commands List, All Releases』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』
BGP の概要	「Cisco BGP 概要」モジュール
基本的な BGP 設定作業	「基本 BGP ネットワークの設定」モジュール

関連項目	マニュアル タイトル
iBGP のマルチパス ロード シェアリング	「iBGP マルチパス ロード シェアリング」モジュール
サービス プロバイダーへの接続	「外部 BGP を使用したサービス プロバイダーとの接続」モジュール
複数の IP ルーティング プロトコルに適用する機能の設定	『*IP Routing: Protocol-Independent Configuration Guide*』

RFC

RFC	タイトル
RFC 1772	『*Application of the Border Gateway Protocol in the Internet*』
RFC 1773	『*Experience with the BGP Protocol*』
RFC 1774	『*BGP-4 Protocol Analysis*』
RFC 1930	『*Guidelines for Creation, Selection, and Registration of an Autonomous System (AS)*』
RFC 2519	『*A Framework for Inter-Domain Route Aggregation*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』
RFC 2918	『*Route Refresh Capability for BGP-4*』
RFC 3392	『*Capabilities Advertisement with BGP-4*』
RFC 4271	『*A Border Gateway Protocol 4 (BGP-4)*』
RFC 4893	『*BGP Support for Four-octet AS Number Space*』
RFC 5396	『*Textual Representation of Autonomous system (AS) Numbers*』
RFC 5398	『*Autonomous System (AS) Number Reservation for Documentation Use*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

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

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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1:* グローバル テーブルから *VRF* テーブルへの *IP* プレフィックス 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 プレフィックスのインポートに対する BGP サポート	Cisco IOS XE Release 2.1	グローバル テーブルから VRF テーブルへの IP プレフィッ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 プレフィックスをグローバル ルーティング テーブルから 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。 この機能により、次のコマンドが導入または変更されました。**debug ip bgp import**、**import ipv4**、**ip verify unicast vrf**