BGP イベントベース VPN インポート

BGP イベントベース VPN インポート機能は、既存のボーダー ゲートウェイ プロトコル（BGP）パスのインポート プロセスに変更を加えるものです。拡張 BGP パス インポートはイベントの発生時に実行されます。BGP パスが変更されると、インポートされたコピーすべてのアップデートも、処理が可能になるとすぐに実行されます。ソフトウェアがアップデート処理前に定期的なスキャナ時間まで待つことに起因するルートの伝播の遅延もなくなるため、コンバージェンス時間が大幅に短縮されます。新しい処理の実装用に、新たなコマンドライン インターフェイス（CLI）が導入されています。

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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「BGP イベントベース VPN インポートの機能情報」（P.12）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 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 からアクセスします。Cisco.com のアカウントは必要ありません。

内容

BGP イベントベース VPN インポートの前提条件

関係するルータすべてで、シスコ エクスプレス フォワーディングまたは分散シスコ エクスプレス フォワーディングがイネーブルになっている必要があります。

BGP イベントベース VPN インポートの概要

BGP イベントベース VPN インポート

BGP イベントベース VPN インポート機能は、既存の BGP パスのインポート プロセスに変更を加えるものです。BGP バーチャル プライベート ネットワーク（VPN）インポートは、BGP パスが BGP VPN テーブルから BGP Virtual Routing and Forwarding（VRF; VPN ルーティング/転送）トポロジへインポートされる場合に、インポート機能を提供するものです。既存のパス インポート プロセスでは、パスにアップデートが発生すると、次のスキャン時間の間にインポート アップデート処理が行われ、スキャンの間隔は 5 ～ 15 秒の間で設定されています。スキャン時間のために、ルートの伝播に遅延が発生します。拡張 BGP パス インポートはイベントの発生時に実行されます。BGP パスが変更されると、インポートされたコピーすべてのアップデートも、処理が可能になるとすぐに実行されます。

BGP イベントベース VPN インポート機能を使用すると、プロバイダー エッジ（PE）ルータは VPN パスをカスタマー エッジ（CE）ルータへとスキャン時間の遅延なしに伝播できるため、コンバージェンス時間は大幅に短縮されます。インポートされたルート ターゲットを VRF に追加するといった設定変更は即時処理されず、これまでどおり 60 秒ごとの定期的なスキャナ通過の間に処理されます。

インポート パス選択ポリシー

イベントベース VPN インポートには、3 種類のパス選択ポリシーが準備されています。

- すべて：インポートする VRF インスタンスに関連付けられた Route Target（RT; ルート ターゲット）のいずれかに一致するエクスポート側ネットから、使用できるパスすべてをインポートします。
- 最良パス：VRF インスタンスの RT に一致する、最適使用可能パスをインポートします。エクスポート側ネット内の最良パスが VRF インスタンスの RT に一致しない場合、VRF インスタンスの RT に一致する、最適使用可能パスがインポートされます。
- マルチパス：VRF インスタンスの RT に一致する、最良パスおよびマルチパスとマークされたすべてのパスをインポートします。一致する最良パスやマルチパスがない場合、最適使用可能パスが選択されます。

マルチパスおよび最良パス オプションは、設定されたオプションでのみ選択されるよう、オプションのキーワードを使用して制限することができます。**strict** キーワードを設定すると、最適使用可能パス選択のフォール バック安全性オプションがソフトウェアによりディセーブルになります。エクスポート側ネットに VRF インスタンスの RT に一致する設定されたオプション（最良パスまたはマルチパス）に適したパスがない場合、どのパスもインポートされません。この動作は、BGP イベントベース VPN インポート機能導入前の動作と一致しています。

制限が設定されない場合、最適使用可能パスとしてインポートされるパスはタグ付きになります。**show** コマンド出力では、これらのパスが「imported safety path」という言い方で識別されます。

