基本 BGP ネットワーク設定

このモジュールでは、基本的な Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）ネットワークを設定するための基本的な作業について説明します。BGP は、組織間にループのないルーティングを提供するために設計されたドメイン間ルーティング プロトコルです。ここでは、ネイバーおよびアドレス ファミリ コマンドの Cisco IOS 実装について説明します。また、このモジュールには BGP ピアの設定およびカスタマイズ、BGP ルート集約の実装、BGP ルート オリジネーションの設定、および BGP バックドア ルートの定義を行うための作業も含まれます。BGP ピア グループを定義し、ピア セッション テンプレートについて紹介するとともに、グループのアップデートについて説明します。

機能情報の検索

ご使用のソフトウェア 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。このモジュールに記載されている機能に関する情報を検索したり、各機能がサポートされているリリースに関するリストを参照したりするには、「基本 BGP ネットワーク設定の機能情報」（P.93）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 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

基本 BGP ネットワーク設定の前提条件

基本 BGP 作業を設定する前に、「Cisco BGP Overview」モジュールを理解しておく必要があります。

基本 BGP ネットワーク設定の制約事項

- Cisco IOS ソフトウェアを実行するルータは、1 つの BGP ルーティング プロセスだけを実行し、1 つの BGP 自律システムだけのメンバになるように設定できます。ただし、BGP ルーティング プロセスと自律システムでは、複数のアドレス ファミリ設定をサポートできます。

基本 BGP ネットワーク設定の概要

基本 BGP ネットワークを設定するには、次の概念について理解する必要があります。

BGP バージョン 4

ボーダー ゲートウェイ プロトコル（BGP）は、独立したルーティング ポリシーを持つルーティング ドメイン（自律システム）の間に、ループのないルーティングを提供するように設計されたドメイン間ルーティング プロトコルです。BGP バージョン 4 の Cisco IOS ソフトウェア実装には、BGP が IP マルチキャスト ルートに関するルーティング情報を伝送できるようにするマルチプロトコル拡張機能と、IP Version 4（IPv4; IP バージョン 4）、IP Version 6（IPv6; IP バージョン 6）、Virtual Private Networks Version 4（VPNv4; バーチャル プライベート ネットワーク バージョン 4）、および Connectionless Network Services（CLNS; コネクションレス型ネットワーク サービス）を含む複数のレイヤ 3 プロトコル アドレス ファミリが組み込まれています。

BGP は主に、ローカル ネットワークを外部ネットワークに接続して、インターネットにアクセスしたり、他の組織に接続したりするために使用されます。外部組織への接続時に、external BGP（eBGP; 外部 BGP）ピアリング セッションが作成されます。BGP は Exterior Gateway Protocol（EGP; 外部ゲートウェイ プロトコル）と呼ばれますが、組織内のネットワークの多くが複雑になってきているため、BGP を使用して、組織内で使用される内部ネットワークを簡略化することができます。同一組織内の BGP ピアは、internal BGP（iBGP; 内部 BGP）ピアリング セッションによってルーティング情報を交換します。

（注） BGP は他のルーティング プロトコルよりも多くの設定を必要としますが、ユーザは設定変更の影響をよく理解しておく必要があります。設定が正しくないと、ルーティング ループが発生し、通常のネットワーク操作に悪影響を及ぼす可能性があります。

BGP スピーカーとピア関係

BGP 対応ルータは、別の BGP 対応デバイスを自動的には検出しません。ネットワーク管理者は、通常、BGP 対応ルータ間の関係を手動で設定します。ピア デバイスとは、別の BGP 対応デバイスへのアクティブな TCP 接続を持つ BGP 対応ルータです。この BGP デバイス間の関係がネイバーと呼ばれることはよくありますが、これは BGP デバイスは直接接続されていて、その間に他のルータははさまっていないということを暗示することがあるため、このマニュアルでは「ネイバー」という語の使用は極力避けています。BGP スピーカーはローカル ルータのことで、その他の BGP 対応ネットワーク デバイスはすべてピアです。

ピアとピアの間に TCP 接続が確立されると、最初、個々の BGP ピアはもう 1 つのピアと、そのルート（完成した BGP ルーティング テーブル）をすべて交換します。この交換の後は、ネットワークでトポロジの変更が行われたとき、またはルーティング ポリシーが実装または変更されたときに差分更新が送信されるだけです。更新と更新の間の非アクティブ期間には、ピアは「キープアライブ」と呼ばれる特別なメッセージを交換します。

BGP 自律システムは、単一のアドミニストレーション エンティティにより制御されるネットワークです。ピア ルータは、異なる自律システムに存在する場合は外部ピア、同一の自律システムに存在する場合は内部ピアと呼ばれます。通常、外部ピアは隣接し、サブネットを共有していますが、内部ピアは同じ自律システムのどのような場所にあってもかまいません。

外部 BGP ピアの詳細については、「Connecting to a Service Provider Using External BGP」モジュールを参照してください。内部 BGP ピアの詳細については、「Configuring Internal BGP Features」モジュールを参照してください。

BGP 自律システム番号の形式

2009 年 1 月まで、企業に割り当てられていた BGP 自律システム番号は、RFC 4271『*A Border Gateway Protocol 4 (BGP-4)*』に記述された、1 ～ 65535 の範囲の 2 オクテットの数値でした。自律システム番号の要求の増加に伴い、Internet Assigned Number Authority（IANA; インターネット割り当て番号局）により割り当てられる自律システム番号は 2009 年 1 月から 65536 ～ 4294967295 の範囲の 4 オクテットの番号になります。RFC 5396『*Textual Representation of Autonomous System (AS) Numbers*』には、自律システム番号を表す 3 つの方式が記述されています。シスコでは、次の 2 つの方式を実装しています。

- asplain：10 進表記方式。2 バイトおよび 4 バイト自律システム番号をその 10 進数値で表します。たとえば、65526 は 2 バイト自律システム番号、234567 は 4 バイト自律システム番号になります。

- asdot：自律システム ドット付き表記。2 バイト自律システム番号は 10 進数で、4 バイト自律システム番号はドット付き表記で表されます。たとえば、65526 は 2 バイト自律システム番号、1.169031（10 進表記の 234567 をドット付き表記にしたもの）は 4 バイト自律システム番号になります。

自律システム番号を表す 3 つ目の方法については、RFC 5396 を参照してください。

asdot だけを使用する自律システム番号形式

Cisco IOS Release 12.0(32)S12、12.4(24)T、およびそれ以降のリリースでは、4 オクテット（4 バイト）の自律システム番号は asdot 表記法だけで入力および表示されます。たとえば、1.10 または 45000.64000 です。4 バイト自律システム番号のマッチングに正規表現を使用する場合、asdot 形式には正規表現で特殊文字となるピリオドが含まれていることに注意します。正規表現でのマッチングに失敗しないよう、1\.14 のようにピリオドの前にバックスラッシュを入力する必要があります。表 1 は、asdot 形式だけが使用できる Cisco IOS イメージで、2 バイトおよび 4 バイト自律システム番号の設定、正規表現とのマッチング、および **show** コマンド出力での表示に使用される形式をまとめたものです。

表 1　asdot だけを使用する 4 バイト自律システム番号形式

形式	設定形式	show コマンド出力および正規表現のマッチング形式
asdot	2 バイト：1 ～ 65535 4 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 65535 4 バイト：1.0 ～ 65535.65535

asplain をデフォルトとする自律システム番号形式

Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、およびそれ以降のリリースでは、シスコ実装の 4 バイト自律システム番号で asplain がデフォルトの自律システム番号表示形式として使用されていますが、4 バイト自律システム番号は asplain および asdot 形式のどちらにも設定できます。また、正規表現で 4 バイト自律システム番号とマッチングするためのデフォルト形式は asplain であるため、4 バイト自律システム番号とマッチングする正規表現はすべて、asplain 形式で記述する必要があります。デフォルトの **show** コマンド出力で、4 バイト自律システム番号が asdot 形式で表示されるように変更する場合は、ルータ コンフィギュレーション モードで **bgp asnotation dot** コマンドを使用します。デフォルトで asdot 形式がイネーブルにされている場合、正規表現の 4 バイト自律システム番号のマッチングには、すべて asdot 形式を使用する必要があり、使用しない場合正規表現によるマッチングは失敗します。表 2 および 表 3 に示すように、4 バイト自律システム番号は asplain と asdot のどちらにも設定できるとはいえ、**show** コマンド出力と正規表現を用いた 4 バイト自律システム番号のマッチング制御には 1 つの形式だけが使用されます。デフォルトは asplain 形式です。**show** コマンド出力の表示と正規表現のマッチング制御で asdot 形式の 4 バイト自律システム番号を使用する場合、**bgp asnotation dot** コマンドを設定する必要があります。**bgp asnotation dot** コマンドをイネーブルにした後で、**clear ip bgp *** コマンドを入力し、すべての BGP セッションについて、ハード リセットを開始する必要があります。

（注） 4 バイト自律システム番号をサポートしているイメージにアップグレードしている場合でも、2 バイト自律システム番号を使用できます。4 バイト自律システム番号に設定された形式にかかわらず、2 バイト自律システムの **show** コマンド出力と正規表現のマッチングは変更されず、asplain（10 進数）形式のままになります。

表 2　asplain をデフォルトとする 4 バイト自律システム番号形式

形式	設定形式	show コマンド出力および正規表現のマッチング形式
asplain	2 バイト：1 ～ 65535 4 バイト：65536 ～ 4294967295	2 バイト：1 ～ 65535 4 バイト：65536 ～ 4294967295
asdot	2 バイト：1 ～ 65535 4 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 65535 4 バイト：65536 ～ 4294967295

表 3　asdot を使用する 4 バイト自律システム番号形式

形式	設定形式	show コマンド出力および正規表現のマッチング形式
asplain	2 バイト：1 ～ 65535 4 バイト：65536 ～ 4294967295	2 バイト：1 ～ 65535 4 バイト：1.0 ～ 65535.65535
asdot	2 バイト：1 ～ 65535 4 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 65535 4 バイト：1.0 ～ 65535.65535

予約済みおよびプライベートの自律システム番号

Cisco IOS Release 12.0(32)S12、12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、12.4(24)T、およびそれ以降のリリースでは、RFC 4893 がシスコの BGP 実装でサポートされています。RFC 4893 は、2 バイト自律システム番号から 4 バイト自律システム番号への段階的移行を BGP がサポートできるように開発されました。RFC 4893 では新たに 23456 が予約済み（プライベート）自律システム番号に指定され、Cisco IOS CLI ではこの番号を自律システム番号として設定できなくなっています。

RFC 5398『*Autonomous System (AS) Number Reservation for Documentation Use*』では、文書化を目的として新たに予約された自律システム番号について説明されています。予約済み番号を使用することで、設定例を正確に文書化しつつ、その設定がそのままコピーされた場合でも製品ネットワークに競合が発生することを防止できます。予約済み番号は IANA 自律システム番号レジストリに記載されています。予約済み 2 バイト自律システム番号は 64496 ～ 64511 の連続したブロック、予約済み 4 バイト自律システム番号は 65536 ～ 65551 をその範囲としています。

64512 ～ 65534 を範囲とするプライベートの 2 バイト自律システム番号は依然有効で、65535 は特殊な目的のために予約されています。プライベート自律システム番号は内部ルーティング ドメインで使用できますが、インターネットにルーティングされるトラフィックについては変換が必要です。プライベート自律システム番号を外部ネットワークへアドバタイズするように BGP を設定しないでください。Cisco IOS ソフトウェアは、デフォルトではルーティング アップデートからプライベート自律システム番号を削除しません。ISP がプライベート自律システム番号をフィルタリングすることを推奨します。

（注）　パブリック ネットワークおよびプライベート ネットワークに対する自律システム番号の割り当ては、IANA が管理しています。予約済み番号の割り当てや自律システム番号の登録申込など、自律システム番号についての情報については、http://www.iana.org/ を参照してください。

BGP ピア セッションの確立

BGP ルーティング プロセスがピアとピアリング セッションを確立するとき、ステートは次のように変化します。

- Idle：ルーティング プロセスがイネーブルになったとき、またはルータがリセットされたときの BGP ルーティング プロセスの初期ステート。このステートでは、ルータはリモート ピアとのピアリング設定など、開始イベントを待ちます。リモート ピアから TCP 接続要求を受信すると、ルータはリモート ピアへの TCP 接続を開始する前に、タイマーを待機するための開始イベントを新たに開始します。ルータがリセットされ、ピアがリセットされると、BGP ルーティング プロセスは Idle ステートに戻ります。
- Connect：ローカル BGP スピーカーとの TCP セッションを確立しようとしていることを BGP ルーティング プロセスが検知します。
- Active：このステートでは、BGP ルーティング プロセスは、ConnectRetry タイマーを使用して、ピア ルータとの TCP セッションを確立しようとします。BGP ルーティング プロセスが Active ステートの間、開始イベントは無視されます。BGP ルーティング プロセスが再構成された場合、またはエラーが発生した場合、BGP ルーティング プロセスはシステム リソースを解放し、Idle ステートに戻ります。
- OpenSent：TCP 接続が確立され、BGP ルーティング プロセスはリモート ピアに OPEN メッセージを送信し、OpenSent ステートに移行します。このステートでは、BGP ルーティング プロセスはその他の OPEN メッセージを受信できます。接続に失敗した場合、BGP ルーティング プロセスは Active ステートに移行します。
- OpenReceive：BGP ルーティング プロセスはリモート ピアから OPEN メッセージを受信し、リモート ピアからの最初のキープアライブ メッセージを待ちます。キープアライブ メッセージを受信すると、BGP ルーティング プロセスは Established ステートに移行します。通知メッセージを受信した場合は、BGP ルーティング プロセスは Idle ステートに移行します。ピアリング セッションに影響を与えるエラー、または設定変更が発生した場合、BGP ルーティング プロセスは、Finite State Machine（FSM; 有限状態マシン）エラー コードが入った通知メッセージを送信してから、Idle ステートに移行します。
- Established：リモート ピアから最初のキープアライブが受信されます。これにより、リモート ネイバーとのピアリングが確立され、BGP ルーティング プロセスは、リモート ピアとのアップデート メッセージの交換を開始します。アップデート メッセージ、またはキープアライブ メッセージが受信されると、ホールド タイマーが再起動されます。エラー通知を受信した BGP プロセスは、Idle ステートに移行します。

シスコシステムズが採用している BGP グローバル コマンドとアドレス ファミリ コンフィギュレーション コマンド

BGP を設定するためのアドレス ファミリ モデルでは、基本的にアドレス ファミリごとに設定が分割されます。設定の最初に、アドレス ファミリとは関係のない（非依存の）コマンドがすべてグループ化され（最上位レベル）、これに各アドレス ファミリに固有のコマンドで使用される個々のサブモードが続きます（ただし、IPv4 ユニキャストに関係するコマンドは例外で、これらは設定の先頭に入力することができます）。ネットワーク オペレータが BGP を設定した場合の BGP 設定カテゴリのフローは、次の箇条書きの順に表されます。

- グローバル コンフィギュレーション：特定のネイバーではなく、BGP に全般的に適用される設定。たとえば、**network**、**redistribute**、**bgp bestpath** などのコマンド。
- アドレス ファミリ依存コンフィギュレーション：個々のネイバーのポリシーなど、特定のアドレス ファミリに適用されるコンフィギュレーション。

BGP グローバルおよび BGP アドレス ファミリ依存設定のカテゴリを表 4 に示します。

表 4　BGP コンフィギュレーション カテゴリの関係

BGP コンフィギュレーション カテゴリ	カテゴリ内のコンフィギュレーション セット
グローバル アドレス ファミリ非依存	グローバル アドレス ファミリ非依存コンフィギュレーション 1 セット
アドレス ファミリ依存	1 アドレス ファミリにつき、グローバル アドレス ファミリ依存コンフィギュレーション 1 セット

（注） アドレス ファミリ コンフィギュレーションは、それが適用されるアドレス ファミリ サブモードで入力する必要があります。

次の BGP コンフィギュレーション文の例は、グループ分けされたグローバル アドレス ファミリ非依存コマンドと、アドレス ファミリ依存コマンドを示しています。

```
router bgp <AS>
 ! AF independent part
 neighbor <ip-address> <command> ! Session config; AF independent
 address-family ipv4 unicast
  ! AF dependant part
  neighbor <ip-address> <command> ! Policy config; AF dependant
  exit-address-family
 address-family ipv4 multicast
  ! AF dependant part
  neighbor <ip-address> <command> ! Policy config; AF dependant
  exit-address-family
 address-family ipv4 unicast vrf <vrf-name>
  ! VRF specific AS independent commands
  ! VRF specific AS dependant commands
  neighbor <ip-address> <command> ! Session config; AF independent
  neighbor <ip-address> <command> ! Policy config; AF dependant
  exit-address-family
```

次の例は、前の例で、BGP コンフィギュレーション文と一致する、実際の BGP コマンドを示しています。

```
router bgp 45000
 router-id 172.17.1.99
 bgp log-neighbor-changes
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.3.2 remote-as 50000
 address-family ipv4 unicast
  neighbor 192.168.1.2 activate
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
 address-family ipv4 multicast
  neighbor 192.168.3.2 activate
  neighbor 192.168.3.2 advertisement-interval 25
  network 172.16.1.0 mask 255.255.255.0
  exit-address-family
 address-family ipv4 vrf vpn1
  neighbor 192.168.3.2 activate
  network 172.21.1.0 mask 255.255.255.0
  exit-address-family
```

Cisco IOS Release 12.0(22)S、12.2(15)T、およびそれ以降のリリースでは、**bgp upgrade-cli** コマンドにより、Network Layer Reachability Information（NLRI; ネットワーク レイヤ到着可能性情報）形式からアドレス ファミリ形式への BGP ネットワークおよび既存のコンフィギュレーションの移行が簡単になっています。ネットワーク オペレータは、Address Family Identifier（AFI）形式でコマンドを設定し、この設定を既存の NLRI 形式の設定に保存できます。NLRI 形式の制限のため、BGP ハイブリッド Command-Line Interface（CLI; コマンドライン インターフェイス）は、AFI および NLRI の統合を完全にはサポートしていません。AFI コマンドおよび機能をすべてサポートするためには、**bgp upgrade-cli** コマンドを使用して、既存の NLRI コンフィギュレーションをアップグレードすることを推奨します。NLRI 形式からアドレス ファミリ形式への BGP コンフィギュレーションの移行例については、「NLRI から AFI へのコンフィギュレーション：例」（P.82）を参照してください。

BGP セッションのリセット

設定変更のためにルーティング ポリシーに変更が生じた場合は、必ず **clear ip bgp** コマンドを使用して、BGP ピアリング セッションをリセットする必要があります。Cisco IOS ソフトウェアは、BGP ピアリング セッションをリセットするために、次の 3 つのメカニズムをサポートしています。

- *ハード リセット*：ハード リセットは、TCP 接続を含む指定されたピアリング セッションを終了し、指定されたピアから到着したルートを削除します。
- *ソフト リセット*：ソフト リセットは、保存されたプレフィクス情報を使用し、既存のピアリング セッションを廃棄せずに BGP ルーティング テーブルの再構成とアクティブ化を行います。ソフト再構成では、保存されているアップデート情報が使用されます。アップデートを保存するために追加のメモリが必要になりますが、ネットワークを中断せずに、新しい BGP ポリシーを適用することができます。ソフト再構成は、インバウンド セッション、またはアウトバウンド セッションに対して設定できます。
- *ダイナミック インバウンド ソフト リセット*：これは RFC 2918 に定義されているルート リフレッシュ機能で、サポートしているピアへのルート リフレッシュ要求を交換することにより、ローカル ルータがインバウンド ルーティング テーブルを動的にリセットできるようにするものです。中断を伴わないポリシー変更については、ルート リフレッシュ機能がアップデート情報をローカルに保存することはありません。その代わり、サポートしているピアとの動的な交換に依存します。ルート リフレッシュは、最初にピア間の BGP 機能ネゴシエーションを通じてアドバタイズされる必要があります。すべての BGP ルータが、ルート リフレッシュ機能をサポートしていなければなりません。

  BGP ルータがこの機能をサポートしているか確認するには、**show ip bgp neighbors** コマンドを使用します。ルータがルート リフレッシュ機能をサポートしている場合、次のメッセージが出力されます。

  ```
  Received route refresh capability from peer.
  ```

Cisco IOS Release 12.3(14)T では、ルート リフレッシュ機能をサポートしていないピアに対してインバウンド ソフト再構成を実行するように BGP を設定するための **bgp soft-reconfig-backup** コマンドが導入されました。このコマンドの設定により、必要な場合にだけ、アップデート（ソフト再構成）を格納するように、BGP を設定することができます。このコマンドを設定しても、ルート リフレッシュ機能をサポートしているピアは影響されません。

BGP ルート集約

BGP ピアはルーティング情報を格納し、交換しますが、設定される BGP スピーカーの数が増えるに従って、ルーティング情報の量が増えます。ルート集約を使用することにより、関係する情報の量が減ります。集約は、複数の異なるルートのアトリビュートを合成し、1 つのルートだけがアドバタイズさ

れるようにするプロセスです。集約プレフィクスは、Classless Interdomain Routing（CIDR; クラスレス ドメイン間ルーティング）の原則を使用して、複数の隣接するネットワークを、ルーティング テーブルに要約できる IP アドレスのクラスレス セット 1 つに合成します。これにより、アドバタイズが必要なルートの数が少なくなります。

BGP でのルート集約の実装方法は 2 種類あります。集約されたルートを BGP に再配布するか、または条件付き集約の形を使用することができます。基本ルートの再配布では、集約ルートの作成後、このルートが BGP に再配布されます。条件付き集約では、集約ルートの作成後、アドバタイズするか、または Autonomous System Set Path（AS-SET）情報、もしくは要約情報に基づいて、特定ルートのアドバタイズを抑制します。

Cisco IOS Release 12.2(25)S、12.2(33)SXH、および 15.0(1)M では、BGP ピアに非アクティブなルートをアドバタイズしないように BGP を設定するための **bgp suppress-inactive** コマンドが導入されました。BGP ルーティング プロセスは、デフォルトで、Routing Information Database（RIB; ルーティング情報データベース）にインストールされていないルートを BGP ピアにアドバタイズできます。RIB にインストールされていないルートは非アクティブなルートです。非アクティブなルートのアドバタイズメントは、たとえば、共通のルート集約を通じてルートがアドバタイズされた場合に行われます。非アクティブなルートのアドバタイズメントを抑制して、より整合性の取れたデータ フォワーディングを行うことができます。

BGP ピア グループ

BGP ネットワークでは、多数のネイバーが同じアップデート ポリシー（つまり、同じアウトバウンド ルート マップ、配布リスト、フィルタ リスト、アップデート ソースなど）を使って設定されていることがよくあります.同じアップデート ポリシーを持つネイバーは、コンフィギュレーションを簡素化するため、またさらに重要なことには、コンフィギュレーションのアップデートをより効率化するために、BGP ピア グループにグループ化されます。多数のピアがある場合、このアプローチを強く推奨します。

ピア グループおよび BGP アップデート メッセージ

リリース 12.0(24)S、12.2(18)S、または 12.3(4)T 以前の Cisco IOS ソフトウェア リリースでは、BGP アップデート メッセージは、ピア グループのコンフィギュレーションに基づいてグループ化されていました。BGP アップデート メッセージ生成において、ネイバーをグループ化するこの方法により、ルーティング テーブルのスキャンに必要なシステム処理リソースの量が削減されました。しかし、この方法には、次のような制約がありました。

- ピア グループ コンフィギュレーションを共有するネイバーはすべて、アウトバウンド ルーティング ポリシーも共有する必要がある。
- すべてのネイバーは同じピア グループとアドレス ファミリに属している必要がある。別のアドレス ファミリで設定されているネイバーは異なるピアグループに属することはできません。

このような制約は、ピア グループ コンフィギュレーションに対して、最適なアップデート生成とレプリケーションのバランスをとるためのものでした。これらの制約により、ネットワーク オペレータは小さめのピア グループを設定するようになるため、アップデート メッセージの生成効率が下がり、ネイバー コンフィギュレーションのスケーラビリティが限定されていました。

BGP アップデート グループ

Cisco IOS Release 12.0(24)S、12.2(18)S、12.3(4)T、または 12.2(27)SBC への BGP（ダイナミック）アップデート グループの導入により、既存の BGP ピア グループから異なるタイプの BGP ピア グループ分けが可能になります。既存のピア グループは影響を受けませんが、現在のピア グループのメンバではない、同一のアウトバウンド ポリシーを持つ設定済みピアをアップデート グループに入れることができます。このアップデート グループのメンバは同一のアップデート生成エンジンを使用します。BGP アップデート グループを設定すると、アウトバウンド ポリシーに基づいて、BGP アップデート グループ メンバシップがダイナミックに計算されます。最適な BGP アップデート メッセージの生成は、単独で自動的に行われます。BGP ネイバー コンフィギュレーションはアウトバウンド ルーティング ポリシーによる制約を受けなくなり、アップデート グループは異なるアドレス ファミリに属すことができるようになります。

ピア テンプレート

構成管理など、ピア グループの制約の一部に対応するため、BGP アップデート グループ コンフィギュレーションをサポートする BGP ピア テンプレートが導入されました。

ピア テンプレートは、ポリシーを共有するネイバーに適用可能なコンフィギュレーション パターンです。ピア テンプレートは再利用が可能で、継承がサポートされているため、ネットワーク オペレータはピア テンプレートを使用して、ポリシーを共有している BGP ネイバーに対して異なるネイバー コンフィギュレーションをグループ化し適用できます。また、ネットワーク オペレータは、別のピア テンプレートからコンフィギュレーションを継承できるというピア テンプレートの機能を使用して、非常に複雑なコンフィギュレーション パターンを定義できるようになります。

ピア テンプレートには 2 種類あります。

- ピア セッション テンプレート。アドレス ファミリ モードおよび NLRI コンフィギュレーション モードすべてに共通する一般的なセッション コマンドのコンフィギュレーションをグループ化し、適用するために使用されます。
- ピア ポリシー テンプレート。特定のアドレス ファミリおよび NLRI コンフィギュレーション モードで適用されるコマンドのコンフィギュレーションをグループ化し、適用するために使用されます。

ピア テンプレートにより、柔軟性が高まり、ネイバー コンフィギュレーションの機能が強化されます。また、ピア テンプレートはピア グループ コンフィギュレーションに代わるものを提供し、ピア グループの制約の一部を解決します。ピア テンプレートを使用した BGP ピア ルータも、自動アップデート グループ コンフィギュレーションの恩恵を受けています。BGP ピア テンプレートが設定され、BGP ダイナミック アップデート ピア グループがサポートされたことにより、ネットワーク オペレータは BGP でピア グループを設定する必要がなくなります。また、ネットワークはコンフィギュレーションの柔軟性が高まり、コンバージェンスが高速化されたことによる恩恵を受けます。

（注） BGP ピア テンプレートのコンフィギュレーションは、ピア グループ コンフィギュレーションと競合したり、これを制約したりすることはありません。また、ピア グループは引き続き、BGP ピア テンプレートをサポートする Cisco IOS リリースでもサポートされます。ただし、ピア グループおよびピア テンプレートの両方で機能するように BGP ネイバーを設定することはできません。BGP ネイバーは、1 つのピア グループだけに属するように設定するか、またはピア テンプレートからポリシーを継承するように設定します。

基本 BGP ネットワークの設定方法

基本 BGP ネットワーク設定は、いくつかの必須作業と、多数の任意の作業から構成されます。BGP ルーティング プロセスと BGP ピアは必ず設定する必要がありますが、このとき、できればアドレス ファミリ コンフィギュレーション モデルを使用してください。BGP ピアが VPN ネットワークの一部である場合、BGP ピアの設定には、IPv4 VRF アドレス ファミリ タスクを使用する必要があります。次にあげるその他の作業は任意です。

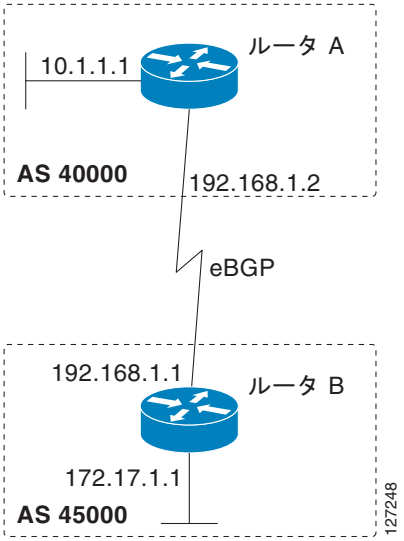
BGP ルーティング プロセスの設定

BGP ルーティング プロセスを設定するには、次の作業を実行します。BGP をイネーブルにするには、必須の手順を少なくとも一度、実行する必要があります。ここで説明する任意の手順を実行すると、BGP ネットワークでその他の機能を設定できます。ネイバー リセットのロギングやリンクが停止したときのピアの即時リセットなど、一部の機能はデフォルトでイネーブルにされていますが、BGP ネットワークの動作方法をよりよく理解できるようにするため、これらの機能についてはここで説明しています。

（注） Cisco IOS ソフトウェアを実行するルータは、1 つの BGP ルーティング プロセスだけを実行し、1 つの BGP 自律システムだけのメンバになるように設定できます。ただし、BGP ルーティング プロセスおよび自律システムは、同時に使用する複数の BGP アドレス ファミリおよびサブアドレス ファミリ コンフィギュレーションをサポートできます。

図 1 では、この作業のコンフィギュレーションはルータ A で行われますが、2 つのルータの間で BGP プロセスを完全に実現するには、たとえば、ルータ B で IP アドレスを適宜、変更してこのコンフィギュレーションを繰り返す必要があります。ここでは、BGP ルーティング プロセスに対して設定されるアドレス ファミリはないため、IPv4 ユニキャスト アドレス ファミリのルーティング情報はデフォルトでアドバタイズされます。

図 1　　2 つの自律システムを持つ BGP トポロジ



BGP ルータ ID

BGP はルータ ID を使用して、BGP 対応ピアを識別します。BGP ルータ ID は 32 ビット値です。この値は、IPv4 アドレスで表現されることがよくあります。デフォルトでは、Cisco IOS ソフトウェアは、ルータのループバック インターフェイスの IPv4 アドレスにこのルータ ID を設定します。ルータでループバック インターフェイスが設定されていない場合、BGP ルータ ID を表現するために、ルータの物理インターフェイスで設定されている最大の IPv4 アドレスが選択されます。BGP ルータ ID は、ネットワークの BGP ピア固有のものでなければなりません。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]
5. **bgp router-id** *ip-address*
6. **timers bgp** *keepalive holdtime*
7. **bgp fast-external-fallover**
8. **bgp log-neighbor-changes**
9. **end**
10. **show ip bgp** [*network*] [*network-mask*]

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 40000`	BGP ルーティング プロセスを設定し、指定されたルーティング 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。 • *autonomous-system-number* 引数を使用して、0 ～ 65534 の範囲の整数を 1 つ指定します。これは、その他の BGP スピーカーへのルータを表します。
ステップ 4	**network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*] **例：** `Router(config-router)# network 10.1.1.0 mask 255.255.255.0`	（任意）ネットワークを、この自律システムに対してローカルに設定し、BGP ルーティング テーブルに追加します。 • 外部プロトコルの場合、**network** コマンドはアドバタイズされるネットワークを制御します。内部プロトコルは **network** コマンドを使用して、アップデートの送信先を判断します。
ステップ 5	**bgp router-id** *ip-address* **例：** `Router(config-router)# bgp router-id 10.1.1.99`	（任意）BGP を実行しているローカル ルータの ID として、32 ビットの固定ルータ ID を設定します。 • *ip-address* 引数を使用して、ネットワーク内で固有のルータ ID を指定します。 **（注）** **bgp router-id** コマンドを使用してルータ ID を設定すると、アクティブな BGP ピアリング セッションすべてがリセットされます。
ステップ 6	**timers bgp** *keepalive holdtime* **例：** `Router(config-router)# timers bgp 70 120`	（任意）BGP ネットワーク タイマーを設定します。 • *keepalive* 引数を使用して、頻度を秒単位で指定します。ソフトウェアはこの間隔で、BGP ペアにキープアライブ メッセージを送信します。デフォルトでは、keepalive タイマーは 60 秒に設定されます。 • *holdtime* 引数を使用して、インターバルを秒単位で指定します。この時間を過ぎても、キープアライブ メッセージが届かなかった場合、BGP ピアはデッドであると宣言されます。デフォルトでは、holdtime タイマーは 180 秒に設定されます。
ステップ 7	**bgp fast-external-fallover** **例：** `Router(config-router)# bgp fast-external-fallover`	（任意）BGP セッションの自動リセットをイネーブルにします。 • デフォルトでは、直接隣接する外部ピアへのアクセスに使用されるリンクがダウンした場合、このピアの BGP セッションはリセットされます。

	コマンドまたはアクション	目的
ステップ 8	**bgp log-neighbor-changes** **例：** `Router(config-router)# bgp log-neighbor-changes`	（任意）BGP ネイバー ステータスの変更（アップまたはダウン）およびネイバーのリセットのロギングをイネーブルにします。 • このコマンドは、ネットワーク接続の問題のトラブルシューティングと、ネットワークの安定性の測定に使用します。予期しないネイバーのリセットは、ネットワークでのエラー率が高いことまたはパケット損失が高いことを示す場合があり、調査する必要があります。
ステップ 9	**end** **例：** `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 10	**show ip bgp** [*network*] [*network-mask*] **例：** `Router# show ip bgp`	（任意）BGP ルーティング テーブル内のエントリを表示します。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次に、この作業を図 1 のルータ A で設定した後で、ルータ A の BGP ルーティング テーブルを表示する **show ip bgp** コマンドの出力例を示します。この自律システムに対してローカルなネットワーク 10.1.1.0 に対するエントリも表示されています。

```
BGP table version is 12, local router ID is 10.1.1.99
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
*> 10.1.1.0/24      0.0.0.0                  0         32768 i
```

トラブルシューティングのヒント

BGP ルータ間の基本的なネットワーク接続性をチェックするには、**ping** コマンドを使用します。

BGP ピアの設定

2 つの IPv4 ルータ（ピア）の間に BGP を設定するには、この作業を実行します。ここで設定するアドレス ファミリは、デフォルトの IPv4 ユニキャスト アドレス ファミリで、設定は図 1（P.12）のルータ A で行われています。BGP ピアとなりうるネイバー ルータすべてについて、必ず、この作業を実行してください。

前提条件

この作業を実行する前に、「BGP ルーティング プロセスの設定」の作業を実行します。

制約事項

デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義されたネイバーは、IPv4 ユニキャスト アドレス プレフィクスだけを交換します。IPv6 プレフィクスなど、その他のアドレス プレフィクス タイプを交換するには、アドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用し、ネイバーをアクティブ化することも必要です。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
6. **neighbor** *ip-address* **activate**
7. **end**
8. **show ip bgp** [*network*] [*network-mask*]
9. **show ip bgp neighbors** [*neighbor-address*]

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 40000`	指定されたルーティング プロセスでルータ 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	**neighbor** *ip-address* **remote-as** *autonomous-system-number* **例：** `Router(config-router)# neighbor 192.168.1.1 remote-as 45000`	指定された自律システムのネイバーの IP アドレスを、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。

	コマンドまたはアクション	目的
ステップ 5	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] **例：** `Router(config-router)# address-family ipv4 unicast`	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。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィクスを指定します。 • **vrf** キーワードと *vrf-name* 引数は、それ以降の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドと関連付けられる Virtual Routing and Forwarding（VRF; 仮想ルーティング/転送）インスタンスの名前を表します。
ステップ 6	**neighbor** *ip-address* **activate** **例：** `Router(config-router-af)# neighbor 192.168.1.1 activate`	ネイバーが IPv4 ユニキャスト アドレス ファミリのプレフィクスをローカル ルータと交換できるようにします。
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 モードを開始します。
ステップ 8	**show ip bgp** [*network*] [*network-mask*] **例：** `Router# show ip bgp`	（任意）BGP ルーティング テーブル内のエントリを表示します。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 9	**show ip bgp neighbors** [*neighbor-address*] **例：** `Router(config-router-af)# show ip bgp neighbors 192.168.2.2`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次に、この作業を図 1（P.12）のルータ A およびルータ B で設定した後で、ルータ A の BGP ルーティング テーブルを表示する **show ip bgp** コマンドの出力例を示します。これで、自律システム 45000 でネットワーク 172.17.1.0 のエントリを確認できるようになります。

```
BGP table version is 13, local router ID is 10.1.1.99
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
```

```
*> 10.1.1.0/24      0.0.0.0                  0         32768 i
*> 172.17.1.0/24    192.168.1.1              0             0 45000 i
```

次に、この作業を図 1 (P.12)のルータ A で設定した後で、ルータ A の BGP ネイバー 192.168.1.1 への TCP および BGP 接続に関する情報を表示する **show ip bgp neighbors** コマンドの出力例を示します。

```
BGP neighbor is 192.168.1.1,  remote AS 45000, external link
  BGP version 4, remote router ID 172.17.1.99
  BGP state = Established, up for 00:06:55
  Last read 00:00:15, last write 00:00:15, hold time is 120, keepalive intervals
  Configured hold time is 120,keepalive interval is 70 seconds, Minimum holdtims
  Neighbor capabilities:
    Route refresh: advertised and received (old & new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1          2
    Keepalives:            13         13
    Route Refresh:          0          0
    Total:                 15         16
  Default minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 13, neighbor version 13/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                               Sent       Rcvd
  Prefix activity:             ----       ----
    Prefixes Current:             1          1 (Consumes 52 bytes)
    Prefixes Total:               1          1
    Implicit Withdraw:            0          0
    Explicit Withdraw:            0          0
    Used as bestpath:           n/a          1
    Used as multipath:          n/a          0

                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    AS_PATH loop:                      n/a          1
    Bestpath from this peer:             1        n/a
    Total:                               1          1
  Number of NLRIs in the update sent: max 0, min 0

  Connections established 1; dropped 0
  Last reset never
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 192.168.1.2, Local port: 179
Foreign host: 192.168.1.1, Foreign port: 37725

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x12F4F2C):
Timer          Starts    Wakeups            Next
Retrans            14          0             0x0
TimeWait            0          0             0x0
AckHold            13          8             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
```

```
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss:  165379618  snduna:  165379963  sndnxt:  165379963     sndwnd:  16040
irs: 3127821601  rcvnxt: 3127821993  rcvwnd:      15993  delrcvwnd:    391

SRTT: 254 ms, RTTO: 619 ms, RTV: 365 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6

Datagrams (max data segment is 1460 bytes):
Rcvd: 20 (out of order: 0), with data: 15, total data bytes: 391
Sent: 22 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 04
```

トラブルシューティングのヒント

BGP ルータ間の基本的なネットワーク接続性を確認するには、**ping** コマンドを使用します。

次の作業

VPN で BGP ピアを使用している場合は、「IPv4 VRF アドレス ファミリ用に BGP ピアを設定」（P.25）に進みます。VPN で BGP ピアを使用していない場合は、「BGP ピアのカスタマイズ」（P.29）に進みます。

BGP ルーティング プロセスと 4 バイト自律システム番号を使用したピアの設定

BGP ピアが 4 バイト自律システム番号に配置されているときに、BGP ルーティング プロセスおよび BGP ピアを設定するには、この作業を実行します。ここで設定するアドレス ファミリは、デフォルトの IPv4 ユニキャスト アドレス ファミリで、設定は図 2（P.19）のルータ B で行われています。この作業にある 4 バイト自律システム番号は、デフォルトの asplain（10 進数値）形式にフォーマットされています。たとえば、図 2（P.19）にあるルータ B の自律システム番号は 65538 です。BGP ピアとなりうるネイバー ルータすべてについて、必ず、この作業を実行してください。

シスコシステムズが採用している 4 バイト自律システム番号

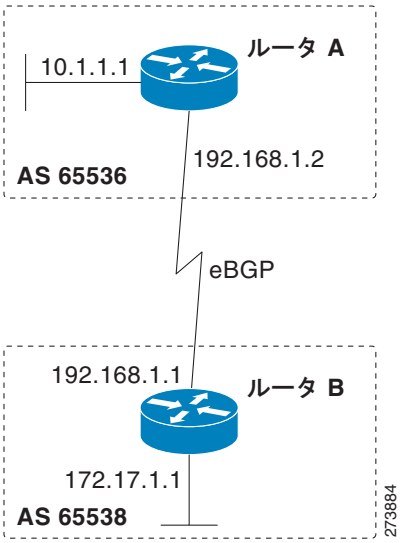
Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、およびそれ以降のリリースでは、シスコシステムズが採用している 4 バイト自律システム番号は、自律システム番号の正規表現のマッチングおよび出力表示形式のデフォルトとして asplain（たとえば、65538）を使用していますが、RFC 5396 に記載されているとおり、4 バイト自律システム番号を asplain 形式および asdot 形式の両方で設定できます。4 バイト自律システム番号の正規表現マッチングと出力表示のデフォルトを asdot 形式に変更するには、**bgp asnotation dot** コマンドに続けて、**clear ip bgp *** コマンドを実行し、現在の BGP セッションをすべてハード リセットします。4 バイト自律システム番号の詳細については、「BGP 自律システム番号の形式」（P.3）を参照してください。

Cisco IOS Release 12.0(32)S12、および 12.4(24)T では、シスコシステムズが採用している 4 バイト自律システム番号は、設定形式、正規表現とのマッチング、および出力表示として、asdot（たとえば、1.2）だけを使用しています。asplain はサポートしていません。asdot 表記法を使用して設定された、異なる 4 バイトの自律システムにある 3 つのネイバー ピアの間での設定例については、「BGP ルーティング プロセスと 4 バイト自律システム番号を使用したピアの設定：例」（P.78）を参照してください。

シスコは、BGP が 2 バイト自律システム番号から 4 バイト自律システム番号へ段階的に移行できるように開発された RFC 4893 もサポートしています。スムーズな移行を確実に行うには、4 バイト自律システム番号を使用して識別される自律システム内の BGP スピーカーをすべて、4 バイト自律システム番号をサポートするようにアップグレードすることを推奨します。

（注） 新しいプライベートの自律システム番号 23456 は RFC 4893 により作成されたもので、この番号を Cisco IOS CLI で自律システム番号として設定することはできません。

図 2　4 バイト番号を使用する 2 つの自律システム内の BGP ピア



前提条件

この作業を行うには、ルータで、Cisco IOS Release 12.0(32)SY8、12.2(33)SXI1、またはそれ以降のリリースが実行されている必要があります。

制約事項

デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義されたネイバーは、IPv4 ユニキャスト アドレス プレフィクスだけを交換します。IPv6 プレフィクスなど、その他のアドレス プレフィクス タイプを交換するには、その他のプレフィクス タイプについて、アドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用し、ネイバーをアクティブ化することも必要です。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. 必要に応じて、ステップ 4. を繰り返し、その他の BGP ネイバーを定義します。
6. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]

7. **neighbor** *ip-address* **activate**
8. 必要に応じて、ステップ 7. を繰り返し、その他の BGP ネイバーをアクティブ化します。
9. **network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]
10. **end**
11. **show ip bgp** [*network*] [*network-mask*]
12. **show ip bgp summary**

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 65538`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。 • この例では、4 バイト自律システム番号 65538 は asplain 表記法で定義されています。
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* **例：** `Router(config-router)# neighbor 192.168.1.2 remote-as 65536`	指定された自律システムのネイバーの IP アドレスを、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • この例では、4 バイト自律システム番号 65536 は asplain 表記法で定義されています。
ステップ 5	必要に応じて、ステップ 4 を繰り返し、その他の BGP ネイバーを定義します。	—
ステップ 6	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] **例：** `Router(config-router)# address-family ipv4 unicast`	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。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィクスを指定します。 • **vrf** キーワードと *vrf-name* 引数は、それ以降の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドと関連付けられる Virtual Routing and Forwarding（VRF; 仮想ルーティング/転送）インスタンスの名前を表します。