VRF インスタンスへインポートされると見なされるエクスポート側ネットの既存のパスは、別のピアルータから受信したものであるために VPN インポートのルールが適用されていない場合があります。ルート識別子（RD）情報はルータに対してローカルなため、これらのパスには同一の RD 情報が含ま

れていることがあります。しかし、これらのパスの一部は、インポートする VRF インスタンスの RT と一致しないため、**show** コマンドの出力では「not-in-vrf」とマークされます。VRF にないパスは VRF にあるパスよりも優先度が低く見えるため、「not-in-vrf」とマークされたどのパスも、最良パスと見なされることはありません。

インポート パスの制限

メモリ利用を制御するため、エクスポート側ネットからインポートされるパスの最大数の制限をインポート側ネットごとに指定できます。インポートされるパスが 1 つ以上のエクスポート側ネットから選択される場合、最も優先的に選択されるのは最良パス、次に優先的に選択されるのがマルチパスとなり、非マルチパスの優先度が最も低くなります。

BGP イベントベース VPN インポートの設定方法

マルチプロトコル VRF の設定

マルチプロトコル VRF を使用して、ルート ターゲット ポリシー（インポートおよびエクスポート）を IPv4 と IPv6 との間で共有したり、IPv4 VPN と IPv6 VPN に別々のルート ターゲット ポリシーを設定したりすることができます。使用するよう設定するには、この作業を実行します。この作業では、IPv4 アドレス ファミリだけを設定しますが、新しい VRF 設定すべてにマルチプロトコル VRF を使用することを推奨します。

（注） この作業は、BGP イベントベース VPN インポート機能特有のものではありません。

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
6. **address-family ipv4** [**unicast**]
7. **exit-address-family**
8. **exit**
9. **interface** *type number*
10. **vrf forwarding** *vrf-name*
11. **ip address** *ip-address mask*
12. **no shutdown**
13. **exit**

14. 他のインターフェイス付き VRF インスタンスを作成しバインドするには、ステップ 3 から ステップ 13 までを繰り返します。
15. **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	**vrf definition** *vrf-name* **例：** `Router(config)# vrf definition vrf-A`	VRF ルーティング テーブルを設定し、VRF コンフィギュレーション モードを開始します。 • VRF に割り当てる名前を指定するには、*vrf-name* 引数を使用します。
ステップ 4	**rd** *route-distinguisher* **例：** `Router(config-vrf)# rd 45000:1`	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、VPN 用のデフォルト ルート識別子を指定します。 • 一意の VPN IPv4 プレフィクスを作成するために、IPv4 プレフィクスに 8 バイト値を追加するには、*route-distinguisher* 引数を使用します。
ステップ 5	**route-target** {**import** | **export** | **both**} *route-target-ext-community* **例：** `Router(config-vrf)# route-target both 45000:100`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • ターゲット VPN 拡張コミュニティからルーティング情報をインポートするには、**import** キーワードを使用します。 • ターゲット VPN 拡張コミュニティにルーティング情報をエクスポートするには、**export** キーワードを使用します。 • ターゲット VPN 拡張コミュニティからルーティング情報をインポートするとともに、ルーティング情報を拡張コミュニティにエクスポートするには、**both** キーワードを使用します。 • インポート、エクスポート、またはその両方（インポートとエクスポート）を行うルート ターゲット拡張コミュニティの VRF のリストに route target extended community 属性を追加するには、*route-target-ext-community* 引数を使用します。
ステップ 6	**address-family ipv4** [**unicast**] **例：** `Router(config-vrf)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、VRF アドレス ファミリ コンフィギュレーション モードを開始します。 • ここでは、この前のステップで定義された VRF にアドレス ファミリを指定するために、このステップが必要になります。