	コマンドまたはアクション	目的
ステップ 7	**neighbor** *ip-address* **activate** **例：** `Router(config-router-af)# neighbor 192.168.1.2 activate`	ネイバーが IPv4 ユニキャスト アドレス ファミリのプレフィクスをローカル ルータと交換できるようにします。
ステップ 8	必要に応じて、ステップ 7 を繰り返し、その他の BGP ネイバーをアクティブ化します。	—
ステップ 9	**network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*] **例：** `Router(config-router)# network 172.17.1.0 mask 255.255.255.0`	（任意）ネットワークを、この自律システムに対してローカルに設定し、BGP ルーティング テーブルに追加します。 • 外部プロトコルの場合、**network** コマンドはアドバタイズされるネットワークを制御します。内部プロトコルは **network** コマンドを使用して、アップデートの送信先を判断します。
ステップ 10	**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。
ステップ 11	**show ip bgp** [*network*] [*network-mask*] **例：** `Router# show ip bgp 10.1.1.0`	（任意）BGP ルーティング テーブル内のエントリを表示します。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 12	**show ip bgp summary** **例：** `Router# show ip bgp summary`	（任意）BGP 接続すべての状況を表示します。

例

次の例は、図 2（P.19）のルータ B で実行された **show ip bgp** コマンドの出力ですが、ここにはルータ A で 192.168.1.2 にある BGP ネイバーから学習されたネットワーク 10.1.1.0 に対する BGP ルーティング テーブル エントリと、デフォルトの asplain 形式で表した 4 バイト自律システム番号 65536 が表示されています。

```
RouterB# show ip bgp 10.1.1.0

BGP routing table entry for 10.1.1.0/24, version 2
Paths: (1 available, best #1)
  Advertised to update-groups:
     2
  65536
    192.168.1.2 from 192.168.1.2 (10.1.1.99)
      Origin IGP, metric 0, localpref 100, valid, external, best
```

次の例は、**show ip bgp summary** コマンドの出力ですが、ここには、図 2（P.19）のルータ B でこの作業を設定した後で、ルータ A にある BGP ネイバー 192.168.1.2 の 4 バイト自律システム番号が 65536 であることが表示されています。

```
RouterB# show ip bgp summary

BGP router identifier 172.17.1.99, local AS number 65538
```

```
BGP table version is 3, main routing table version 3
2 network entries using 234 bytes of memory
2 path entries using 104 bytes of memory
3/2 BGP path/bestpath attribute entries using 444 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 806 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down  Stated
192.168.1.2     4       65536       6       6        3    0    0 00:01:33       1
```

トラブルシューティングのヒント

BGP ルータ間の基本的なネットワーク接続性を確認するには、**ping** コマンドを使用します。

4 バイト自律システム番号で使用される出力および正規表現とのマッチング形式のデフォルトを変更

4 バイト自律システム番号のデフォルト出力形式を asplain 形式から asdot 表記法形式に変更するには、この作業を実行します。4 バイト自律システム番号の出力形式の変化を表示するには、**show ip bgp summary** コマンドを使用します。

4 バイト自律システム番号の詳細については、「BGP 自律システム番号の形式」（P.3）を参照してください。

前提条件

この例では、ルータで、Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、またはそれ以降のリリースが実行されている必要があります。

手順の概要

1. **enable**
2. **show ip bgp summary**
3. **configure terminal**
4. **router bgp** *autonomous-system-number*
5. **bgp asnotation dot**
6. **end**
7. **clear ip bgp ***
8. **show ip bgp summary**
9. **show ip bgp regexp** *regexp*
10. **configure terminal**
11. **router bgp** *autonomous-system-number*
12. **no bgp asnotation dot**
13. **end**
14. **clear ip bgp ***

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	**show ip bgp summary** **例：** `Router# show ip bgp summary`	BGP 接続すべての状況を表示します。
ステップ 3	**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 4	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 65538`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。 • この例では、4 バイト自律システム番号 65538 は asplain 表記法で定義されています。
ステップ 5	**bgp asnotation dot** **例：** `Router(config-router)# bgp asnotation dot`	BGP 4 バイト自律システム番号のデフォルト出力形式を asplain（10 進数値）からドット表記法に変更します。 **（注）** 4 バイト自律システム番号は、asplain 形式、または asdot 形式を使用して設定できます。このコマンドの影響を受けるのは、**show** コマンドの出力、または正規表現のマッチングだけです。
ステップ 6	**end** **例：** `Router(config-router)# 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。
ステップ 7	**clear ip bgp *** **例：** `Router# clear ip bgp *`	現在の BGP セッションをすべてクリアし、リセットします。 • この例では、4 バイト自律システム番号形式の変更がすべての BGP セッションに反映されていることを確認するために、ハード リセットが実行されています。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 8	**show ip bgp summary** **例：** `Router# show ip bgp summary`	BGP 接続すべての状況を表示します。
ステップ 9	**show ip bgp regexp** *regexp* **例：** `Router# show ip bgp regexp ^1\.0$`	自律システム パスの正規表現と一致するルートを表示します。 • この例では、4 バイトの自律システム パスをマッチングする正規表現は、asdot 形式で設定されています。

	コマンドまたはアクション	目的
ステップ 10	**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 11	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 65538`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。 • この例では、4 バイト自律システム番号 65538 は asplain 表記法で定義されています。
ステップ 12	**no bgp asnotation dot** **例：** `Router(config-router)# no bgp asnotation dot`	BGP 4 バイト自律システム番号のデフォルト出力形式を asplain（10 進数値）にリセットします。 **（注）** 4 バイト自律システム番号は、asplain 形式、または asdot 形式を使用して設定できます。このコマンドの影響を受けるのは、**show** コマンドの出力、または正規表現のマッチングだけです。
ステップ 13	**end** **例：** `Router(config-router)# end`	ルータ 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。
ステップ 14	**clear ip bgp *** **例：** `Router# clear ip bgp *`	現在の BGP セッションをすべてクリアし、リセットします。 • この例では、4 バイト自律システム番号形式の変更がすべての BGP セッションに反映されていることを確認するために、ハード リセットが実行されています。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次の **show ip bgp summary** コマンドの出力は、4 バイト自律システム番号のデフォルト asplain 形式を示しています。ここで、asplain 形式で表された 4 バイト自律システム番号 65536 および 65550 に注意してください。

```
Router# show ip bgp summary

BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4        65536       7       7        1    0    0 00:03:04       0
192.168.3.2     4        65550       4       4        1    0    0 00:00:15       0
```

bgp asnotation dot コマンドの設定後（これに、現在の BGP セッションをすべてハード リセットする **clear ip bgp *** コマンドが続きます）、出力は、次の **show ip bgp summary** コマンドの出力に示すように、asdot 表記法の形式に変換されます。asdot 形式で表された 4 バイト自律システム番号 1.0 および 1.14 に注意してください。これらは自律システム番号 65536 と 65550 を asdot 変換したものです。

```
Router# show ip bgp summary

BGP router identifier 172.17.1.99, local AS number 1.2
```

```
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4          1.0       9       9        1    0    0 00:04:13        0
192.168.3.2     4         1.14       6       6        1    0    0 00:01:24        0
```

bgp asnotation dot コマンドの設定後（これに、現在の BGP セッションをすべてハード リセットする **clear ip bgp *** コマンドが続きます）、4 バイトの自律システム パスで使用される正規表現とのマッチング形式は asdot 表記法の形式に変更されます。4 バイト自律システム番号は、asplain 形式または asdot 形式のいずれかを使用して、正規表現で設定できますが、現在のデフォルト形式を使用して設定された 4 バイト自律システム番号だけがマッチングされます。下の先頭の例では、**show ip bgp regexp** コマンドは、asplain 形式で表された 4 バイト自律システム番号を使って設定されています。現在のデフォルト形式は asdot 形式なのでマッチングは失敗し、何も出力されません。asdot 形式を使用した 2 番目の例では、マッチングは成功し、4 バイトの自律システム パスに関する情報が asdot 表記法を使って表示されます。

（注） この asdot 表記法で使用されているピリオドは、シスコの正規表現では特殊文字です。特殊な意味を取り除くには、ピリオドの前にバックスラッシュをつけます。

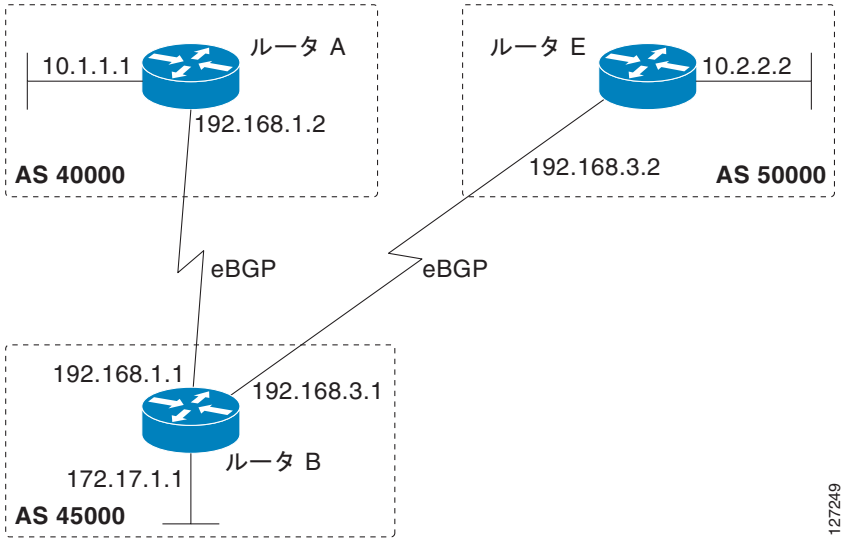
```
Router# show ip bgp regexp ^65536$


Router# show ip bgp regexp ^1\.0$

BGP table version is 2, local router ID is 172.17.1.99
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
*> 10.1.1.0/24      192.168.1.2              0             0 1.0 i
```

IPv4 VRF アドレス ファミリ用に BGP ピアを設定

VPN 内に存在するため IPv4 VRF 情報を交換しなければならない 2 つの IPv4 ルータ（ピア）の間に BGP を設定するには、次の作業を任意で実行します。ここで設定するアドレス ファミリは IPv4 VRF アドレス ファミリで、設定は図 3 のルータ B で自律システム 50000 のルータ E にあるネイバー 192.168.3.2 を使って行われています。BGP IPv4 VRF アドレス ファミリ ピアとなりうるネイバー ルータすべてについて、必ず、この作業を実行してください。

（注） この作業は、VPN ルーティングに必要な設定をすべて示しているわけではありません。完全な設定サンプル、および 4 バイト自律システム番号を使用する、ルート ターゲットを使った VRF の作成方法を示した設定サンプルについては、「4 バイトの BGP 自律システム番号を使用した VRF および拡張コミュニティの設定：例」（P.81）を参照してください。

図 3　IPv4 VRF アドレス ファミリ用 BGP トポロジ



前提条件

この作業を実行する前に、「BGP ルーティング プロセスの設定」の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
6. **exit**
7. **router bgp** *autonomous-system-number*
8. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
9. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
10. **neighbor** {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**restart** *restart-interval*] [**warning-only**]
11. **neighbor** *ip-address* **activate**
12. **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 vpn1`	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 45000:5`	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。 • インポートおよびエクスポート ルーティング情報の両方をターゲット VPN 拡張コミュニティへインポートするには、**both** キーワードを使用します。 • ルート ターゲット拡張コミュニティ アトリビュートを VRF のインポート、エクスポート、または両方（インポートとエクスポート）のルート ターゲット拡張コミュニティ リストに追加するには、*route-target-ext-community* 引数を使用します。
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	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 45000`	指定されたルーティング プロセスでルータ 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 8	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] **例：** `Router(config-router)# address-family ipv4 vrf vpn1`	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。 • IPv4 ユニキャスト アドレス ファミリを指定するには、キーワード **unicast** を使用します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • IPv4 マルチキャスト アドレス プレフィクスを指定するには、**multicast** キーワードを使用します。 • 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。
ステップ 9	**neighbor** *ip-address* **remote-as** *autonomous-system-number* **例：** `Router(config-router-af)# neighbor 192.168.3.2 remote-as 45000`	指定された自律システムのネイバーの IP アドレスを、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 10	**neighbor** {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**restart** *restart-interval*] [**warning-only**] **例：** `Router(config-router-af)# neighbor 192.168.3.2 maximum-prefix 10000 warning-only`	ネイバーから受信できるプレフィクスの数を制御します。 • 特定のネイバーから受信できるプレフィクス数の最大値を指定するには、*maximum* 引数を使用します。設定可能なプレフィクス数を制限するものは、ルータ上で使用可能なシステム リソースだけです。 • プレフィクスの上限をパーセント単位で表した整数を指定するには、*threshold* 引数を使用します。この上限に達すると、ルータは警告メッセージの生成を開始します。 • プレフィクスの上限を超えた場合に、ピアリング セッションを終了する代わりに、ログ メッセージを生成するようにルータを設定するには、**warning-only** キーワードを使用します。
ステップ 11	**neighbor** *ip-address* **activate** **例：** `Router(config-router-af)# neighbor 192.168.3.2 activate`	ネイバーが IPv4 VRF アドレス ファミリのプレフィクスをローカル ルータと交換できるようにします。
ステップ 12	**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 モードを開始します。

トラブルシューティングのヒント

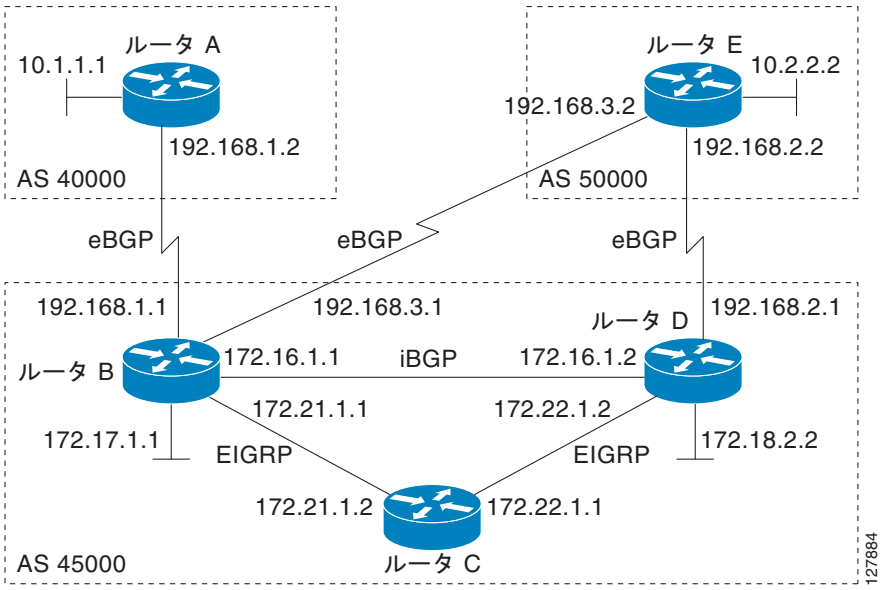
BGP ルータ間の基本的なネットワーク接続を検証するには **ping** コマンドを使用します。また、VRF インスタンスが作成されたことを確認するには **show ip vrf** コマンドを使用します。

BGP ピアのカスタマイズ

BGP ピアをカスタマイズするには、次の作業を実行します。この作業の手順の多くは任意ですが、ネイバーとアドレス ファミリ コンフィギュレーション コマンドの関係がどのように機能しているかを示しています。IPv4 マルチキャスト アドレス ファミリの例を使用して、IPv4 マルチキャスト アドレス ファミリを設定する前に、ネイバー アドレス ファミリに依存しないコマンドが設定されます。その後、アドレス ファミリに依存するコマンドが設定され、**exit address-family** コマンドが表示されます。任意の手順は、ネイバーをディセーブルにする方法を示しています。

図 4 では、この作業のコンフィギュレーションがルータ B で行われます。2 つのルータの間で BGP プロセスを完全に実現するには、たとえば、ルータ E で IP アドレスを適宜、変更してこのコンフィギュレーションを繰り返す必要があります。

図 4　　BGP ピア トポロジ



制約事項

デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義されたネイバーは、IPv4 ユニキャスト アドレス プレフィクスだけを交換します。IPv6 プレフィクスなど、その他のアドレス プレフィクス タイプを交換するには、アドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用し、ネイバーをアクティブ化することも必要です。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **no bgp default ipv4-unicast**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **description** *text*

7. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
8. **network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]
9. **neighbor** {*ip-address* | *peer-group-name*} **activate**
10. **neighbor** {*ip-address* | *peer-group-name*} **advertisement-interval** *seconds*
11. **neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*]
12. **exit-address-family**
13. **neighbor** {*ip-address* | *peer-group-name*} **shutdown**
14. **end**
15. **show ip bgp ipv4 multicast** [*command*]
16. **show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes** | **received** *prefix-filter*]]

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`	指定されたルーティング プロセスでルータ 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	**no bgp default ipv4-unicast** **例：** `Router(config-router)# no bgp default ipv4-unicast`	BGP ルーティング プロセスで使用される IPv4 ユニキャスト アドレス ファミリをディセーブルにします。 **（注）** IPv4 ユニキャスト アドレス ファミリのルーティング情報は、**neighbor remote-as** ルータ コンフィギュレーション コマンドで設定された各 BGP ルーティング セッションに対して、デフォルトでアドバタイズされます。ただし、**neighbor remote-as** コマンドを設定する前に、**no bgp default ipv4-unicast** ルータ コンフィギュレーション コマンドを設定した場合は例外です。既存のネイバー コンフィギュレーションは影響されません。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* **例：** `Router(config-router)# neighbor 192.168.3.2 remote-as 50000`	指定された自律システムのネイバーの IP アドレスを、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。

	コマンドまたはアクション	目的
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **description** *text* **例：** `Router(config-router)# neighbor 192.168.3.2 description finance`	（任意）テキストによる説明を指定されたネイバーと関連付けます。
ステップ 7	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] **例：** `Router(config-router)# address-family ipv4 multicast`	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。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィクスを指定します。 • **vrf** キーワードと *vrf-name* 引数は、後続の 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 インスタンスの名前を指定します。
ステップ 8	**network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*] **例：** `Router(config-router-af)# network 172.17.1.0 mask 255.255.255.0`	（任意）ネットワークを、この自律システムに対してローカルに設定し、BGP ルーティング テーブルに追加します。 • 外部プロトコルの場合、**network** コマンドはアドバタイズされるネットワークを制御します。内部プロトコルは **network** コマンドを使用して、アップデートの送信先を判断します。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*} **activate** **例：** `Router(config-router-af)# neighbor 192.168.3.2 activate`	BGP ネイバーとの情報の交換をイネーブルにします。
ステップ 10	**neighbor** {*ip-address* | *peer-group-name*} **advertisement-interval** *seconds* **例：** `Router(config-router-af)# neighbor 192.168.3.2 advertisement-interval 25`	（任意）BGP ルーティング アップデートの最小送信間隔を設定します。
ステップ 11	**neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*] **例：** `Router(config-router-af)# neighbor 192.168.3.2 default-originate`	（任意）デフォルト ルートとして使用するために、BGP スピーカー（ローカル ルータ）がデフォルト ルート 0.0.0.0 をピアに送信することを許可します。
ステップ 12	**exit-address-family** **例：** `Router(config-router-af)# exit-address-family`	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、ルータ 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 13	**neighbor** {*ip-address* | *peer-group-name*} **shutdown** **例：** `Router(config-router)# neighbor 192.168.3.2 shutdown`	（任意）BGP ピア、またはピア グループをディセーブルにします。 **（注）** このステップを実行すると、ネイバーがディセーブルにされるため、この後の **show** コマンドを使ったステップをいずれも実行できなくなります。
ステップ 14	**end** **例：** `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 15	**show ip bgp ipv4 multicast** [*command*] **例：** `Router# show ip bgp ipv4 multicast`	（任意）IPv4 マルチキャスト データベース関連情報を表示します。 • サポートされているマルチプロトコル BGP コマンドがあれば、*command* 引数を使用して指定します。サポートされているコマンドを表示するには、CLI で ? プロンプトを使用します。
ステップ 16	**show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes** | **received prefix-filter**]] **例：** `Router# show ip bgp neighbors 192.168.3.2`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。

例

次に、この作業を図 4（P.29）のルータ B およびルータ E で設定した後で、ルータ B の BGP IPv4 マルチキャスト情報を表示する **show ip bgp ipv4 multicast** コマンドの出力例を示します。IPv4 マルチキャスト アドレス ファミリの下に設定されている各ルータに対してローカルなネットワークは、出力テーブルに表示されます。

```
BGP table version is 3, local router ID is 172.17.1.99
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
*> 10.2.2.0/24      192.168.3.2              0             0 50000 i
*> 172.17.1.0/24    0.0.0.0                  0         32768 i
```

次は、ネイバー 192.168.3.2 に対する **show ip bgp neighbors** コマンドからの出力例の一部分ですが、これにはこのネイバーに関する一般的な BGP 情報と、具体的な BGP IPv4 マルチキャスト アドレス ファミリ情報が表示されます。このコマンドは、図 4（P.29）のルータ B とルータ E でこの作業を設定した後、ルータ B で入力されたものです。

```
BGP neighbor is 192.168.3.2,  remote AS 50000, external link
 Description: finance
  BGP version 4, remote router ID 10.2.2.99
  BGP state = Established, up for 01:48:27
  Last read 00:00:26, last write 00:00:26, hold time is 120, keepalive intervals
  Configured hold time is 120,keepalive interval is 70 seconds, Minimum holdtims
  Neighbor capabilities:
    Route refresh: advertised and received (old & new)
    Address family IPv4 Unicast: advertised
    Address family IPv4 Multicast: advertised and received
```

```
!
 For address family: IPv4 Multicast
  BGP table version 3, neighbor version 3/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
    Uses NEXT_HOP attribute for MBGP NLRIs
                                 Sent       Rcvd
  Prefix activity:               ----       ----
    Prefixes Current:               1          1 (Consumes 48 bytes)
    Prefixes Total:                 1          1
    Implicit Withdraw:              0          0
    Explicit Withdraw:              0          0
    Used as bestpath:             n/a          1
    Used as multipath:            n/a          0

                                   Outbound    Inbound
  Local Policy Denied Prefixes:    --------    -------
    Bestpath from this peer:              1        n/a
    Total:                                1          0
  Number of NLRIs in the update sent: max 0, min 0
  Minimum time between advertisement runs is 25 seconds

  Connections established 8; dropped 7
  Last reset 01:48:54, due to User reset
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 192.168.3.1, Local port: 13172
Foreign host: 192.168.3.2, Foreign port: 179
!
```

再配布の例を使用した BGP コンフィギュレーション コマンドの削除

小規模な BGP ネットワークであっても、BGP CLI コンフィギュレーションは非常に複雑になることがあります。すべての CLI コンフィギュレーションを削除する必要がある場合は、CLI を削除することで生じるあらゆる影響を考慮する必要があります。現在の実行コンフィギュレーションを分析し、現在の BGP ネイバー関係、アドレス ファミリの考慮事項、その他の設定済みルーティング プロトコルを判断します。BGP CLI コマンドの多くは、CLI コンフィギュレーションのその他の部分に影響を与えています。

EIGRP への BGP ルートの再配布で使用されている BGP コンフィギュレーション コマンドをすべて削除するには、この作業を実行します。ルート マップをパラメータのマッチングや設定、再配布ルートのフィルタに使用して、これらのルートが EIGRP によりアドバタイズされるときに、ルーティング ループが発生しないようにすることができます。BGP コンフィギュレーション コマンドを削除する場合は、必ず、関連するコマンドをすべて削除、またはディセーブルにしてください。この例では、**route-map** CLI を削除しても、再配布は行われ、ルート マップのフィルタリングが取り除かれているために、予期しない結果となる可能性があります。単に **redistribute** CLI を削除するだけでは、ルート マップは適用されませんが、実行コンフィギュレーションに未使用の CLI が残ります。

BGP CLI の削除の詳細については、「Cisco BGP Overview」モジュールの「BGP CLI Removal Considerations」の概念を参照してください。

CLI を削除する前と後の再配布コンフィギュレーションの表示については、「再配布の例を使用した BGP コンフィギュレーション コマンドの削除：例」（P.84）を参照してください。

手順の概要

1. **enable**

2. **configure terminal**
3. **no route-map** *map-tag*
4. **router eigrp** *autonomous-system-number*
5. **no redistribute** *protocol* [*as-number*]
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	**no route-map** *map-name* **例：** `Router(config)# no route-map bgp-to-eigrp`	実行コンフィギュレーションからルート マップを削除します。 • この例では、bgp-to-eigrp というルート マップがコンフィギュレーションから削除されています。
ステップ 4	**router eigrp** *autonomous-system-number* **例：** `Router(config)# router eigrp 100`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
ステップ 5	**no redistribute** *protocol* [*as-number*] **例：** `Router(config-router)# no redistribute bgp 45000`	あるルーティング ドメインから別のルーティング ドメインへのルートの再配布をディセーブルにします。 • この例では、EIGRP ルーティング プロセスへの BGP ルートの再配布のコンフィギュレーションが、実行コンフィギュレーションから削除されています。 **（注）** オリジナルの **redistribute** コマンド コンフィギュレーションにルート マップが含まれていた場合は、この作業例のステップ 3 にあるとおり、**route-map** コマンド コンフィギュレーションを必ず削除してください。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

	コマンドまたはアクション	目的
ステップ 6	**end** **例：** `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 7	**show running-config** **例：** `Router# show running-config`	（任意）ルータの現在の実行コンフィギュレーションを表示します。 • このコマンドは、ルータ コンフィギュレーションから、**redistribute** および **route-map** コマンドが削除されたことを確認するために使用します。

基本的な BGP のモニタリングとメンテナンス

ここでは、基本的な BGP プロセスとピア関係についての情報のリセットおよび表示に関する作業を説明します。BGP ネイバーになるように定義された 2 つのルータは、BGP 接続を形成し、ルーティング情報を交換します。その後、BGP フィルタ、重み、距離、バージョン、タイマーなどを変更したり、何らかのコンフィギュレーション変更を行ったりした場合、コンフィギュレーションの変更を有効にするために、BGP 接続のリセットが必要になることがあります。

- 「ルート リフレッシュ機能が失われたときのインバウンド ソフト再構成を設定」（P.37）
- 「基本 BGP 情報のリセットと表示」（P.40）

ルーティング ポリシーの変更管理

ピアのルーティング ポリシーには、インバウンドまたはアウトバウンド ルーティング テーブルの更新に影響する可能性のあるルート マップ、配布リスト、プレフィクス リスト、フィルタ リストなど、すべての要素に関するコンフィギュレーションが含まれています。ルーティング ポリシーを変更した場合、変更後のポリシーを有効にするには、必ず BGP セッションをソフト クリア、またはソフト リセットしてください。インバウンド リセットを実行すると、ルータで設定されている新しいインバウンド ポリシーが有効になります。アウトバウンド リセットを実行すると、BGP セッションをリセットしなくても、ルータで設定されている新しいローカル アウトバウンド ポリシーが有効になります。アウトバウンド ポリシーのリセット中に、新しい一連のアップデートが送信されると、ネイバーの新しいインバウンド ポリシーも有効になります。つまり、インバウンド ポリシーの変更後は、ローカル ルータでインバウンド リセットを実行するか、ピア ルータでアウトバウンド リセットを実行する必要があります。アウトバウンド ポリシーを変更した場合は、ローカル ルータでのアウトバウンド リセット、またはピア ルータでのインバウンド リセットが必要になります。

リセットには、ハード リセットとソフト リセットの 2 種類があります。表 5 は、これらの利点と欠点をまとめたものです。

表 5　ハード リセットとソフト リセットの長所と短所

リセットのタイプ	長所	短所
ハード リセット	メモリ オーバーヘッドが起こらない。	ネイバーにより提供される BGP、IP、および Forwarding Information Base（FIB; 転送情報ベース）テーブル内のプレフィクスが失われる。推奨されない。
アウトバウンド ソフト リセット	設定が必要ない。ルーティング テーブル アップデートの保存が必要ない。	インバウンド ルーティング テーブル アップデートがリセットされない。

表 5　ハード リセットとソフト リセットの長所と短所 （続き）

リセットのタイプ	長所	短所
ダイナミック インバウンド ソフト リセット	BGP セッションおよびキャッシュがクリアされない。 ルーティング テーブル アップデートの保存が必要ない。また、メモリのオーバーヘッドが発生しない。	両方の BGP ルータでルート リフレッシュ機能（Cisco IOS Release 12.1 以降）がサポートされている必要がある。 **（注）** アウトバウンド ルーティング テーブル アップデートがリセットされない。
設定済みのインバウンド ソフト リセット（**neighbor soft-reconfiguration** ルータ コンフィギュレーション コマンドを使用）	どちらの BGP ルータも自動ルート リフレッシュ機能をサポートしていない場合に使用可能。 Cisco IOS Release 12.3(14)T では、ルート リフレッシュ機能をサポートしていないピアに対してインバウンド ソフト再構成を設定するための **bgp soft-reconfig-backup** コマンドが導入されている。	再構成が必要である。 受信した（インバウンド）ルーティング ポリシー アップデートをすべてそのまま格納するため、メモリが大量に使用される。 どちらの BGP ルータも自動ルート リフレッシュ機能をサポートしていない場合など、絶対に必要な場合だけ推奨される。 **（注）** アウトバウンド ルーティング テーブル アップデートがリセットされない。

BGP ネイバーになるように定義された 2 つのルータは、BGP 接続を形成し、ルーティング情報を交換します。その後、BGP フィルタ、重み、距離、バージョン、タイマーなどを変更したり、何らかのコンフィギュレーション変更を行ったりした場合、コンフィギュレーションの変更を有効にするために、BGP 接続をリセットする必要があります。

ソフト リセットは、インバウンドおよびアウトバウンド ルーティング アップデートで使用されるルーティング テーブルをアップデートします。Cisco IOS Release 12.1 以降では、事前設定を必要としないソフト リセットがサポートされています。このソフト リセットにより、BGP ルータの間でルート リフレッシュ要求やルーティング情報をダイナミックに交換し、対応するアウトバウンド ルーティング テーブルをアドバタイズできるようになります。ソフト リセットには 2 種類があります。

- ソフト リセットを使用して、ネイバーからインバウンド アップデートを生成することを、ダイナミック インバウンド ソフト リセットと呼びます。
- ソフト リセットを使用して、ネイバーに新しい一連のアップデートを送信することを、アウトバウンド ソフト リセットと呼びます。

事前にコンフィギュレーションを行わずにソフト リセットを使用するためには、BGP ピアでソフト ルート リフレッシュ機能がサポートされていなければなりません。これは、ピアが TCP セッションを確立したときに送信される OPEN メッセージでアドバタイズされます。リリース 12.1 以前の Cisco IOS リリースが実行されているルータでは、ルート リフレッシュ機能はサポートされていないため、**neighbor soft-reconfiguration** ルータ コンフィギュレーション コマンドを使用して、BGP セッションをクリアする必要があります。この方法で BGP セッションをクリアすると、ネットワークの動作が悪い影響を受けるため、これは最後の手段として使用してください。

ルート リフレッシュ機能が失われたときのインバウンド ソフト再構成を設定

ルート リフレッシュ機能をサポートしていない BGP ピアに対して、**bgp soft-reconfig-backup** コマンドを使用してインバウンド ソフトコンフィギュレーションを設定するには、この作業を実行します。このコマンドを設定しても、ルート リフレッシュ機能をサポートしている BGP ピアは影響されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp log-neighbor-changes**
5. **bgp soft-reconfig-backup**
6. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
7. **neighbor** {*ip-address* | *peer-group-name*} **soft-reconfiguration** [**inbound**]
8. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
9. soft-reconfiguration inbound を使って設定される各ピアについて、ステップ 6 ～ 8 を繰り返します。
10. **exit**
11. **route-map** *map-tag* [**permit** | **deny**] [**sequence-number**]
12. **set local-preference** *number-value*
13. **end**
14. **show ip bgp neighbors** [*neighbor-address*]
15. **show ip bgp** [*network*] [*network-mask*]

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`	指定されたルーティング プロセスでルータ 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	**bgp log-neighbor-changes** **例：** `Router(config-router)# bgp log-neighbor-changes`	BGP ネイバー リセットのロギングをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**bgp soft-reconfig-backup** **例：** `Router(config-router)# bgp soft-reconfig-backup`	ルート リフレッシュ機能をサポートしていないピアに対して、インバウンド ソフトウェア再構成を実行するように、BGP スピーカーを設定します。 • このコマンドは、ルート リフレッシュ機能をサポートしていないピアに対して、インバウンド ソフトウェア再構成を実行するように、BGP スピーカーを設定するために使用します。このコマンドの設定により、必要な場合にだけ、アップデート（ソフト再構成）を格納するように、BGP を設定することができます。このコマンドを設定しても、ルート リフレッシュ機能をサポートしているピアは影響されません。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* **例：** `Router(config-router)# neighbor 192.168.1.2 remote-as 40000`	指定された自律システムのネイバーの IP アドレスを、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **soft-reconfiguration** [**inbound**] **例：** `Router(config-router)# neighbor 192.168.1.2 soft-reconfiguration inbound`	アップデートの格納を開始するように、Cisco IOS ソフトウェアを設定します。 • このネイバーから受信したアップデートは、インバウンド ポリシーに関係なく、すべてそのまま格納されます。インバウンド ソフトウェア再構成を後で行う場合、格納された情報を使用して、新たに一連のインバウンド アップデートが生成されます。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**} **例：** `Router(config-router)# neighbor 192.168.1.2 route-map LOCAL in`	受信または発信ルートにルート マップを適用します。 • この例では、LOCAL という名前のルート マップが着信ルートに適用されます。
ステップ 9	soft-reconfiguration inbound を使って設定される各ピアについて、ステップ 6 ～ 8 を繰り返します。	—
ステップ 10	**exit** **例：** `Router(config-router)# exit`	ルータ 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 11	**route-map** *map-name* [**permit** | **deny**] [**sequence-number**] **例：** `Router(config)# route-map LOCAL permit 10`	ルート マップを設定し、ルート マップ コンフィギュレーション モードを開始します。 • この例では、LOCAL という名前のルート マップが作成されます。
ステップ 12	**set local-preference** *number-value* **例：** `Router(config-route-map)# set local-preference 200`	自律システム パスのプリファレンス値を指定します。 • この例では、ローカル プリファレンス値は 200 に設定されています。

	コマンドまたはアクション	目的
ステップ 13	**end** **例：** `Router(config-route-map)# end`	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 モードを開始します。
ステップ 14	**show ip bgp neighbors** [*neighbor-address*] **例：** `Router(config-router-af)# show ip bgp neighbors 192.168.1.2`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 15	**show ip bgp** [*network*] [*network-mask*] **例：** `Router# show ip bgp`	（任意）BGP ルーティング テーブル内のエントリを表示します。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次に、BGP ネイバー 192.168.2.1 への TCP および BGP 接続に関する情報を表示する **show ip bgp neighbors** コマンドの出力例の一部を示します。このピアでは、ルート リフレッシュがサポートされています。

```
BGP neighbor is 192.168.1.2,  remote AS 40000, external link
 Neighbor capabilities:
   Route refresh: advertised and received(new)
```

次に、BGP ネイバー 192.168.3.2 への TCP および BGP 接続に関する情報を表示する **show ip bgp neighbors** コマンドの出力例の一部を示します。このピアでは、ルート リフレッシュがサポートされておらず、インバウンド ポリシー アップデートを更新する方法が他にはないため、BGP ピア 192.168.3.2 の soft-reconfig inbound パスが保存されます。

```
BGP neighbor is 192.168.3.2,  remote AS 50000, external link
 Neighbor capabilities:
   Route refresh: advertised
```

次の **show ip bgp** コマンドの出力例には、ネットワーク 172.17.1.0 のエントリがあります。BGP ピアは両方とも 172.17.1.0/24 をアドバタイズしていますが、192.168.3.2 については、received-only パスだけが格納されます。

```
BGP routing table entry for 172.17.1.0/24, version 11
Paths: (3 available, best #3, table Default-IP-Routing-Table, RIB-failure(4))
Flag: 0x820
 Advertised to update-groups:
    1
 50000
   192.168.3.2 from 192.168.3.2 (172.17.1.0)
     Origin incomplete, metric 0, localpref 200, valid, external
 50000, (received-only)
   192.168.3.2 from 192.168.3.2 (172.17.1.0)
     Origin incomplete, metric 0, localpref 100, valid, external
 40000
   192.168.1.2 from 192.168.1.2 (172.16.1.0)
     Origin incomplete, metric 0, localpref 200, valid, external, best
```

基本 BGP 情報のリセットと表示

基本 BGP プロセスとピア関係に関する情報をリセットおよび表示するには、この作業を実行します。

手順の概要

1. **enable**
2. **clear ip bgp** {***** | *autonomous-system-number* | *neighbor-address*} [**soft** [**in** | **out**]
3. **show ip bgp** [*network-address*] [*network-mask*] [**longer-prefixes**] [**prefix-list** *prefix-list-name* | **route-map** *route-map-name*] [**shorter prefixes** *mask-length*]
4. **show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes** | **received** *prefix-filter*]]
5. **show ip bgp paths**
6. **show ip bgp summary**

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 **clear ip bgp** {***** | *autonomous-system-number* | *neighbor-address*}} [**soft** [**in** | **out**]

BGP ネイバー セッションをクリアおよびリセットするにはこのコマンドを使用します。特定のネイバーをクリアするには *neighbor-address* 引数、自律システムにあるすべてのピアをクリアするには *autonomous-system-number* 引数を使用します。引数が指定されていない場合、このコマンドは BGP ネイバー セッションをすべてクリアし、リセットします。

（注） また、**clear ip bgp *** コマンドは内部 BGP 構造をすべてクリアするため、トラブルシューティング ツールとして便利です。

次に、BGP ネイバー セッションをすべてクリアし、リセットする例を示します。Cisco IOS Release 12.2(25)S 以降の構文では **clear ip bgp all** です。

```
Router# clear ip bgp *
```

ステップ 3 **show ip bgp** [*network-address*] [*network-mask*] [**longer-prefixes**] [**prefix-list** *prefix-list-name* | **route-map** *route-map-name*] [**shorter prefixes** *mask-length*]

BGP ルーティング テーブル内のエントリをすべて表示するには、このコマンドを使用します。次に、10.1.1.0 ネットワークの BGP ルーティング テーブル情報を表示する例を示します。

```
Router# show ip bgp 10.1.1.0 255.255.255.0

BGP routing table entry for 10.1.1.0/24, version 2
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Advertised to update-groups:
     1
  40000
    192.168.1.2 from 192.168.1.2 (10.1.1.99)
      Origin IGP, metric 0, localpref 100, valid, external, best
```

ステップ 4 **show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes** | **received** *prefix-filter*]]

TCP および BGP 接続に関する情報をネイバーに表示するには、このコマンドを使用します。

次の例は、図 3（P.26）のルータ B から、ルータ E にある BGP ネイバー 192.168.3.2 にアドバタイズされるルートを示しています。

```
Router# show ip bgp neighbors 192.168.3.2 advertised-routes

BGP table version is 3, local router ID is 172.17.1.99
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
*> 10.1.1.0/24      192.168.1.2              0             0 40000 i
*> 172.17.1.0/24    0.0.0.0                  0         32768 i

Total number of prefixes 2
```

ステップ 5 **show ip bgp paths**

データベースにある BGP パスをすべて表示するには、このコマンドを使用します。次に、図 4（P.29）のルータ B に対する BGP パス情報を表示する例を示します。

```
Router# show ip bgp paths

Address    Hash Refcount Metric Path
0x2FB5DB0     0        5      0 i
0x2FB5C90     1        4      0 i
0x2FB5C00  1361        2      0 50000 i
0x2FB5D20  2625        2      0 40000 i
```

ステップ 6 **show ip bgp summary**

BGP パスすべてのステータスを表示するには、このコマンドを使用します。次に、図 4（P.29）のルータ B に対する BGP ルーティング テーブル情報を表示する例を示します。

```
Router# show ip bgp summary

BGP router identifier 172.17.1.99, local AS number 45000
BGP table version is 3, main routing table version 3
2 network entries using 234 bytes of memory
2 path entries using 104 bytes of memory
4/2 BGP path/bestpath attribute entries using 496 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 882 total bytes of memory
BGP activity 14/10 prefixes, 16/12 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.1.2     4 40000     667     672        3    0    0 00:03:49        1
192.168.3.2     4 50000     468     467        0    0    0 00:03:49 (NoNeg)
```

BGP を使用したルート プレフィクスの集約

BGP ピアは、ローカル ネットワークに関する情報を交換しますが、このために、BGP ルーティング テーブルはすぐに巨大になります。CIDR は、ルーティング テーブルのサイズを最小限に抑えるため、集約ルート（*supernets*）の作成を可能にします。BGP ルーティング テーブルが小さければ小さいほど、ネットワークのコンバージェンス時間が短縮され、ネットワークのパフォーマンスが高まります。集約されたルートは、BGP を使用して、設定およびアドバタイズできます。集約の中には、サマリー ルートだけをアドバタイズするものもありますが、別の方法を使ってルートを集約すると、より具体的なルートが転送できるようになります。集約は、BGP ルーティング テーブルに存在するルートだけに適用されます。集約されたルートは、BGP ルーティング テーブルに具体的な集約ルートが少なくともあと 1 つ存在する場合に転送されます。BGP 内でルートを集約するには、次の作業のいずれかを行います。

BGP へのスタティック集約ルートの再配布

スタティック集約ルートを BPG に再配布するには、この作業を使用します。スタティック集約ルートは設定後、BGP ルーティング テーブルに再配布されます。スタティック ルートは、インターフェイス ヌル 0 をポイントするように設定する必要があります。また、プレフィクスは、既知の BGP ルートのスーパーセットでなければなりません。BGP パケットを受信したルータは、より具体的な BGP ルートを使用します。BGP ルーティング テーブルにルートがない場合、パケットはヌル 0 に転送され、廃棄されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [*distance*] [*name*] [**permanent** | **track** *number*] [**tag** *tag*]
4. **router bgp** *autonomous-system-number*
5. **redistribute static**
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	**ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [*distance*] [*name*] [**permanent** | **track** *number*] [**tag** *tag*] **例：** `Router(config)# ip route 172.0.0.0 255.0.0.0 null 0`	スタティック ルートを作成します。
ステップ 4	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 45000`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
ステップ 5	**redistribute static** **例：** `Router(config-router)# redistribute static`	BGP ルーティング テーブルにルートを再配布します。
ステップ 6	**end** **例：** `Router(config-router)# end`	ルータ 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 を使用した条件付き集約ルートの設定

少なくとも 1 つのルートが指定された範囲に含まれる場合、この作業を使用して、BGP ルーティング テーブルに集約ルート エントリを作成します。集約ルートは、このユーザの自律システムから始まるものとしてアドバタイズされます。

AS-SET 生成

AS-SET 情報は、**aggregate-address** コマンドを使用して、BGP ルートが集約されたときに生成されます。このようなルートについてアドバタイズされたパスは、コミュニティを含め、要約されているすべてのパスに含まれる、すべての要素から構成される AS-SET です。集約される AS-PATH が同じものである場合、AS-PATH だけがアドバタイズされます。**aggregate-address** コマンド用にデフォルトで設定されている ATOMIC-AGGREGATE アトリビュートは、AS-SET には追加されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*

4. **aggregate-address** *address mask* [**as-set**]
5. **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`	指定されたルーティング プロセスでルータ 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	**aggregate-address** *address mask* [**as-set**] **例：** `Router(config-router)# aggregate-address 172.0.0.0 255.0.0.0 as-set`	BGP ルーティング テーブルに集約エントリを作成します。 • 指定されたルートは、BGP テーブル内に存在する必要があります。 • 指定された範囲に含まれる、より詳しい BGP ルートがある場合は、キーワードを指定せずに **aggregate-address** コマンドを使用して、集約エントリを作成します。 • このルートについてアドバタイズされるパスが AS-SET であることを指定するには、**as-set** キーワードを使用します。このルートは、集約されたルートの到達可能性情報が変更されるたびに取り消され、アップデートされるため、多数のパスを集約するときには、**as-set** キーワードは使用しないでください。 **（注）** この例では、一部の構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 5	**end** **例：** `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

BGP を使用した集約されたルートのアドバタイズの抑制および抑制解除

集約ルートを作成し、BGP を使用してルートのアドバタイズメントを抑制して、その後、ルートのアドバタイズの抑制を解除するには、この作業を使用します。抑制されているルートはいかなるネイバーにもアドバタイズされませんが、特定のネイバーに対してすでに抑制されているルートの抑制を解除することはできます。