	コマンドまたはアクション	目的
ステップ 7	**exit-address-family** **例：** `Router(config-vrf-af)# exit-address-family`	VRF アドレス ファミリ コンフィギュレーション モードを終了し、VRF コンフィギュレーション モードに戻ります。
ステップ 8	**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 9	**interface** *type number* **例：** `Router(config)# interface FastEthernet 1/1`	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 10	**vrf forwarding** *vrf-name* **例：** `Router(config-if)# vrf forwarding vrf-A`	VRF インスタンスをステップ 9で設定したインターフェイスと関連付けます。 • インターフェイスが VRF にバインドされている場合、それ以前に設定されていた IP アドレスは削除され、インターフェイスはディセーブルにされます。
ステップ 11	**ip address** *ip-address mask* **例：** `Router(config-if)# ip address 10.4.8.149 255.255.255.0`	インターフェイスに IP アドレスを設定します。
ステップ 12	**no shutdown** **例：** `Router(config-if)# no shutdown`	ディセーブルにされたインターフェイスをリスタートします。
ステップ 13	**exit** **例：** `Router(config-if)# exit`	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、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 14	他のインターフェイス付き VRF インスタンスをバインドするには、ステップ 3 から ステップ 13 までを繰り返します。	—
ステップ 15	**end** **例：** `Router(config)# end`	グローバル 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。

BGP パスへのイベントベース VPN インポート処理の設定

次の作業を行って、BGP パスを VRF テーブルへインポートするためイベントベース処理設定で BGP パスを変更する場合のコンバージェンス時間を短くします。2 つの新しい CLI コマンドにより、インポート側ネットごとのインポート パスの上限値の設定と、パス選択ポリシーの設定が可能になっています。

前提条件

この作業は、VRF が VRF アドレス ファミリ構文で使用されるようすでに設定されているものとしています。VRF を設定するには、「マルチプロトコル VRF の設定」（P.3）を参照してください。

BGP ネイバーの設定も完了しているものとします。設定例については、「BGP パスへのイベントベース VPN インポート処理の設定：例」（P.9）を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4 vrf** *vrf-name*
5. **import path selection** {**all** | **bestpath** [**strict**] | **multipath** [**strict**]}
6. **import path limit** *number-of-import-paths*
7. **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	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 45000`	指定したルーティング プロセスのルータ 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	**address-family ipv4 vrf** *vrf-name* **例：** `Router(config-router)# address-family ipv4 vrf vrf-A`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • 後続する IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンス名を指定するには、**vrf** キーワードと *vrf-name* 引数を使用します。

	コマンドまたはアクション	目的
ステップ 5	**import path selection** {**all** | **bestpath** [**strict**] | **multipath** [**strict**]} **例：** `Router(config-router-af)# import path selection all`	VRF テーブルにルートをインポートする BGP パスの選択ポリシーを指定します。 • この例では、VRF インスタンスの RT に一致するすべてのパスがインポートされます。
ステップ 6	**import path limit** *number-of-import-paths* **例：** `Router(config-router-af)# import path limit 3`	エクスポート側ネットからインポート可能な BGP パスの最大数をインポート側ネットごとに指定します。
ステップ 7	**end** **例：** `Router(config-router-af)# end`	アドレス ファミリ 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。

BGP イベントベース VPN インポート処理のモニタリングとトラブルシューティング

必要に応じて BGP イベントベース VPN インポート処理のモニタリングとトラブルシューティングを行うには、この作業の手順を実行します。

この作業で使用する **show** コマンドについて、ここではコマンド構文の一部だけが表示されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

手順の概要

1. **enable**
2. **show ip bgp vpnv4** {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*} [*network-address* [*mask*]]
3. **show ip route** [**vrf** *vrf-name*] [*ip-address* [*mask*]]
4. **debug ip bgp import** {**events** | **updates** [*access-list* | *expanded-access-list*]}

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*} [*network-address* [*mask*]]