手順の概要

1. **enable**

2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **aggregate-address** *address mask* [**summary-only**]
   または
   aggregate-address *address mask* [**suppress-map** *map-name*]
6. **neighbor** {*ip-address* | *peer-group-name*} **unsuppress-map** *map-name*
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`	指定されたルーティング プロセスでルータ 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	**neighbor** *ip-address* **remote-as** *autonomous-system-number* **例：** `Router(config-router)# neighbor 192.168.1.2 remote-as 40000`	指定された自律システムのネイバーの IP アドレスを、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 5	**aggregate-address** *address mask* [**summary-only**] または **aggregate-address** *address mask* [**suppress-map** *map-name*] **例：** `Router(config-router)# aggregate-address 172.0.0.0 255.0.0.0 summary-only` または `Router(config-router)# aggregate-address 172.0.0.0 255.0.0.0 suppress-map map1`	集約ルートを作成します。 • 集約ルート（たとえば、10.*.*.*）を作成し、すべてのネイバーに対するより具体的なルートのアドバタイズメントを抑制するには、オプションの **summary-only** キーワードを使用します。 • 集約ルートを作成するが、指定されたルートのアドバタイズメントを抑制するには、オプションの **suppress-map** キーワードを使用します。抑制されたルートは、いかなるネイバーにもアドバタイズされません。ルート マップの **match** 句を使用して、集約ルートのうち、より具体的なものを選択的に抑制し、その他のルートを抑制せずにそのまま残すことができます。IP アクセス リスト、および自律システム パス アクセス リストの **match** 句はサポートされています。 **（注）** この例では、一部の構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

	コマンドまたはアクション	目的
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **unsuppress-map** *map-name* **例：** `Router(config-router)# neighbor 192.168.1.2 unsuppress map1`	（任意）**aggregate-address** コマンドにより、すでに抑制されているルートを選択的にアドバタイズします。 • この例では、ステップ 5 ですでに抑制されているルートが、ネイバー 192.168.1.2 にアドバタイズされます。
ステップ 7	**end** **例：** `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

BGP を使用した非アクティブなルート アドバタイズメントの抑制

BGP により、非アクティブなルートのアドバタイズメントを抑制するには、この作業を実行します。Cisco IOS Release 12.2(25)S、12.2(33)SXH、および 15.0(1)M では、BGP ピアに非アクティブなルートをアドバタイズしないように BGP を設定するための **bgp suppress-inactive** コマンドが導入されました。BGP ルーティング プロセスは、デフォルトで、RIB にインストールされていないルートを BGP ピアにアドバタイズできます。RIB にインストールされていないルートは非アクティブなルートです。非アクティブなルートのアドバタイズメントは、たとえば、共通のルート集約を通じてルートがアドバタイズされた場合に行われます。

非アクティブなルートのアドバタイズメントを抑制して、より整合性の取れたデータ フォワーディングを行うことができます。この機能は、IPv4 アドレス ファミリごとに設定できます。たとえば、**maximum routes** グローバル コンフィギュレーション コマンドを使用して、VRF で設定できるルート数の最大値を指定するときに、この上限を超えた後、非アクティブなルートが VRF で使用されるのを防ぐために、このようなルートのアドバタイズメントを抑制することもできます。

前提条件

この作業は、BGP がイネーブルにされ、ピアリングが確立されていることを前提にしています。

制約事項

非アクティブ ルートの抑制を設定できるのは、IPv4 アドレス ファミリ、またはデフォルトの IPv4 汎用セッションの下だけです。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family** {**ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]}
5. **bgp suppress-inactive**
6. **end**
7. **show ip bgp rib-failure**

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** *as-number* **例：** `Router(config)# router bgp 45000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**address-family** {**ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]} **例：** `Router(config-router)# address-family ipv4 unicast`	アドレス ファミリ固有のコンフィギュレーションを使用するように BGP ピアを設定するために、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。 • この例では、IPv4 ユニキャスト アドレス ファミリ セッションを作成します。
ステップ 5	**bgp suppress-inactive** **例：** `Router(config-router-af)# bgp suppress-inactive`	非アクティブなルートの BGP アドバタイジングを抑制します。 • デフォルトの設定では、BGP は非アクティブなルートをアドバタイズします。 • 非アクティブ ルートのアドバタイズメントを再度イネーブルにするには、このコマンドの **no** 形式を入力します。
ステップ 6	**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 モードを開始します。
ステップ 7	**show ip bgp rib-failure** **例：** `Router# show ip bgp rib-failure`	（任意）RIB にインストールされていない BGP ルートを表示します。

例

次の例に示す **show ip bgp rib-failure** コマンドの出力には、RIB にインストールされていないルートが表示されています。この出力からは、表示されたルートがインストールされなかったのは、より都合のよい管理ディスタンスのルートがすでに RIB に存在していたからであることがわかります。

```
Router# show ip bgp rib-failure

Network            Next Hop                  RIB-failure   RIB-NH Matches
10.1.15.0/24       10.1.35.5          Higher admin distance             n/a
10.1.16.0/24       10.1.15.1          Higher admin distance             n/a
```

BGP ルートの条件付きアドバタイズ

選択した BGP ルートを条件付きでアドバタイズするには、この作業を実行します。条件付きでアドバタイズされるルートまたはプレフィクスは、アドバタイズ マップと存在マップまたは不在マップの 2 つのルート マップで定義されます。存在マップまたは不在マップと関連付けられているルート マップは、BGP スピーカーが追跡するプレフィクスを指定します。アドバタイズ マップと関連付けられているルート マップは、条件が満たされたときに、指定されたネイバーにアドバタイズされるプレフィクスを指定します。

- 存在マップが設定されている場合、プレフィクスがアドバタイズ マップと存在マップの両方に存在するときに条件が満たされます。
- 不在マップが設定されている場合、プレフィクスがアドバタイズ マップには存在するが、不在マップには存在しないときに条件が満たされます。

条件が満たされない場合、ルートは取り消され、条件付きアドバタイズメントは行われません。条件付きアドバタイズメントを行うには、ダイナミックにアドバタイズされるルート、またはアドバタイズされないルートがすべて BGP ルーティング テーブルに存在する必要があります。これらのルートは、アクセス リストから、または IP プレフィクス リストから参照されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
5. **neighbor** *ip-address* **advertise-map** *map-name* {**exist-map** *map-name* | **non-exist-map** *map-name*}
6. **exit**
7. **route-map** *map-tag* [**permit** | **deny**] [**sequence-number**]
8. **match ip address** {*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]}
9. トラッキングの対象となる各プレフィクスについて、ステップ 7 と 8 を繰り返します。
10. **exit**
11. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]
12. 作成される各アクセス リストについて、ステップ 11 を繰り返します。
13. **exit**

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。

	コマンドまたはアクション	目的
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 45000`	指定されたルーティング プロセスでルータ 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	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* **例：** `Router(config-router)# neighbor 192.168.1.2 remote-as 40000`	指定された自律システムのネイバーの IP アドレスを、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 5	**neighbor** *ip-address* **advertise-map** *map-name* {**exist-map** *map-name* | **non-exist-map** *map-name*} **例：** `Router(config-router)# neighbor 192.168.1.2 advertise-map map1 exist-map map2`	指定された自律システムのネイバーの IP アドレスを、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • この例では、**アドバタイズ マップ** map1 に関連付けられているルート マップで、**存在マップ** map2 にも同じプレフィクスが存在する場合に、指定されたネイバーにアドバタイズされるプレフィクスを指定します。 • この例では、プレフィクス 172.17.0.0（ステップ 11 より）が map1 および map2 に存在する場合に、ネイバー 192.168.1.2 にアドバタイズされます。
ステップ 6	**exit** **例：** `Router(config-router)# exit`	ルータ 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 map1 permit 10`	ルート マップを設定し、ルート マップ コンフィギュレーション モードを開始します。 • この例では、map1 という名前のルート マップが作成されます。
ステップ 8	**match ip address** {*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...*| *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]} **例：** `Router(config-route-map)# match ip address 1`	標準アクセス リスト、拡張アクセス リスト、またはプレフィクス リストにより許可されているプレフィクスと一致するルート マップを作成します。 • この例では、ルート マップは、アクセス リスト 1 で許可されているプレフィクスとマッチングされます。
ステップ 9	トラッキングの対象となる各プレフィクスについて、ステップ 7 と 8 を繰り返します。	—
ステップ 10	**exit** **例：** `Router(config-route-map)# exit`	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、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 11	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**] **例：** `Router(config)# access-list 1 permit 172.17.0.0`	標準アクセス リストを設定します。 • この例では、アクセス リスト 1 で、**neighbor advertise-map** コマンドによって設定された他の条件に応じて、172.17.0.0 プレフィクスのアドバタイズが許可されます。

	コマンドまたはアクション	目的
ステップ 12	作成される各アクセス リストについて、ステップ 11 を繰り返します。	—
ステップ 13	**exit** **例：** `Router(config)# exit`	グローバル 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 ルートの開始

ルート集約は BGP テーブルのサイズを最小化するには便利ですが、BGP テーブルに特定のプレフィクスを追加する必要が生じることがあります。ルート集約では、特定のプレフィクスをさらに非表示にすることができます。「BGP ルーティング プロセスの設定」（P.11）の説明のとおり **network** コマンドを使用して、ルートを開始し、次のオプション作業に従って、さまざまな状況に対応した BGP テーブルへの BGP ルートを開始します。

- 「BGP を使用したデフォルト ルートのアドバタイジング」（P.50）
- 「BGP ルートの条件付き挿入」（P.52）
- 「バックドア ルートを使用した BGP ルートの開始」（P.56）

BGP を使用したデフォルト ルートのアドバタイジング

BGP ピアへのデフォルト ルートをアドバタイズするには、次の作業を実行します。デフォルト ルートはローカルに開始されます。コンフィギュレーションを簡素化する、またはルータがシステム リソースを過剰にしないように防ぐには、デフォルト ルートが便利です。ルータが Internet Service Provider（ISP; インターネット サービス プロバイダー）のピアである場合、ISP は完全なルーティング テーブルを持っているため、ISP ネットワークへのデフォルト ルートを設定しておくと、ローカル ルータのリソースが節約されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*]
4. **route-map** *map-tag* [**permit** | **deny**] [**sequence-number**]
5. **match ip address** {*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]}
6. **exit**
7. **router bgp** *autonomous-system-number*
8. **neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-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 prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network*/*length* | **permit** *network*/*length*} [**ge** *ge-value*] [**le** *le-value*] **例：** `Router(config)# ip prefix-list DEFAULT permit 10.1.1.0/24`	IP プレフィクス リストを設定します。 • この例では、プレフィクス リスト DEFAULT は、**match ip address** コマンドで設定されたマッチングに基づいて、10.1.1.0/24 プレフィクスのアドバタイジングを許可しています。
ステップ 4	**route-map** *map-tag* [**permit** | **deny**] [**sequence-number**] **例：** `Router(config)# route-map ROUTE`	ルート マップを設定し、ルート マップ コンフィギュレーション モードを開始します。 • この例では、ROUTE という名前のルート マップが作成されます。
ステップ 5	**match ip address** {*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]} **例：** `Router(config-route-map)# match ip address prefix-list DEFAULT`	標準アクセス リスト、拡張アクセス リスト、またはプレフィクス リストにより許可されているプレフィクスと一致するルート マップを作成します。 • この例では、ルート マップは、プレフィクス リスト DEFAULT で許可されているプレフィクスとマッチングされます。
ステップ 6	**exit** **例：** `Router(config-route-map)# exit`	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、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	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 40000`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*] **例：** `Router(config-router)# neighbor 192.168.3.2 default-originate`	（任意）デフォルト ルートとして使用するために、BGP スピーカー（ローカル ルータ）がデフォルト ルート 0.0.0.0 をピアに送信することを許可します。
ステップ 9	**end** **例：** `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

トラブルシューティングのヒント

デフォルト ルートが設定されていることを確認するには、ローカル ルータではなく受信側 BGP ピアで **show ip route** コマンドを使用します。この出力で、次に類似した行にデフォルト ルート 0.0.0.0 が表示されていることを確認します。

```
B*   0.0.0.0/0 [20/0] via 192.168.1.2, 00:03:10
```

BGP ルートの条件付き挿入

標準のルート集約を通じて選択された具体性にかけるプレフィクスではなく、より具体的なプレフィクスを BGP ルーティング テーブルに挿入するには、この作業を実行します。より具体的なプレフィクスを使用すると、集約されたルートを使う場合よりも、よりきめ細かなトラフィック エンジニアリングや管理制御を行うことができます。

条件付き BGP ルートの挿入

BGP を通じてアドバタイズされるルートは、通常、使用されるルートの数が最小化され、グローバル ルーティング テーブルのサイズが小さくなるように集約されます。しかし、共通のルート集約では、より具体的なルーティング情報（より正確であるが、パケットを宛先に転送するために必要なわけではない）がわかりにくくなってしまいます。ルーティングの精度は、共通のルート集約により低下します。これは、トポロジ的に大きな領域に広がる複数のアドレスやホストを表すプレフィクスを 1 つのルートに正確に反映させることはできないからです。Cisco IOS ソフトウェアには、プレフィクスを BGP にする方法がいくつか用意されています。現在使用されている方法には、再配布する方法や、**network** または **aggregate-address** コマンドを使った方法などがあります。これらの方法は、ルーティング テーブル、または BGP テーブルのいずれかにより具体的なルーティング情報（開始されるルートと一致するもの）が存在することを前提にしています。

BGP の条件付きルートの挿入により、一致するものがなくても、プレフィクスを BGP ルーティング テーブルにすることができます。この機能を使って、管理ポリシーやトラフィック エンジニアリング情報に基づいて、より具体的なルートを生成することができます。これにより、設定された条件が満たされた場合にだけ BGP ルーティング テーブルに挿入される、より具体的なルートへのパケットの転送をさらに厳密に制御できるようになります。この機能をイネーブルにすると、条件に応じて、あまり具体的ではないプレフィクスにより具体的なプレフィクスを挿入または置き換えることにより、共通のルート集約の精度を高めることができるようになります。元のプレフィクスと同じ、またはより具体的なプレフィクスだけが挿入されます。BGP 条件付きルート挿入をイネーブルにするには、**bgp inject-map exist-map** コマンドを使用します。また、BGP 条件付きルート挿入では、2 つのルートマップ（挿入マップと存在マップ）を使用して、1 つ（または複数）のより具体的なプレフィクスが BGP ルーティング テーブルに挿入されます。exist-map は、BGP スピーカーにより追跡されるプレフィクスを表します。inject map は、ローカル BGP テーブルで作成され、このテーブルにインストールされるプレフィクスを定義します。

前提条件

この作業は、BGP ピアに対して、IGP がすでに設定されていることを前提にしています。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp inject-map** *inject-map-name* **exist-map** *exist-map-name* [**copy-attributes**]

5. **exit**
6. **route-map** *map-tag* [**permit** | **deny**] [**sequence-number**]
7. **match ip address** {*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]}
8. **match ip route-source** {*access-list-number* | *access-list-name*} [*access-list-number...*| *access-list-name...*]
9. **exit**
10. **route-map** *map-tag* [**permit** | **deny**] [**sequence-number**]
11. **set ip address** {*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...*| *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]}
12. **set community** {*community-number* [**additive**] [*well-known-community*] | **none**}
13. **exit**
14. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*]
15. 作成される各プレフィクス リストについて、ステップ 14 を繰り返します。
16. **exit**
17. **show ip bgp injected-paths**

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 40000`	指定されたルーティング プロセスでルータ 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	**bgp inject-map** *inject-map-name* **exist-map** *exist-map-name* [**copy-attributes**] **例：** `Router(config-router)# bgp inject-map ORIGINATE exist-map LEARNED_PATH`	条件付きルート挿入のために、挿入マップと存在マップを指定します。 • 挿入したルートが集約ルートのアトリビュートを継承することを指定するには、**copy-attributes** キーワードを使用します。
ステップ 5	**exit** **例：** `Router(config-router)# exit`	ルータ 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 6	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **例：** `Router(config)# route-map LEARNED_PATH permit 10`	ルート マップを設定し、ルート マップ 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	**match ip address** {*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]} **例：** `Router(config-route-map)# match ip address prefix-list SOURCE`	より具体的なルートの挿入先となる集約ルートを指定します。 • この例では、ルートのソースの再配布に、プレフィクス リスト SOURCE が使用されています。
ステップ 8	**match ip route-source** {*access-list-number* | *access-list-name*} [*access-list-number...*| *access-list-name...*] **例：** `Router(config-route-map)# match ip route-source prefix-list ROUTE_SOURCE`	ルートのソースを再配布するための一致条件を指定します。 • この例では、ルートのソースの再配布に、プレフィクス リスト ROUTE_SOURCE が使用されています。 **（注）** ルート ソースは、**neighbor remote-as** コマンドで設定されたネイバー アドレスです。条件付きルート挿入が行われるようにするには、トラッキングされるプレフィクスはこのネイバーから来たものでなければなりません。
ステップ 9	**exit** **例：** `Router(config-route-map)# exit`	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、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 10	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **例：** `Router(config)# route-map ORIGINATE permit 10`	ルート マップを設定し、ルート マップ 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	**set ip address** {*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [access-list-number... | access-list-name] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]} **例：** `Router(config-route-map)# set ip address prefix-list ORIGINATED_ROUTES`	挿入されるルートを指定します。 • この例では、ルートのソースの再配布に、プレフィクス リスト originated_routes が使用されています。
ステップ 12	**set community** {*community-number* [**additive**] [*well-known-community*] | **none**} **例：** `Router(config-route-map)# set community 14616:555 additive`	挿入されたルートの BGP コミュニティ アトリビュートを設定します。
ステップ 13	**exit** **例：** `Router(config-route-map)# exit`	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、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 14	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network*/*length* | **permit** *network*/*length*} [**ge** *ge-value*] [**le** *le-value*] **例：** `Router(config)# ip prefix-list SOURCE permit 10.1.1.0/24`	プレフィクス リストを作成します。 • この例では、プレフィクス リスト SOURCE は、ネットワーク 10.1.1.0/24 からのルートを許可するように設定されています。
ステップ 15	作成される各プレフィクス リストについて、ステップ 14 を繰り返します。	—
ステップ 16	**exit** **例：** `Router(config)# exit`	グローバル 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。
ステップ 17	**show ip bgp injected-paths** **例：** `Router# show ip bgp injected-paths`	（任意）挿入されたパスに関する情報を表示します。

例

次の出力例は、**show ip bgp injected-paths** コマンドを入力したときに表示される出力に類似しています。

```
Router# show ip bgp injected-paths

BGP table version is 11, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 172.16.0.0       10.0.0.2                               0 ?
*> 172.17.0.0/16    10.0.0.2                               0 ?
```

トラブルシューティングのヒント

BGP 条件付きルート挿入は、あまり具体的ではないプレフィクスがある場合に行われる、BGP ルーティング テーブルへのより具体的なプレフィクスの挿入に基づいています。条件付きルート挿入が適切に行われない場合は、次の点を確認してください。

- 条件付きルート挿入は設定されているが、行われないという場合は、BGP ルーティング テーブルに集約プレフィクスが存在することを確認します。BGP ルーティング テーブルにトラッキングされたプレフィクスが存在するかしないかは、**show ip bgp** コマンドで確認できます。
- 集約プレフィクスは存在するが、条件付きルート挿入は行われないという場合は、集約プレフィクスが正しいネイバーから来ていること、およびこのネイバーを識別するプレフィクス リストが /32 一致であることを確認します。
- **show ip bgp injected-paths** コマンドを使用して、より具体的なプレフィクスが挿入されたかどうかを確認します。
- 挿入されるプレフィクスが、集約プレフィクスの範囲から外れていないことを確認します。
- 挿入ルート マップが、**match ip address** コマンドではなく、**set ip address** コマンドを使用して設定されていることを確認します。

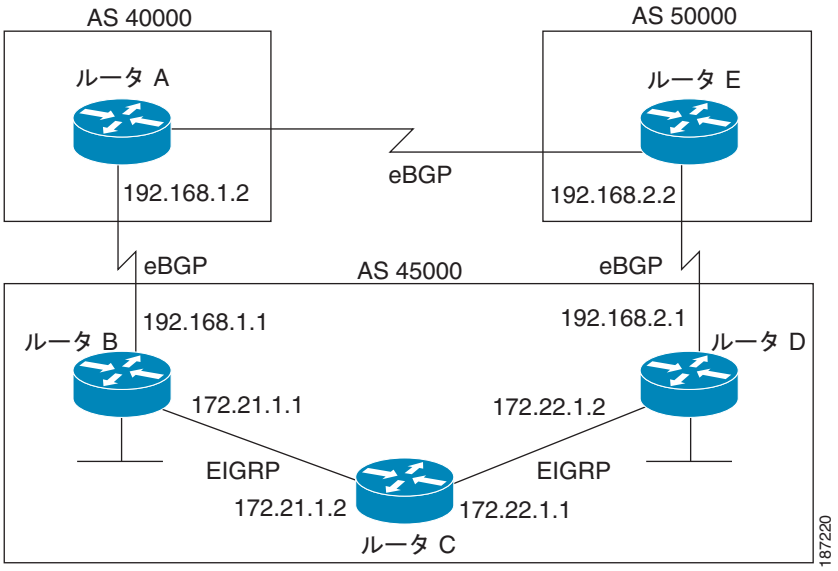
バックドア ルートを使用した BGP ルートの開始

バックドア ルートを使用して到達可能なネットワークを示すには、この作業を実行します。バックドア ネットワークはローカル ネットワークと同様に扱われますが、アドバタイズされません。

BGP バックドア ルート

さまざまな自律システムとの通信に eBGP を使用する境界ルータを 2 つ使った BGP ネットワーク トポロジでは、2 つの境界ルータ間の通信で、最も効果的なルーティング方法は eBGP を使用することではありません。図 5 では、ルータ B は BGP スピーカーとして、eBGP を通るルータ D へのルートを受け取りますが、このルートは少なくとも 2 つの自律システムを横切っています。また、ルータ B とルータ D は Enhanced Interior Gateway Routing Protocol（EIGRP）ネットワーク（ここでは、すべての IGP を使用可能）を通じて接続されていますが、これが最短ルートです。しかし、EIGRP ルートのデフォルト アドミニストレーティブ ディスタンスは 90 で、eBGP ルートのデフォルト アドミニストレーティブ ディスタンスは 20 であるため、BGP は eBGP ルートを選びます。アドミニストレーティブ ディスタンスを変更すると、ルーティングがループする可能性があるため、デフォルト アドミニストレーティブ ディスタンスの変更は推奨しません。BGP に EIGRP ルートを選択させるには、**network backdoor** コマンドを使用します。BGP は、network backdoor コマンドで指定されたネットワークをローカルに割り当てられたネットワークとして扱います。ただし、BGP アップデートで指定されたネットワークのアドバタイズは行いません。これは、図 5 では、ルータ B は長い eBGP ルートの代わりに、短い EIGRP を使ってルータ D と通信するという意味です。

図 5　　BGP バックドア ルートのトポロジ



前提条件

この作業は、BGP ピアに対して、IGP（この例では EIGRP）がすでに設定されていることを前提にしています。この設定は図 5 のルータ B で行われます。また、BGP ピアはルータ D です。

手順の概要

1. **enable**
2. **configure terminal**

3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **network** *ip-address* **backdoor**
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	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 45000`	指定されたルーティング プロセスでルータ 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	**neighbor** *ip-address* **remote-as** *autonomous-system-number* **例：** `Router(config-router)# neighbor 172.22.1.2 remote-as 45000`	指定された自律システムのネイバーの IP アドレスを、ローカル ルータのマルチプロトコル BGP ネイバー テーブルに追加します。 • この例では、ピアに指定されている自律システム番号はステップ 3 で指定された番号と同じであるため、このピアは内部ピアです。
ステップ 5	**network** *ip-address* **backdoor** **例：** `Router(config-router)# network 172.21.1.0 backdoor`	バックドア ルートを通じて到達可能なネットワークを示します。
ステップ 6	**end** **例：** `Router(config-router)# end`	ルータ 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 ピア グループの設定

この作業では、BGP ピア グループの設定方法を説明します。BGP スピーカーでは、多数のネイバーが同じアップデート ポリシー（つまり、同じアウトバウンド ルート マップ、配布リスト、フィルタ リスト、アップデート ソースなど）を使って設定されていることがよくあります。同じアップデート ポリシーを持つネイバーは、コンフィギュレーションを簡素化するため、またさらに重要なことには、アップデートをより効率化するために、ピア グループにグループ化されます。多数のピアがある場合、このアプローチを強く推奨します。

次の作業で説明されている、BGP ピア グループを設定するための 3 つの手順は次のとおりです。

- ピア グループを作成する
- ピア グループへオプションに割り当てる

- ピア グループのメンバをネイバーにする

neighbor shutdown ルータ コンフィギュレーション コマンドを使用して、コンフィギュレーション情報を削除せずに、BGP ピア、またはピア グループを削除することができます。

制約事項

デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義されたネイバーは、IPv4 ユニキャスト アドレス プレフィクスだけを交換します。IPv6 プレフィクスなど、その他のアドレス プレフィクス タイプを交換するには、その他のプレフィクス タイプについて、アドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用し、ネイバーをアクティブ化することも必要です。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *peer-group-name* **peer-group**
5. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
6. **neighbor** *ip-address* **peer-group** *peer-group-name*
7. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
8. **neighbor** *peer-group-name* **activate**
9. **neighbor** *ip-address* **peer-group** *peer-group-name*
10. **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 40000`	指定されたルーティング プロセスでルータ 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	**neighbor** *peer-group-name* **peer-group** **例：** `Router(config-router)# neighbor fingroup peer-group`	BGP ピア グループを作成します。

	コマンドまたはアクション	目的
ステップ 5	**neighbor** *ip-address* **remote-as** *autonomous-system-number* **例：** `Router(config-router)# neighbor 192.168.1.1 remote-as 45000`	指定された自律システムのネイバーの IP アドレスを、ローカル ルータのマルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 6	**neighbor** *ip-address* **peer-group** *peer-group-name* **例：** `Router(config-router)# neighbor 192.168.1.1 peer-group fingroup`	BGP ネイバーの IP アドレスをピア グループに割り当てます。
ステップ 7	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] **例：** `Router(config-router)# address-family ipv4 multicast`	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。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。これがデフォルトです。 • キーワード **multicast** は、IPv4 マルチキャスト アドレス プレフィクスが交換されることを表します。 • **vrf** キーワード、および *vrf-name* 引数は、IPv4 VRF インスタンス情報が交換されることを示します。
ステップ 8	**neighbor** *peer-group-name* **activate** **例：** `Router(config-router-af)# neighbor fingroup activate`	ネイバーが IPv4 アドレス ファミリのプレフィクスをローカル ルータと交換できるようにします。 **（注）** デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義されたネイバーは、ユニキャスト アドレス プレフィクスだけを交換します。この例で設定しているマルチキャストなど、その他のアドレス プレフィクス タイプを BGP が交換できるようにするには、ネイバーのアクティブ化にも **neighbor activate** コマンドを使用する必要があります。
ステップ 9	**neighbor** *ip-address* **peer-group** *peer-group-name* **例：** `Router(config-router-af)# neighbor 192.168.1.1 peer-group fingroup`	BGP ネイバーの IP アドレスをピア グループに割り当てます。
ステップ 10	**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。

ピア セッション テンプレートの設定

次に説明する作業では、ピア セッション テンプレートを作成し、設定します。

- 「基本的なピア セッション テンプレートの設定」（P.60）
- 「inherit peer-session コマンドを使用したピア セッション テンプレートの継承の設定」（P.63）
- 「neighbor inherit peer-session コマンドを使用したピア セッション テンプレートの継承の設定」（P.65）

ピア テンプレートでの継承

継承機能は、ピア テンプレート操作の重要なコンポーネントです。ピア テンプレートでの継承は、たとえば、ファイルとディレクトリ ツリーなど、一般的なコンピューティングで見られるノードとツリーの構造に似ています。ピア テンプレートは、別のピア テンプレートから直接、または間接的にコンフィギュレーションを継承することができます。直接継承されたピア テンプレートは、構造体のツリーを表します。間接的に継承されたピア テンプレートはツリーのノードを表します。個々のノードも継承をサポートしているため、チェーン内で間接的に継承されたピア テンプレートすべてのコンフィギュレーションを、直接継承されたピア テンプレート、またはツリーのソースに適用するブランチも作成できます。この構造により、ネイバーのグループに通常、再適用されるコンフィギュレーション文を繰り返す必要がなくなります。これは、共通のコンフィギュレーション文を一度適用しておくと、その後は共通のコンフィギュレーションを持つネイバー グループに適用されるピア グループにより間接的に継承されるからです。ノードとツリーの内部で別々に複製されたコンフィギュレーション文は、直接継承したテンプレートにより、ツリーのソースでフィルタ処理されます。直接継承されたテンプレートは、直接継承されたテンプレートで複製された、間接的に継承された文をすべて上書きします。

継承によりネイバー コンフィギュレーションのスケーラビリティと柔軟性がさらに広がり、複数のピア テンプレート コンフィギュレーションをチェーンして、共通のコンフィギュレーション文を継承する単純なコンフィギュレーションを作成したり、共通に継承されるコンフィギュレーションとともに非常に限定的なコンフィギュレーション文を適用する複雑なコンフィギュレーションを作成したりできるようになります。ピア セッション テンプレートおよびピア ポリシー テンプレートでの継承の設定についての詳細は、これ以降のセクションで説明します。

BGP ネイバーが継承したピア テンプレートを使用する場合、特定のテンプレートに関連付けられているポリシーを判断するのが難しいことがあります。Cisco IOS 12.0(25)S、12.4(11)T、12.2(33)SRB、12.2(33)SB 以降のリリースでは、**show ip bgp template peer-policy** コマンドに、特定のテンプレートに関連付けられているローカル ポリシーおよび継承されたポリシーの詳しいコンフィギュレーションを表示するためのキーワード **detail** が追加されました。

基本的なピア セッション テンプレートの設定

一般的な BGP ルーティング セッション コマンドを使って、この次に説明する 2 つの作業のうち 1 つを使用して、多数のネイバーに適用できる基本的なピア セッション テンプレートを作成するには、この作業を実行します。

（注） ステップ 5 と 6 のコマンドは任意で、サポートされている一般的なセッション コマンドのいずれとでも置き換えが可能です。

ピア セッション テンプレート

ピア セッション テンプレートは、一般的なセッション コマンドのコンフィギュレーションをグループ化し、セッション コンフィギュレーション要素を共有するネイバーのグループに適用するために使用されます。異なるアドレス ファミリで設定されているネイバーに共通する一般的なセッション コマンドは、同じピア セッション テンプレートに設定できます。ピア セッション テンプレートの作成と設定は、ピア セッション コンフィギュレーション モードで行います。ピア セッション テンプレートで設定できるのは、一般的なセッション コマンドだけです。次の一般的なセッション コマンドは、ピア セッション テンプレートでサポートされています。

- **description**
- **disable-connected-check**
- **ebgp-multihop**
- **exit peer-session**

- **inherit peer-session**
- **local-as**
- **password**
- **remote-as**
- **shutdown**
- **timers**
- **translate-update**
- **update-source**
- **version**

一般的なセッション コマンドをピア セッションで一度設定しておくと、ピア セッション テンプレートの直接適用、またはピア セッション テンプレートの間接継承によって、多数のネイバーに適用できます。ピア セッション テンプレートのコンフィギュレーションにより、自律システム内のすべてのネイバーに共通に適用される一般的なセッション コマンドのコンフィギュレーションが簡素化されます。

ピア セッション テンプレートは、直接継承と間接継承をサポートします。一度にピアの設定に使用できるピア セッション テンプレートは 1 つだけです。また、このピア セッション テンプレートは、間接継承されたピア セッション テンプレートを 1 つだけ含むことができます。

（注） 1 つのピア セッション テンプレートを使って、複数の継承文を設定しようとすると、エラー メッセージが表示されます。

この動作により、BGP ネイバーは 1 つのセッション テンプレートだけを直接継承し、最高 7 個のピア セッション テンプレートを間接継承できます。したがって、1 つのネイバーに最高 8 個のピア セッション コンフィギュレーション（直接継承されたピア セッション テンプレートのコンフィギュレーションと最高 7 個の間接継承されたピア セッション テンプレートのコンフィギュレーション）を適用できます。継承されたピア セッション コンフィギュレーションが最初に評価され、ブランチの最後のノードから、ツリーのソースで直接適用されたピア セッション テンプレートまで適用されます。直接適用されたピア セッション テンプレートは、継承されたピア セッション テンプレート コンフィギュレーションよりも優先されます。継承されたピア セッション テンプレートで複製されたコンフィギュレーション文はすべて、直接適用されたピア セッション テンプレートにより上書きされます。したがって、異なる値を使って、一般セッション コマンドを再度適用した場合、それ以降の値が優先され、間接継承されたテンプレートで設定された直前の値が上書きされます。次に、この機能を使用した例を示します。

次の例では、一般セッション コマンド **remote-as 1** がピア セッション テンプレート SESSION-TEMPLATE-ONE に適用されます。

```
template peer-session SESSION-TEMPLATE-ONE
 remote-as 1
 exit peer-session
```

ピア セッション テンプレートは、一般的なセッション コマンドだけをサポートします。特定のアドレス ファミリ、または NLRI コンフィギュレーション モードだけのために設定される BGP ポリシー コンフィギュレーション コマンドは、ピア ポリシー テンプレートで設定されます。

制約事項

ピア セッション テンプレートには、次の制約事項が適用されます。

- ピア セッション テンプレートが直接継承できるセッション テンプレートは 1 つだけです。また、継承されたセッション テンプレートはそれぞれ、間接継承されたセッション テンプレートを 1 つ含むことができます。したがって、ネイバー、またはネイバー グループの設定には、直接適用されたピア セッション テンプレートを 1 個だけと、間接継承されたピア セッション テンプレートを 7 個使用できます。
- ピア グループおよびピア テンプレートの両方で機能するように BGP ネイバーを設定することはできません。BGP ネイバーは、1 つのピア グループだけに属するように設定するか、またはピア テンプレートだけからポリシーを継承するように設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-session** *session-template-name*
5. **remote-as** *autonomous-system-number*
6. **timers** *keepalive-interval hold-time*
7. **end**
8. **show ip bgp template peer-session** [*session-template-name*]

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 101`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**template peer-session** *session-template-name* **例：** `Router(config-router)# template peer-session INTERNAL-BGP`	セッション テンプレート コンフィギュレーション モードを開始して、ピア セッション テンプレートを作成します。
ステップ 5	**remote-as** *autonomous-system-number* **例：** `Router(config-router-stmp)# remote-as 202`	（任意）指定された自律システムでリモート ネイバーとのピアリングを設定します。 **（注）** ここでは、サポートされている一般セッション コマンドならどれでも使用できます。サポートされているコマンドのリストについては、「ピア セッション テンプレート」（P.60）を参照してください。

	コマンドまたはアクション	目的
ステップ 6	**timers** *keepalive-interval hold-time* **例：** `Router(config-router-stmp)# timers 30 300`	（任意）BGP キープアライブとホールド タイマーを設定します。 • ホールド タイムは、少なくともキープアライブ タイムの 2 倍の長さが必要です。 **（注）** ここでは、サポートされている一般セッション コマンドならどれでも使用できます。サポートされているコマンドのリストについては、「ピア セッション テンプレート」（P.60）を参照してください。
ステップ 7	**end** **例：** `Router(config-router)# end`	セッション テンプレート 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。
ステップ 8	**show ip bgp template peer-session** [*session-template-name*] **例：** `Router# show ip bgp template peer-session`	ローカルに設定されたピア セッション テンプレートを表示します。 • *session-template-name* 引数を使用して、ピア ポリシー テンプレートが 1 つだけ表示されるように、出力をフィルタできます。また、このコマンドは、標準出力修飾子すべてをサポートしています。

次の作業

ピア セッション テンプレートの作成後、ピア セッション テンプレートのコンフィギュレーションは、**inherit peer-session** コマンド、または **neighbor inherit peer-session** コマンドを使って、別のピア セッション テンプレートに継承させる、または適用することができます。

inherit peer-session コマンドを使用したピア セッション テンプレートの継承の設定

この作業は、**inherit peer-session** コマンドを使用して、ピア セッション テンプレートの継承を設定します。これは、ピア セッション テンプレートを作成、設定し、別のピア セッション テンプレートからコンフィギュレーションを継承できるようにします。

（注） ステップ 5 と 6 のコマンドは任意で、サポートされている一般的なセッション コマンドのいずれとでも置き換えが可能です。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-session** *session-template-name*
5. **description** *text-string*
6. **update-source** *interface-type interface-number*
7. **inherit peer-session** *session-template-name*
8. **end**

9. **show ip bgp template peer-session** [*session-template-name*]

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 101`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**template peer-session** *session-template-name* **例：** `Router(config-router)# template peer-session CORE1`	セッション テンプレート コンフィギュレーション モードを開始して、ピア セッション テンプレートを作成します。
ステップ 5	**description** *text-string* **例：** `Router(config-router-stmp)# description CORE-123`	（任意）説明を設定します。 • text-string には最大 80 文字を使用できます。 **（注）** ここでは、サポートされている一般セッション コマンドならどれでも使用できます。サポートされているコマンドのリストについては、「ピア セッション テンプレート」（P.60）を参照してください。
ステップ 6	**update-source** *interface-type interface-number* **例：** `Router(config-router-stmp)# update-source loopback 1`	（任意）ルーティング テーブル アップデートを受信するための特定のソース、またはインターフェイスを選択するようにルータを設定します。 • この例では、ループバック インターフェイスを使用します。このコンフィギュレーションの利点は、ループバック インターフェイスはフラッピング インターフェイスの効果の影響を受けにくいところにあります。 **（注）** ここでは、サポートされている一般セッション コマンドならどれでも使用できます。サポートされているコマンドのリストについては、「ピア セッション テンプレート」（P.60）を参照してください。

	コマンドまたはアクション	目的
ステップ 7	**inherit peer-session** *session-template-name* **例：** `Router(config-router-stmp)# inherit peer-session INTERNAL-BGP`	別のピア セッション テンプレートのコンフィギュレーションを継承するように、このピア セッション テンプレートを設定します。 • この例では、INTERNAL-BGP からコンフィギュレーションを継承するようにピア セッション テンプレートを設定しています。このテンプレートはネイバーに適用可能で、コンフィギュレーション INTERNAL-BGP は間接的に適用されます。その他のピア セッション テンプレートは直接適用できません。ただし、直接継承されたテンプレートは最高 7 個の間接継承されたピア セッション テンプレートを持つことができます。
ステップ 8	**end** **例：** `Router(config-router)# end`	セッション テンプレート コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 9	**show ip bgp template peer-session** [*session-template-name*] **例：** `Router# show ip bgp template peer-session`	ローカルに設定されたピア セッション テンプレートを表示します。 • オプションの *session-template-name* 引数を使用して、ピア ポリシー テンプレートが 1 つだけ表示されるように、出力をフィルタできます。また、このコマンドは、標準出力修飾子すべてをサポートしています。

次の作業

ピア セッション テンプレートの作成後、ピア セッション テンプレートのコンフィギュレーションは、**inherit peer-session** コマンド、または **neighbor inherit peer-session** コマンドを使って、別のピア セッション テンプレートに継承させる、または適用することができます。

neighbor inherit peer-session コマンドを使用したピア セッション テンプレートの継承の設定

この作業では、**neighbor inherit peer-session** コマンドを使用して、ピア セッション テンプレートをネイバーに送信し、指定されたピア セッション テンプレートからコンフィギュレーションを継承させるようにルータを設定します。次の手順に従って、ピア セッション テンプレート コンフィギュレーションをネイバーに送信し、継承させます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** ***ip-address*** **remote-as** *autonomous-system-number*
5. **neighbor** *ip-address* **inherit peer-session** *session-template-name*
6. **end**
7. **show ip bgp template peer-session** [*session-template-name*]

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 101`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* **例：** `Router(config-router)# neighbor 172.16.0.1 remote-as 202`	指定されたネイバーを使ってピアリング セッションを設定します。 • ステップ 5 のネイバー継承文を動作させるには、**remote-as** 文を明示的に使用する必要があります。ピアリングが設定されていない場合、ステップ 5 で指定されたネイバーはセッション テンプレートを受け付けません。
ステップ 5	**neighbor** *ip-address* **inherit peer-session** *session-template-name* **例：** `Router(config-router)# neighbor 172.16.0.1 inherit peer-session CORE1`	ネイバーがコンフィギュレーションを継承できるように、このネイバーにピア セッション テンプレートを送信します。 • この例では、ピア セッション テンプレート CORE1 を 172.16.0.1 ネイバーに送信し、継承させるようにルータを設定しています。このテンプレートはネイバーに適用できます。また、別のピア セッション テンプレートが CORE1 で間接継承された場合、間接継承されたコンフィギュレーションも適用されます。その他のピア セッション テンプレートは直接適用できません。ただし、直接継承されたテンプレートも、さらに最高 7 個の間接継承されたピア セッション テンプレートを継承することができます。
ステップ 6	**end** **例：** `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 7	**show ip bgp template peer-session** [*session-template-name*] **例：** `Router# show ip bgp template peer-session`	ローカルに設定されたピア セッション テンプレートを表示します。 • オプションの *session-template-name* 引数を使用して、ピア ポリシー テンプレートが 1 つだけ表示されるように、出力をフィルタできます。また、このコマンドは、標準出力修飾子すべてをサポートしています。

次の作業

ピア ポリシー テンプレートを作成する方法については、「ピア ポリシー テンプレートの設定」（P.67）を参照してください。

ピア ポリシー テンプレートの設定

次に説明する作業では、ピア ポリシー テンプレートを作成し、設定します。

基本的なピア ポリシー テンプレートの設定

BGP ポリシー コンフィギュレーション コマンドを使って、この次に説明する 2 つの作業のうち 1 つを使用して、多数のネイバーに適用できる基本的なピア ポリシー テンプレートを作成するには、この作業を実行します。

（注） ステップ 5 ～ 7 のコマンドは任意で、サポートされている BGP ポリシー コンフィギュレーション コマンドのいずれとでも置き換えが可能です。

制約事項

ピア ポリシー テンプレートには、次の制約事項が適用されます。

- ピア ポリシー テンプレートは、直接的、または間接的に、最高 8 個のピア ポリシー テンプレートを継承できます。
- ピア グループおよびピア テンプレートの両方で機能するように BGP ネイバーを設定することはできません。BGP ネイバーは、1 つのピア グループだけに属するように設定するか、またはピア テンプレートだけからポリシーを継承するように設定できます。

ピア ポリシー テンプレート

ピア ポリシー テンプレートは、特定のアドレス ファミリおよび NLRI コンフィギュレーション モードで適用されるコマンドのコンフィギュレーションをグループ化し、適用するために使用されます。ピア ポリシー テンプレートの作成と設定は、ピア ポリシー コンフィギュレーション モードで行います。特定のアドレス ファミリ専用に設定される BGP ポリシー コマンドは、ピア ポリシー テンプレートで設定されます。ピア ポリシー テンプレートでは、次の BGP ポリシー コマンドがサポートされています。

- **advertisement-interval**
- **allowas-in**
- **as-override**
- **capability**
- **default-originate**
- **distribute-list**
- **dmzlink-bw**
- **exit-peer-policy**
- **filter-list**
- **inherit peer-policy**
- **maximum-prefix**

- **next-hop-self**
- **next-hop-unchanged**
- **prefix-list**
- **remove-private-as**
- **route-map**
- **route-reflector-client**
- **send-community**
- **send-label**
- **soft-reconfiguration**
- **unsuppress-map**
- **weight**

ピア ポリシー テンプレートは、特定のアドレス ファミリに属するネイバーに設定される BGP ポリシー コマンドの設定に使用されます。ピア セッション テンプレートと同様、ピア ポリシー テンプレートを一度設定しておくと、直接適用、または継承を通じて、多数のネイバーにピア ポリシー テンプレートを適用することができます。ピア ポリシー テンプレートの設定により、自律システム内のすべてのネイバーに適用される BGP ポリシー コマンドの設定が簡略化されます。