この出力例では、**strict** キーワードが **import path selection** コマンドを使用して設定されていないため、安全インポート パス選択ポリシーが有効になっています。あるパスが最適使用可能パスとしてインポートされる場合（インポートの際に最良パスやマルチパスが不適切である場合）、出力にあるように「imported safety path」とマークされます。

```
Router# show ip bgp vpnv4 all 172.17.0.0

BGP routing table entry for 45000:1:172.17.0.0/16, version 10
Paths: (1 available, best #1, table vrf-A)
```

```
Flag: 0x820
   Not advertised to any peer
   2, imported safety path from 50000:2:172.17.0.0/16
     10.0.101.1 from 10.0.101.1 (10.0.101.1)
       Origin IGP, metric 200, localpref 100, valid, internal, best
       Extended Community: RT:45000:100
```

VRF インスタンスへインポートされると見なされるエクスポート側ネットの既存のパスは、別のピアルータから受信したものであるために VPN インポートのルールが適用されていない場合があります。ルート識別子（RD）情報はルータに対してローカルなため、これらのパスには同一の RD 情報が含まれていることがあります。しかし、これらのパスの一部は、インポートする VRF インスタンスの RT と一致しないため、**show** コマンドの出力では「not-in-vrf」とマークされます。

次の出力例では、パスは別のピア ルータから受信したもので、VPN インポート規則が適用されていません。この 10.0.101.2 というパスは、VPNv4 テーブルに追加され、vrf-A ネットに関連付けられています。元のルータからの RD 情報とはいえ、RD 情報との一致を含んでいるからです。しかし、このパスは vrf-A に RT 一致ではないため、「not-in-vrf」とマークされています。vrf-A のネットでは、このパスは最良パスとはならないことに注意してください。VRF にないどのパスも、VRF にあるパスより適したパスとは見られないからです。

```
Router# show ip bgp vpnv4 all 172.17.0.0

BBGP routing table entry for 45000:1:172.17.0.0/16, version 11
Paths: (2 available, best #2, table vrf-A)
Flag: 0x820
   Not advertised to any peer
   2
     10.0.101.2 from 10.0.101.2 (10.0.101.2)
       Origin IGP, metric 100, localpref 100, valid, internal, not-in-vrf
       Extended Community: RT:45000:200
       mpls labels in/out nolabel/16
   2
     10.0.101.1 from 10.0.101.1 (10.0.101.1)
       Origin IGP, metric 50, localpref 100, valid, internal, best
       Extended Community: RT:45000:100
       mpls labels in/out nolabel/16
```

ステップ 3 **show ip route** [**vrf** *vrf-name*] [*ip-address* [*mask*]]

この出力例には、VRF vrf-A のルーティング テーブルについての情報が表示されています。

```
Router# show ip route vrf vrf-A 172.17.0.0

Routing Table: vrf-A
Routing entry for 172.17.0.0/16
  Known via "bgp 1", distance 200, metric 50
  Tag 2, type internal
  Last update from 10.0.101.33 00:00:32 ago
  Routing Descriptor Blocks:
  * 10.0.101.33 (default), from 10.0.101.33, 00:00:32 ago
      Route metric is 50, traffic share count is 1
      AS Hops 1
      Route tag 2
      MPLS label: 16
      MPLS Flags: MPLS Required
```

ステップ 4 **debug ip bgp vpnv4 unicast import** {**events** | **updates** [*access-list*]}

BGP パスの VRF インスタンス テーブルへのインポートに関連したデバッグ情報を表示するには、このコマンドを使用します。実際の出力は、続けて入力されるコマンドによって変化します。

（注） updates キーワード使用時にフィルタ プレフィクスへのアクセス リストを指定しない場合、全プレフィクスに対するアップデートすべてが表示されることになり、ネットワークの速度低下が発生することがあります。

```
Router# debug ip bgp vpnv4 unicast import events

BGP import events debugging is on
```