ピア セッション テンプレートと同様、ピア ポリシー テンプレートは継承をサポートしています。しかし、多少の違いはあります。直接適用されたピア ポリシー テンプレートは、最大 7 つのピア ポリシー テンプレートから設定を直接的または間接的に継承できます。したがって、合計 8 つのピア ポリシー テンプレートをネイバーまたはネイバー グループに適用できます。継承されたピア ポリシー テンプレートは、ルート マップのように、シーケンス番号付きで設定されます。ルート マップ同様、継承されたピア ポリシー テンプレートは、継承文のシーケンス番号の小さい順に評価されます。ただし、ピア ポリシー テンプレートはルート マップのように折りたたむことはできません。シーケンスはすべて評価されます。異なる値を使って、BGP ポリシー コマンドが再適用された場合は、シーケンス番号の小さいものから順に、前の値がすべて上書きされます。

直接適用されたピア ポリシー テンプレートと、シーケンス番号が最も大きい継承文のプライオリティは常に最も高く、最後に適用されます。これ以降のピア テンプレートに再適用されるコマンドは、必ず、前の値を上書きします。この動作は、個々のポリシー コンフィギュレーション コマンドを重複させることなく、共通のポリシー コンフィギュレーションは大規模なネイバー グループに適用し、特定のポリシー コンフィギュレーションは特定のネイバーやネイバー グループだけに適用できるように設計されています。

ピア ポリシー テンプレートは、ポリシー コンフィギュレーション コマンドだけをサポートします。特定のアドレス ファミリ用に設定される BGP ポリシー コンフィギュレーション コマンドは、ピア ポリシー テンプレートで設定されます。

ピア ポリシー テンプレートの設定により、BGP 設定が簡略化され、柔軟性が向上します。特定のポリシーを 1 回設定すれば、何回も参照できます。ピア ポリシーは最大 8 レベルの継承をサポートするため、非常に具体的で複雑な BGP ポリシーも作成できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-policy** *policy-template-name*
5. **maximum-prefix** *prefix-limit* [*threshold*] [**restart** *restart-interval* | **warning-only**]

6. **weight** *weight-value*
7. **prefix-list** *prefix-list-name* {**in** | **out**}
8. **exit-peer-policy**

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`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**template peer-policy** *policy-template-name* **例：** `Router(config-router)# template peer-policy GLOBAL`	ポリシー テンプレート コンフィギュレーション モードを開始し、ピア ポリシー テンプレートを作成します。
ステップ 5	**maximum-prefix** *prefix-limit* [*threshold*] [**restart** *restart-interval* | **warning-only**] **例：** `Router(config-router-ptmp)# maximum-prefix 10000`	（任意）このピアがネイバーから受け入れるプレフィクスの最大数を設定します。 **（注）** ここでは、サポートされている BGP ポリシー コンフィギュレーション コマンドならどれでも使用できます。サポートされているコマンドのリストについては、「ピア ポリシー テンプレート」（P.67）を参照してください。
ステップ 6	**weight** *weight-value* **例：** `Router(config-router-ptmp)# weight 300`	（任意）このネイバーから送信されるルートのデフォルトの重みを設定します。 **（注）** ここでは、サポートされている BGP ポリシー コンフィギュレーション コマンドならどれでも使用できます。サポートされているコマンドのリストについては、「ピア ポリシー テンプレート」（P.67）を参照してください。

	コマンドまたはアクション	目的
ステップ 7	**prefix-list** *prefix-list-name* {**in** | **out**} **例：** `Router(config-router-ptmp)# prefix-list NO-MARKETING in`	（任意）ルータにより受信、またはルータから送信されるプレフィクスをフィルタします。 • この例のプレフィクス リストは、インバウンド内部アドレスをフィルタします。 **（注）** ここでは、サポートされている BGP ポリシー コンフィギュレーション コマンドならどれでも使用できます。サポートされているコマンドのリストについては、「ピア ポリシー テンプレート」（P.67）を参照してください。
ステップ 8	**end** **例：** `Router(config-router-ptmp)# end`	ポリシー テンプレート 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。

次の作業

ピア ポリシー テンプレートの作成後、ピア ポリシー テンプレートのコンフィギュレーションを、別のピア ポリシー テンプレートに継承、または適用することができます。ピア ポリシーの継承の詳細については、「inherit peer-policy コマンドを使用したピア ポリシー テンプレートの継承の設定」（P.70）、または「neighbor inherit peer-policy コマンドを使用したピア ポリシー テンプレートの継承の設定」（P.73）を参照してください。

inherit peer-policy コマンドを使用したピア ポリシー テンプレートの継承の設定

この作業は、**inherit peer-policy** コマンドを使用して、ピア ポリシー テンプレートの継承を設定します。これは、ピア ポリシー テンプレートを作成、設定し、別のピア ポリシー テンプレートからコンフィギュレーションを継承できるようにします。

BGP ネイバーが継承したピア テンプレートを使用する場合、特定のテンプレートに関連付けられているポリシーを判断するのが難しいことがあります。Cisco IOS Release 12.0(25)S、12.4(11)T、12.2(33)SRB、12.2(33)SB、およびそれ以降のリリースでは、**show ip bgp template peer-policy** コマンドに、特定のテンプレートに関連付けられているローカル ポリシーおよび継承されたポリシーの詳しいコンフィギュレーションを表示するためのキーワード **detail** が追加されました。

（注） ステップ 5 と 6 のコマンドは任意で、サポートされている BGP ポリシー コンフィギュレーション コマンドのいずれとでも置き換えが可能です。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-policy** *policy-template-name*
5. **route-map** *map-name* {**in** | **out**}
6. **inherit peer-policy** *policy-template-name sequence-number*

7. **end**
8. **show ip bgp template peer-policy** [*policy-template-name* [**detail**]]

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`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**template peer-policy** *policy-template-name* **例：** `Router(config-router)# template peer-policy NETWORK1`	ポリシー テンプレート コンフィギュレーション モードを開始し、ピア ポリシー テンプレートを作成します。
ステップ 5	**route-map** *map-name* {**in** | **out**} **例：** `Router(config-router-ptmp)# route-map ROUTE in`	（任意）指定されたルート マップをインバウンド ルート、またはアウトバウンド ルートに適用します。 **（注）** ここでは、サポートされている BGP ポリシー コンフィギュレーション コマンドならどれでも使用できます。サポートされているコマンドのリストについては、「ピア ポリシー テンプレート」（P.67）を参照してください。
ステップ 6	**inherit peer-policy** *policy-template-name sequence-number* **例：** `Router(config-router-ptmp)# inherit peer-policy GLOBAL 10`	別のピア ポリシー テンプレートのコンフィギュレーションを継承するように、このピア ポリシー テンプレートを設定します。 • *sequence-number* 引数は、ピア ポリシー テンプレートの評価順序を設定します。ルート マップのシーケンス番号と同様、最も小さいシーケンス番号が最初に評価されます。 • この例では、GLOBAL からコンフィギュレーションを継承するようにピア ポリシー テンプレートを設定しています。これらの手順で作成されたテンプレートをネイバーに適用すると、コンフィギュレーション GLOBAL も間接的に継承され、適用されます。GLOBAL からはさらに最高 6 個のピア ポリシー テンプレートが間接継承され、合計 8 個のピア ポリシー テンプレートが直接適用、および間接継承されます。 • 他のテンプレートで、これより小さいシーケンス番号が設定されていなければ、この例のこのテンプレートが最初に評価されます。

	コマンドまたはアクション	目的
ステップ 7	**end** **例：** `Router(config-router-ptmp)# end`	ポリシー テンプレート 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。
ステップ 8	**show ip bgp template peer-policy** [*policy-template-name* [**detail**]] **例：** `Router# show ip bgp template peer-policy NETWORK1 detail`	ローカルに設定されたピア ポリシー テンプレートを表示します。 • *policy-template-name* 引数を使用して、ピア ポリシー テンプレートが 1 つだけ表示されるように、出力をフィルタできます。また、このコマンドは、標準出力修飾子すべてをサポートしています。 • 詳細なポリシー情報を表示するには、**detail** キーワードを使用します。 （注） **detail** キーワードがサポートされているのは、Cisco IOS Release 12.0(25)S、12.4(11)T、12.2(33)SRB、12.2(33)SB、およびそれ以降のリリースだけです。

例

次の例は、**show ip bgp template peer-policy** コマンドに **detail** キーワードをつけた場合の出力で、NETWORK1 というポリシーの詳細が表示されています。この例の出力からは、GLOBAL テンプレートが継承されたことがわかります。ルート マップおよびプレフィクス リスト コンフィギュレーションの詳細も表示されています。

```
Router# show ip bgp template peer-policy NETWORK1 detail

Template:NETWORK1, index:2.
Local policies:0x1, Inherited polices:0x80840
This template inherits:
  GLOBAL, index:1, seq_no:10, flags:0x1
Locally configured policies:
  route-map ROUTE in
Inherited policies:
  prefix-list NO-MARKETING in
  weight 300
  maximum-prefix 10000

 Template:NETWORK1 <detail>
Locally configured policies:
  route-map ROUTE in
route-map ROUTE, permit, sequence 10
  Match clauses:
    ip address prefix-lists: DEFAULT
ip prefix-list DEFAULT: 1 entries
   seq 5 permit 10.1.1.0/24

  Set clauses:
  Policy routing matches: 0 packets, 0 bytes

Inherited policies:
  prefix-list NO-MARKETING in
ip prefix-list NO-MARKETING: 1 entries
   seq 5 deny 10.2.2.0/24
```

neighbor inherit peer-policy コマンドを使用したピア ポリシー テンプレートの継承の設定

この作業では、**neighbor inherit peer-policy** コマンドを使用して、ピア ポリシー テンプレートをネイバーに送信し、継承させるようにルータを設定します。次の手順に従って、ピア ポリシー テンプレート コンフィギュレーションをネイバーに送信し、継承させます。

BGP ネイバーが複数レベルのピア テンプレートを使用する場合、ネイバーに適用されているポリシーを判断するのが難しいことがあります。Cisco IOS Release 12.0(25)S、12.4(11)T、12.2(33)SRB、12.2(33)SB、およびそれ以降のリリースでは、指定されたネイバーで継承されたポリシーと、直接設定されたポリシーを表示するためのキーワード **policy** と **detail** が **show ip bgp neighbors** コマンドに追加されました。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
6. **neighbor** *ip-address* **inherit peer-policy** *policy-template-name*
7. **end**
8. **show ip bgp neighbors** [*ip-address* [**policy** [**detail**]]]

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`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* **例：** `Router(config-router)# neighbor 192.168.1.2 remote-as 40000`	指定されたネイバーを使ってピアリング セッションを設定します。 • ステップ 6 の **neighbor inherit** 文を動作させるには、**remote-as** 文を明示的に使用する必要があります。ピアリングが設定されていない場合、ステップ 6 で指定されたネイバーはセッション テンプレートを受け付けません。

	コマンドまたはアクション	目的
ステップ 5	**address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*] **例：** `Router(config-router)# address-family ipv4 unicast`	アドレス ファミリ固有のコマンド コンフィギュレーションを使用するようにネイバーを設定するために、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。
ステップ 6	**neighbor** *ip-address* **inherit peer-policy** *policy-template-name* **例：** `Router(config-router-af)# neighbor 192.168.1.2 inherit peer-policy GLOBAL`	ネイバーが設定を継承できるように、ピア ポリシー テンプレートをこのネイバーに送信します。 • この例では、ピア ポリシー テンプレート GLOBAL を 192.168.1.2 ネイバーに送信し、継承させるようにルータを設定しています。このテンプレートはネイバーに適用できます。また、別のピア ポリシー テンプレートが GLOBAL から間接継承された場合、間接継承されたコンフィギュレーションも適用されます。GLOBAL からは、さらに最高 7 個のピア ポリシー テンプレートを間接継承できます。
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。
ステップ 8	**show ip bgp neighbors** [*ip-address* [**policy** [**detail**]]] **例：** `Router# show ip bgp neighbors 192.168.1.2 policy`	ローカルに設定されたピア ポリシー テンプレートを表示します。 • *policy-template-name* 引数を使用して、ピア ポリシー テンプレートが 1 つだけ表示されるように、出力をフィルタできます。また、このコマンドは、標準出力修飾子すべてをサポートしています。 • このネイバーに適用されているポリシーをアドレス ファミリごとに表示するには、**policy** キーワードを使用します。 • 詳細なポリシー情報を表示するには、**detail** キーワードを使用します。 • **policy** および **detail** キーワードがサポートされているのは、Cisco IOS Release 12.0(25)S、12.4(11)T、12.2(33)SRB、12.2(33)SB、およびそれ以降のリリースだけです。 **（注）** この作業に必要な構文だけが示されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次の出力例に表示されているのは、192.168.1.2 にあるネイバーに適用されたポリシーです。この出力には、継承されたポリシーと、このネイバー デバイスで設定されたポリシーの両方が表示されています。継承されたポリシーは、ピア グループ、またはピア ポリシー テンプレートからネイバーが継承したポリシーです。

```
Router# show ip bgp neighbors 192.168.1.2 policy

Neighbor: 192.168.1.2, Address-Family: IPv4 Unicast
```

```
Locally configured policies:
 route-map ROUTE in
Inherited polices:
 prefix-list NO-MARKETING in
 route-map ROUTE in
 weight 300
 maximum-prefix 10000
```

BGP ダイナミック アップデート グループのモニタリングとメンテナンス

ダイナミック BGP アップデート グループの処理に関する情報の表示およびクリアには、この作業を使用します。BGP アップデート グループを使用すると、BGP アップデート メッセージ生成のパフォーマンスが向上します。BGP ピア テンプレートが設定され、ダイナミック BGP アップデート ピア グループがサポートされたことにより、ネットワーク オペレータは BGP でピア グループを設定する必要がなくなります。また、コンフィギュレーションの柔軟性とシステム パフォーマンスの向上による恩恵を受けます。BGP ピア テンプレートの使用の詳細については、「ピア セッション テンプレートの設定」（P.59）、および「ピア ポリシー テンプレートの設定」（P.67）を参照してください。

BGP ダイナミック アップデート グループのコンフィギュレーション

Cisco IOS Release 12.0(24)S、12.2(18)S、12.3(4)T、12.2(27)SBC、およびそれ以降のリリースには、同一のアウトバウンド ポリシーを共有し、同一のアップデート メッセージを共有するネイバーのアップデート グループをダイナミックに計算および最適化できる新しいアルゴリズムが導入されました。BGP ダイナミック アップデート グループをイネーブルにするための設定は必要ありません。アルゴリズムは自動的に実行されます。アウトバウンド ポリシーが変更された場合、ルータは、1 分間のタイマー期限が切れた後で、アウトバウンド ソフト リセットをトリガーすることにより、自動的にアップデート グループ メンバシップを再計算し、変更を適用します。この動作は、ネットワーク オペレータがミスを犯した場合に、コンフィギュレーションを変更する時間を与えるように設計されています。タイマー期限が切れる前に、アウトバウンド ソフト リセットを手動でイネーブルにするには、**clear ip bgp** *ip-address* **soft out** コマンドを入力します。

（注） Cisco IOS Release 12.0(22)S、12.2(14)S、12.3(2)T およびそれ以前のリリースでは、アップデート グループの再計算遅延タイマーは 3 分間に設定されています。

BGP アップデート グループの生成を最適化するには、ネットワーク オペレータは、類似するアウトバウンド ポリシーを持つネイバーのアウトバウンド ルーティング ポリシーを同じものにしておくことを推奨します。

手順の概要

1. **enable**
2. **clear ip bgp update-group** [*index-group* | *ip-address*]
3. **show ip bgp replication** [*index-group* | *ip-address*]
4. **show ip bgp update-group** [*index-group* | *ip-address*] [**summary**]

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 **clear ip bgp update-group** [*index-group* | *ip-address*]

BGP アップデート メンバシップをクリアし、BGP アップデート グループを再計算するには、このコマンドを使用します。特定のアップデート グループをクリアするには、*index-group* 引数を使用します。アップデート グループのインデックス番号の範囲は 1 ～ 4294967295 です。特定のネイバーをクリアするには、*ip-address* 引数を使用します。引数が指定されていない場合、このコマンドは BGP アップデート グループをすべてクリアし、再計算します。

次の例は、アップデート グループから、ネイバー 192.168.2.2 のメンバシップをクリアします。

```
Router# clear ip bgp update-group 192.168.2.2
```

ステップ 3 **show ip bgp replication** [*index-group* | *ip-address*]

このコマンドは、BGP アップデート グループ レプリケーションの統計情報を表示します。特定のアップデート グループ レプリケーションの統計情報を表示するには、*index-group* 引数を使用します。アップデート グループのインデックス番号の範囲は 1 ～ 4294967295 です。特定のアップデート グループ レプリケーションの統計情報を表示するには、*ip-address* 引数を使用します。引数が指定されていない場合、このコマンドは、すべてのアップデート グループのレプリケーション統計情報を表示します。

次の例は、すべての BGP ネイバーのアップデート グループ レプリケーション情報を表示します。

```
Router# show ip bgp replication

BGP Total Messages Formatted/Enqueued : 0/0

     Index     Type  Members          Leader   MsgFmt  MsgRepl  Csize  Qsize
         1 internal        1     192.168.1.2        0        0      0      0
         2 internal        2     192.168.3.2        0        0      0      0
```

ステップ 4 **show ip bgp update-group** [*index-group* | *ip-address*] [**summary**]

BGP アップデート グループに関する情報を表示するには、このコマンドを使用します。特定のアップデート グループの統計情報を表示するには、*index-group* 引数を使用します。アップデート グループのインデックス番号の範囲は 1 ～ 4294967295 です。特定のアップデート グループの情報を表示するには、*ip-address* 引数を使用します。引数が指定されていない場合、このコマンドは、すべてのアップデート グループの統計情報を表示します。概要を表示するには、**summary** キーワードを使用します。

次の例は、すべてのネイバーのアップデート グループ情報を表示します。

```
Router# show ip bgp update-group

BGP version 4 update-group 1, external, Address Family: IPv4 Unicast
  BGP Update version : 8/0, messages 0
  Update messages formatted 11, replicated 3
  Number of NLRIs in the update sent: max 1, min 0
  Minimum time between advertisement runs is 30 seconds
  Has 2 members (* indicates the members currently being sent updates):
   192.168.1.2      192.168.3.2
```

トラブルシューティングのヒント

BGP アップデート グループの処理に関する情報を表示するには、**debug ip bgp groups** コマンドを使用します。すべてのアップデート グループ、個々のアップデート グループ、または特定の BGP ネイバーに関する情報を表示できます。このコマンドからは非常に詳しい情報が表示されます。問題のトラブルシューティングを行う場合を除き、運用中のネットワークでは、このコマンドを使用しないでください。

基本 BGP ネットワーク設定のコンフィギュレーション例

ここでは、次の例について説明します。

BGP プロセスの設定とピアのカスタマイズ：例

次の例は、図 4（P.29）に示されている異なる自律システムにある 2 つのネイバー ピア（ルータ A のピアとルータ E のピア）を使って BGP プロセスが設定されているルータ B のコンフィギュレーションを示しています。IPv4 ユニキャスト ルートは両方のピアと交換され、IPv4 マルチキャスト ルートはルータ E の BGP ピアと交換されます。

ルータ B

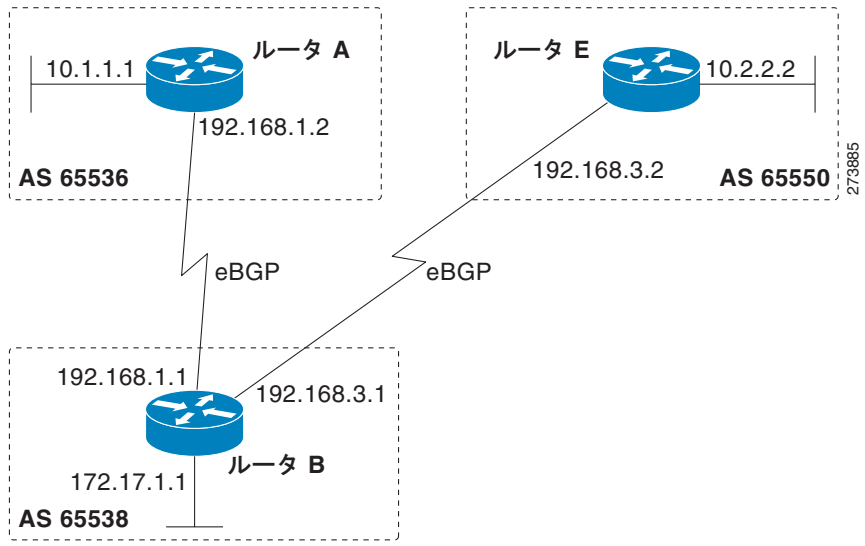
```
router bgp 45000
 bgp router-id 172.17.1.99
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.3.2 remote-as 50000
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
 !
 address-family ipv4 multicast
  neighbor 192.168.3.2 activate
  neighbor 192.168.3.2 advertisement-interval 25
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

BGP ルーティング プロセスと 4 バイト自律システム番号を使用したピアの設定：例

Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)SXI1、およびそれ以降のリリースにおける asplain デフォルト形式

次に、Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、およびそれ以降のリリースで使用可能な例を示します。これは、図 6 における BGP プロセスを使ったルータ A、B、E のコンフィギュレーションの例で、このプロセスは、asplain 表記法を使用して設定された 4 バイトの自律システムのルータ A、B、および E にある 3 つのネイバー ピアの間に設定されています。IPv4 ユニキャスト ルートはすべてのピアと交換されます。

図 6　　asplain 形式の 4 バイト自律システム番号を使用する BGP ピア



ルータ A

```
router bgp 65536
 bgp router-id 10.1.1.99
 no bgp default ipv4-unicast
 bgp fast-external-fallover
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.1.1 remote-as 65538
 !
 address-family ipv4
  neighbor 192.168.1.1 activate
  no auto-summary
  no synchronization
  network 10.1.1.0 mask 255.255.255.0
  exit-address-family
```

ルータ B

```
router bgp 65538
 bgp router-id 172.17.1.99
 no bgp default ipv4-unicast
 bgp fast-external-fallover
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.1.2 remote-as 65536
 neighbor 192.168.3.2 remote-as 65550
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