BGP イベントベース VPN インポートの設定例

BGP パスへのイベントベース VPN インポート処理の設定：例

この設定例では、VRF（vrf-A）が設定され、ファスト イーサネット インターフェイス 1/1 に VRF フォワーディングが適用されます。アドレス ファミリ モードでは、インポート パス選択が「すべて」に、インポート パス数は「3」に設定されています。IPv4 アドレス ファミリのもとで 2 つの BGP ネイバーが設定され、VPNv4 アドレス ファミリのもとでアクティブにされています。

```
vrf definition vrf-A
 rd 45000:1
 route-target import 45000:100
 address-family ipv4
  exit-address-family
!
interface FastEthernet1/1
 no ip address
 vrf forwarding vrf-A
 ip address 10.4.8.149 255.255.255.0
 no shut
 exit
!
router bgp 45000
 network 172.17.1.0 mask 255.255.255.0
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.3.2 remote-as 50000
 address-family ipv4 vrf vrf-A
  import path selection all
  import path limit 3
  exit-address-family
 address-family vpnv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  end
```

次の作業

- 外部サービス プロバイダーに接続して、他の外部 BGP 機能を使用するには、『Connecting to a Service Provider Using External BGP』モジュールを参照してください。
- 一部の内部 BGP 機能を設定するには、『*Cisco IOS IP Routing Protocols Configuration Guide*』の「BGP」の項で、『Configuring Internal BGP Features』の章を参照してください。
- BGP ネイバー セッションのオプションを設定するには、『Configuring BGP Neighbor Session Options』モジュールを参照してください。
- BGP の拡張機能の一部を設定する場合は、『Configuring Advanced BGP Features』モジュールを参照してください。

その他の参考資料

ここでは、BGP イベントベース VPN インポート機能に関する参考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、コマンド モード、デフォルト、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*』
Cisco BGP のコンセプト情報の概要と各 BGP モジュールへのリンク	『*Cisco IOS IP Routing: BGP Configuration Guide*』の『Cisco BGP Overview』モジュール
BGP の基本作業のコンセプトと設定の詳細。	『*Cisco IOS IP Routing Protocols Configuration Guide*』の『Configuring a Basic BGP Network』モジュール
コマンド ルックアップ ツール	http://tools.cisco.com/Support/CLILookup
Cisco IOS マスター コマンド リスト	http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html

標準

標準	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ 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
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC の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

BGP イベントベース VPN インポートの機能情報

表 1 に、この機能のリリース履歴を示します。

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。Cisco IOS Release 15.0(1)M、12.2(33)SRE、またはそれ以降のリリースで導入または変更された機能だけを表に示します。

このテクノロジーの機能でここに記載されていない情報については、『Cisco BGP Implementation Roadmap』を参照してください。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関する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、Cisco IOS および Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://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。

（注） 表 1 に、特定の Cisco IOS ソフトウェア リリース トレインの中で特定の機能のサポートが導入された Cisco IOS ソフトウェア リリースだけを示します。その機能は、特に断りがない限り、それ以降の一連の Cisco IOS ソフトウェア リリースでもサポートされます。

表 1　BGP イベントベース VPN インポートの機能情報

機能名	リリース	機能情報
BGP イベントベース VPN インポート	12.2(33)SRE 15.0(1)M 15.0(1)S Cisco IOS XE 3.1.0SG	BGP イベントベース VPN インポート機能は、既存のボーダー ゲートウェイ プロトコル（BGP）パスのインポート プロセスに変更を加えるものです。拡張 BGP パス インポートはイベントの発生時に実行されます。BGP パスが変更されると、インポートされたコピーすべてのアップデートも、処理が可能になるとすぐに実行されます。ソフトウェアがアップデート処理前に定期的なスキャナ時間まで待つことに起因するルートの伝播の遅延もなくなるため、コンバージェンス時間が大幅に短縮されます。新しい処理の実装用に、新たなコマンドライン インターフェイス（CLI）が導入されています。 新たに導入されたり変更されたりしたのは、次のコマンドです。**bgp scan-time**、**import path limit**、**import path selection**、**maximum-path ebgp**、**maximum-path ibgp**、**show ip bgp vpnv4**、**show ip bgp vpnv6**