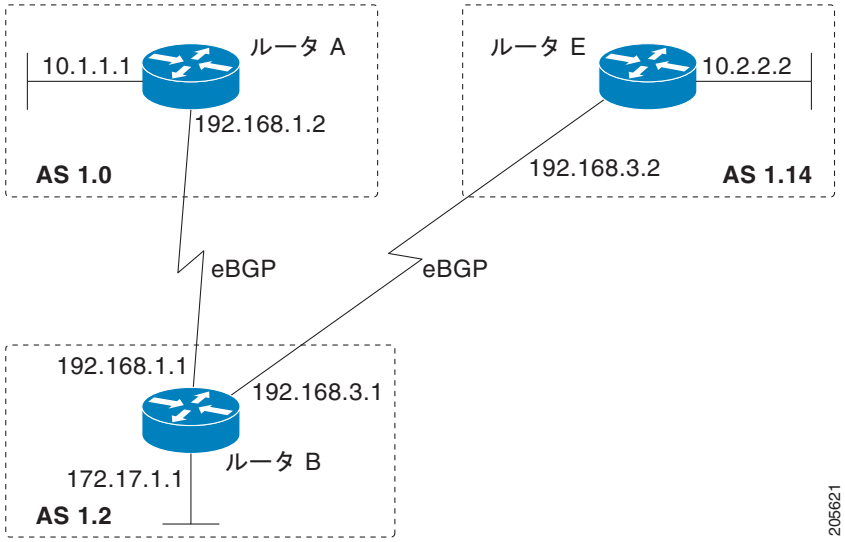
ルータ E

```
router bgp 65550
 bgp router-id 10.2.2.99
 no bgp default ipv4-unicast
 bgp fast-external-fallover
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.3.1 remote-as 65538
 !
 address-family ipv4
  neighbor 192.168.3.1 activate
  no auto-summary
  no synchronization
  network 10.2.2.0 mask 255.255.255.0
  exit-address-family
```

Cisco IOS Release 12.0(32)S12 および 12.4(24)T における asdot デフォルト形式

次に、Cisco IOS Release 12.0(32)S12 および 12.4(24)T で使用可能な例を示します。これは、図 6 における BGP プロセスを使ったルータ A、B、E のコンフィギュレーションを作成する方法の例で、このプロセスは、デフォルトの asdot 形式を使用して設定された 4 バイトの自律システムのルータ A、B、および E にある 3 つのネイバー ピアの間に設定されています。IPv4 ユニキャスト ルートはすべてのピアと交換されます。

図 7　asdot 形式の 4 バイト自律システム番号を使用する BGP ピア



ルータ A

```
router bgp 1.0
 bgp router-id 10.1.1.99
 no bgp default ipv4-unicast
 bgp fast-external-fallover
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.1.1 remote-as 1.2
 !
 address-family ipv4
  neighbor 192.168.1.1 activate
  no auto-summary
  no synchronization
  network 10.1.1.0 mask 255.255.255.0
  exit-address-family
```

ルータ B

```
router bgp 1.2
 bgp router-id 172.17.1.99
 no bgp default ipv4-unicast
 bgp fast-external-fallover
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.1.2 remote-as 1.0
 neighbor 192.168.3.2 remote-as 1.14
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

ルータ E

```
router bgp 1.14
 bgp router-id 10.2.2.99
```

```
 no bgp default ipv4-unicast
 bgp fast-external-fallover
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.3.1 remote-as 1.2
 !
 address-family ipv4
  neighbor 192.168.3.1 activate
  no auto-summary
  no synchronization
  network 10.2.2.0 mask 255.255.255.0
  exit-address-family
```

4 バイトの BGP 自律システム番号を使用した VRF および拡張コミュニティの設定：例

Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)SXI1、およびそれ以降のリリースにおける asplain デフォルト形式

次の例は、Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、およびそれ以降のリリースで使用可能です。この例は、4 バイト自律システム番号 65537 を使用するルート ターゲットを使って VRF を作成する方法、およびルート ターゲットに、ルート マップにより許可されたルートの拡張コミュニティ値 65537:100 を設定する方法を示しています。

```
ip vrf vpn_red
 rd 64500:100
 route-target both 65537:100
 exit
route-map red_map permit 10
 set extcommunity rt 65537:100
 end
```

コンフィギュレーションの完了後、**show route-map** コマンドを使用して、拡張コミュニティが、4 バイト自律システム番号 65537 を含むルート ターゲットに設定されていることを確認します。

```
RouterB# show route-map red_map

route-map red_map, permit, sequence 10
  Match clauses:
  Set clauses:
    extended community RT:65537:100
  Policy routing matches: 0 packets, 0 bytes
```

Cisco IOS Release 12.0(32)S12 および 12.4(24)T における asdot デフォルト形式

次の例は、Cisco IOS Release 12.0(32)S12 および 12.4(24)T で使用可能です。この例は、4 バイト自律システム番号 1.1 を使用するルート ターゲットを使って VRF を作成する方法、およびルート ターゲットに、ルート マップにより許可されたルートの拡張コミュニティ値 1.1:100 を設定する方法を示しています。

（注） Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SXI1、およびそれ以降のリリースでは、この例が正常に動作するのは、**bgp asnotation dot** コマンドを使用して、asdot をデフォルトの表示形式として設定した場合だけです。

```
ip vrf vpn_red
 rd 64500:100
 route-target both 1.1:100
 exit
route-map red_map permit 10
 set extcommunity rt 1.1:100
 end
```

コンフィギュレーションの完了後、**show route-map** コマンドを使用して、拡張コミュニティが、4 バイト自律システム番号 1.1 を含むルート ターゲットに設定されていることを確認します。

```
RouterB# show route-map red_map

route-map red_map, permit, sequence 10
  Match clauses:
  Set clauses:
    extended community RT:1.1:100
  Policy routing matches: 0 packets, 0 bytes
```

NLRI から AFI へのコンフィギュレーション：例

次の例は、既存のルータ コンフィギュレーション ファイルを NLRI 形式から AFI 形式にアップグレードし、AFI 形式のコマンドだけを使用するようにルータの CLI を設定します。

```
router bgp 60000
 bgp upgrade-cli
```

既存のルータ コンフィギュレーション ファイルが NLRI 形式から AFI 形式にアップグレードされていることを確認するには、特権 EXEC モードで **show running-config** コマンドを使用します。次のセクションでは、NLRI 形式のルータ コンフィギュレーション ファイルからの出力例と、ルータ コンフィギュレーション モードで **bgp upgrade-cli** コマンドを使って、このファイルを AFI 形式にアップグレードした後の出力例を示します。

- 次の「アップグレード前の NLRI 形式のルータ コンフィギュレーション ファイル」
- 「アップグレード後の AFI 形式のルータ コンフィギュレーション ファイル」（P.83）

（注） **bgp upgrade-cli** コマンドを使って、AFI 形式から NLRI 形式にルータをアップグレードすると、NLRI コマンドを使用したり、設定したりできなくなります。

アップグレード前の NLRI 形式のルータ コンフィギュレーション ファイル

次に示すのは、特権 EXEC モードでの **show running-config** コマンドからの出力例です。この出力例には、**bgp upgrade-cli** コマンドを使って AFI 形式にアップグレードする前のルータ コンフィギュレーション ファイルが NLRI 形式で表示されています。この出力例は、ルータ コンフィギュレーションのうち、影響を受ける部分だけが表示されるようにフィルタ処理されています。

```
Router# show running-config | begin bgp

router bgp 101
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.1.1.1 remote-as 505 nlri unicast multicast
 no auto-summary
!
ip default-gateway 10.4.9.1
ip classless
!
!
```

```
route-map REDISTRIBUTE-MULTICAST permit 10
 match ip address prefix-list MULTICAST-PREFIXES
 set nlri multicast
!
route-map MULTICAST-PREFIXES permit 10
!
route-map REDISTRIBUTE-UNICAST permit 20
 match ip address prefix-list UNICAST-PREFIXES
 set nlri unicast
!
!
!
line con 0
line aux 0
line vty 0 4
 password PASSWORD
 login
!
end
```

アップグレード後の AFI 形式のルータ コンフィギュレーション ファイル

次に示すのは、AFI 形式にアップグレードした後のルータ コンフィギュレーション ファイルの出力例です。この出力例は、ルータ コンフィギュレーション ファイルのうち、影響を受ける部分だけが表示されるようにフィルタ処理されています。

```
Router# show running-config | begin bgp

router bgp 101
 bgp log-neighbor-changes
 neighbor 10.1.1.1 remote-as 505
 no auto-summary
 !
 address-family ipv4 multicast
  neighbor 10.1.1.1 activate
  no auto-summary
  no synchronization
  exit-address-family
 !
 address-family ipv4
  neighbor 10.1.1.1 activate
  no auto-summary
  no synchronization
  exit-address-family
!
ip default-gateway 10.4.9.1
ip classless
!
!
route-map REDISTRIBUTE-MULTICAST_mcast permit 10
 match ip address prefix-list MULTICAST-PREFIXES
!
route-map REDISTRIBUTE-MULTICAST permit 10
 match ip address prefix-list MULTICAST-PREFIXES
!
route-map MULTICAST-PREFIXES permit 10
!
route-map REDISTRIBUTE-UNICAST permit 20
 match ip address prefix-list UNICAST-PREFIXES
!
!
!
line con 0
line aux 0
```

```
line vty 0 4
 password PASSWORD
 login
!
end
```

再配布の例を使用した BGP コンフィギュレーション コマンドの削除：例

次の例は、ルート マップを使用して、EIGRP への BGP ルートの再配布をイネーブルにする CLI コンフィギュレーションと、再配布とルート マップを削除する CLI コンフィギュレーションの両方を示しています。BGP コンフィギュレーション コマンドの中には、他の CLI コマンドに影響を与えるものもありますが、この例は、あるコマンドの削除が他のコマンドにどのような影響を与えるかを示しています。

1 つ目のコンフィギュレーション例では、ルート マップは、自律システム番号をマッチングおよび設定するように設定されています。3 つの異なる自律システムにある BGP ネイバーが設定およびアクティブ化されます。EIGRP ルーティング プロセスが開始され、ルート マップを使用して、EIGRP への BGP ルートの再配布が設定されます。

EIGRP への BGP ルート再配布をイネーブルにする CLI

```
route-map bgp-to-eigrp permit 10
 match tag 50000
 set tag 65000
 exit
router bgp 45000
 bgp log-neighbor-changes
 address-family ipv4
  neighbor 172.16.1.2 remote-as 45000
  neighbor 172.21.1.2 remote-as 45000
  neighbor 192.168.1.2 remote-as 40000
  neighbor 192.168.3.2 remote-as 50000
  neighbor 172.16.1.2 activate
  neighbor 172.21.1.2 activate
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
 exit
router eigrp 100
 redistribute bgp 45000 metric 10000 100 255 1 1500 route-map bgp-to-eigrp
 no auto-summary
 exit
```

2 つ目のコンフィギュレーション例では、**route-map** コマンドと **redistribute** コマンドの両方がディセーブルにされています。route-map コマンドだけを削除した場合、再配布が自動的にディセーブルにされることはありません。再配布は行われますが、マッチングやフィルタリングは行われません。再配布コンフィギュレーションを削除するには、**redistribute** コマンドもディセーブルにする必要があります。

EIGRP への BGP ルート再配布を削除する CLI

```
configure terminal
 no route-map bgp-to-eigrp
 router eigrp 100
  no redistribute bgp 45000
  end
```

BGP ソフト リセット：例

次の例は、BGP ピア 192.168.1.1 の接続をリセットする 2 通りの方法を示しています。

ダイナミック インバウンド ソフト リセットの例

次の例では、**clear ip bgp 192.168.1.1 soft in** EXEC コマンドを使用して、BGP ピア 192.168.1.1 でダイナミック ソフト再構成を開始します。このコマンドを使用するには、ピアでルート リフレッシュ機能がサポートされている必要があります。

```
clear ip bgp 192.168.1.1 soft in
```

格納された情報を使用したインバウンド ソフト リセットの例

次の例では、ネイバー 192.168.1.1 に対してインバウンド ソフト再構成をイネーブルにする方法を示しています。このネイバーから受信したアップデートは、インバウンド ポリシーに関係なく、すべてそのまま格納されます。インバウンド ソフトウェア再構成を後で行う場合、格納された情報を使用して、新たに一連のインバウンド アップデートが生成されます。

```
router bgp 100
 neighbor 192.168.1.1 remote-as 200
 neighbor 192.168.1.1 soft-reconfiguration inbound
```

次の例では、ネイバー 192.168.1.1 のセッションがクリアされます。

```
clear ip bgp 192.168.1.1 soft in
```

4 バイト自律システム番号を使用する BGP ピアのリセット：例

次の例は、4 バイト自律システム番号を使用する自律システムに属する BGP ピアをクリアする方法を示しています。この例では、ルータで、Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1 またはそれ以降のリリースが実行されている必要があります。BGP ルーティング テーブルの初期状態が、**show ip bgp** コマンドを使用して示されています。また、4 バイトの自律システム 65536 と 65550 にあるピアも表示されます。

```
RouterB# show ip bgp

BGP table version is 4, local router ID is 172.17.1.99
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
*> 10.1.1.0/24      192.168.1.2              0             0 65536  i
*> 10.2.2.0/24      192.168.3.2              0             0 65550  i
*> 172.17.1.0/24    0.0.0.0                  0         32768 i
```

4 バイトの自律システム 65550 にある BGP ピアをすべて削除するために、**clear ip bgp 65550** コマンドが実行されます。ADJCHANGE メッセージからは、192.168.3.2 にある BGP ピアがリセットされていることがわかります。

```
RouterB# clear ip bgp 65550
RouterB#
*Nov 30 23:25:27.043: %BGP-5-ADJCHANGE: neighbor 192.168.3.2 Down User reset
```

もう一度、**show ip bgp** コマンドが実行されますが、今度は 4 バイトの自律システム 65536 内のピアだけが表示されます。

```
RouterB# show ip bgp
```

```
BGP table version is 5, local router ID is 172.17.1.99
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
*> 10.1.1.0/24      192.168.1.2              0             0 65536  i
*> 172.17.1.0/24    0.0.0.0                  0         32768 i
```

その直後、次の ADJCHANGE メッセージが表示され、4 バイトの自律システム 65550 で、192.168.3.2 の BGP ピアが稼動状態になったことが示されます。

```
RouterB#
*Nov 30 23:25:55.995: %BGP-5-ADJCHANGE: neighbor 192.168.3.2 Up
```

BGP を使用したプレフィクスの集約：例

次の例は、集約ルートを BGP に再配布するか、または BGP 条件付き集約ルーティング機能を使用することにより、BGP で集約ルートを使用する方法を示します。

次の例では、**redistribute static** ルータ コンフィギュレーション コマンドを使用して、集約ルート 10.0.0.0 が再配布されます。

```
ip route 10.0.0.0 255.0.0.0 null 0
!
router bgp 100
 redistribute static
```

次のコンフィギュレーションは、少なくとも 1 つのルートが指定された範囲に含まれる場合に、BGP ルーティング テーブルに集約エントリを作成する方法を示します。自律システムから受け取られるに従って、集約ルートはアドバタイズされます。また、この集約ルートには、情報が失われている可能性を示すために、atomic aggregate アトリビュートが設定されています（デフォルトでは、**aggregate-address** ルータ コンフィギュレーション コマンドで **as-set** キーワードを使用しない限り、atomic aggregate は設定されています）。

```
router bgp 100
 aggregate-address 10.0.0.0 255.0.0.0
```

次の例は、直前の例と同じルールを使用して集約エントリを作成する方法を示していますが、このルートでアドバタイズされるパスは、要約されているパスすべてに含まれるすべての要素から構成される AS-SET です。

```
router bgp 100
 aggregate-address 10.0.0.0 255.0.0.0 as-set
```

次の例は、10.0.0.0 に対する集約ルートを作成しながら、すべてのネイバーへのより具体的なルートのアドバタイズメントを抑制する方法を示します。

```
router bgp 100
 aggregate-address 10.0.0.0 255.0.0.0 summary-only
```

グローバル コンフィギュレーション モードで始まる次の例は、非アクティブなルートをアドバタイズしないように BGP を設定します。

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 unicast
Router(config-router-af)# bgp suppress-inactive
Router(config-router-af)# end
```

次の例は、red という名前の VRF でルートの上限を設定し、RED という名前の VRF 経由で非アクティブなルートをアドバタイズしないように BGP を設定します。

```
Router(config)# ip vrf RED
Router(config-vrf)# rd 50000:10
Router(config-vrf)# maximum routes 1000 10
Router(config-vrf)# exit
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 vrf RED
Router(config-router-af)# bgp suppress-inactive
Router(config-router-af)# end
```

BGP ピア グループの設定：例

次の例は、アドレス ファミリを使用して、ピア グループのすべてのメンバがユニキャストとマルチキャストの両方に対応できるようにピア グループを設定する方法を示しています。

```
router bgp 45000
neighbor 192.168.1.2 remote-as 40000
neighbor 192.168.3.2 remote-as 50000
address-family ipv4 unicast
 neighbor mygroup peer-group
 neighbor 192.168.1.2 peer-group mygroup
 neighbor 192.168.3.2 peer-group mygroup

router bgp 45000
neighbor 192.168.1.2 remote-as 40000
neighbor 192.168.3.2 remote-as 50000
address-family ipv4 multicast
 neighbor mygroup peer-group
 neighbor 192.168.1.2 peer-group mygroup
 neighbor 192.168.3.2 peer-group mygroup
 neighbor 192.168.1.2 activate
 neighbor 192.168.3.2 activate
```

ピア セッション テンプレートの設定：例

次の例は、セッション テンプレート コンフィギュレーション モードで、INTERNAL-BGP という名前のピア セッション テンプレートを作成します。

```
router bgp 45000
 template peer-session INTERNAL-BGP
 remote-as 50000
 timers 30 300
 exit-peer-session
```

次の例は、ピア セッション テンプレート CORE1 を作成します。この例は、INTERNAL-BGP というピア セッション テンプレートのコンフィギュレーションを継承します。

```
router bgp 45000
 template peer-session CORE1
 description CORE-123
 update-source loopback 1
 inherit peer-session INTERNAL-BGP
 exit-peer-session
```

次の例は、CORE1 ピア セッション テンプレートを継承するように、192.168.3.2 ネイバーを設定します。192.168.3.2 ネイバーも、ピア セッション テンプレート INTERNAL-BGP から間接的にコンフィギュレーションを継承します。ネイバー継承文を動作させるには、**remote-as** 文を明示的に使用する必要があります。ピアリングが設定されていない場合、指定されたネイバーはセッション テンプレートを受け付けません。

```
router bgp 45000
 neighbor 192.168.3.2 remote-as 50000
 neighbor 192.168.3.2 inherit peer-session CORE1
```

ピア ポリシー テンプレートの設定：例

次の例は、ポリシー テンプレート コンフィギュレーション モードで、GLOBAL という名前のピア ポリシー テンプレートを作成します。

```
router bgp 45000
 template peer-policy GLOBAL
 weight 1000
 maximum-prefix 5000
 prefix-list NO_SALES in
 exit-peer-policy
```

次の例は、ポリシー テンプレート コンフィギュレーション モードで、PRIMARY-IN という名前のピア ポリシー テンプレートを作成します。

```
template peer-policy PRIMARY-IN
 prefix-list ALLOW-PRIMARY-A in
 route-map SET-LOCAL in
 weight 2345
 default-originate
 exit-peer-policy
```

次の例は、ピア ポリシー テンプレート CUSTOMER-A を作成します。このピア ポリシー テンプレートは、PRIMARY-IN および GLOBAL という名前のピア ポリシー テンプレートからコンフィギュレーションを継承するように設定されています。

```
template peer-policy CUSTOMER-A
 route-map SET-COMMUNITY in
 filter-list 20 in
 inherit peer-policy PRIMARY-IN 20
 inherit peer-policy GLOBAL 10
 exit-peer-policy
```

次の例は、アドレス ファミリ モードでピア ポリシー テンプレート名 CUSTOMER-A を継承するように、192.168.2.2 ネイバーを設定します。192.168.2.2 ネイバーも、ピア ポリシー テンプレート PRIMARY-IN および GLOBAL から間接的に継承します。

```
router bgp 45000
 neighbor 192.168.2.2 remote-as 50000
 address-family ipv4 unicast
  neighbor 192.168.2.2 inherit peer-policy CUSTOMER-A
  end
```

BGP ダイナミック アップデート ピア グループのモニタリングとメンテナンス：例

ピア グループの BGP ダイナミック アップデート グループをイネーブルにするための設定は必要ありません。アルゴリズムは自動的に実行されます。次の例は、BGP アップデート グループ情報をクリアまたは表示する方法を示しています。

clear ip bgp update-group の例

次の例は、アップデート グループから、ネイバー 10.0.0.1 のメンバシップをクリアします。

```
Router# clear ip bgp update-group 10.0.0.1
```

debug ip bgp groups の例

次に示す **debug ip bgp groups** コマンドからの出力例からは、**clear ip bgp groups** コマンドの実行後に、アップデート グループが再計算されていることがわかります。

```
Router# debug ip bgp groups

5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.5 Down User reset
5w4d: BGP-DYN(0): Comparing neighbor 10.4.9.5 flags 0x0 cap 0x0 and updgrp 2 fl0
5w4d: BGP-DYN(0): Update-group 2 flags 0x0 cap 0x0 policies same as 10.4.9.5 fl0
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.8 Down User reset
5w4d: BGP-DYN(0): Comparing neighbor 10.4.9.8 flags 0x0 cap 0x0 and updgrp 2 fl0
5w4d: BGP-DYN(0): Update-group 2 flags 0x0 cap 0x0 policies same as 10.4.9.8 fl0
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.21 Down User reset
5w4d: BGP-DYN(0): Comparing neighbor 10.4.9.21 flags 0x0 cap 0x0 and updgrp 1 f0
5w4d: BGP-DYN(0): Update-group 1 flags 0x0 cap 0x0 policies same as 10.4.9.21 f0
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.5 Up
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.21 Up
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.8 Up
```

show ip bgp replication の例

次の **show ip bgp replication** コマンドからの出力例には、すべてのネイバーに関するアップデート グループ レプリケーション情報が表示されます。

```
Router# show ip bgp replication

BGP Total Messages Formatted/Enqueued : 0/0

     Index     Type  Members          Leader   MsgFmt  MsgRepl  Csize  Qsize
         1 internal        1       10.4.9.21        0        0      0      0
         2 internal        2        10.4.9.5        0        0      0      0
```

show ip bgp update-group の例

次の **show ip bgp update-group** コマンドからの出力例には、すべてのネイバーに関するアップデート グループ情報が表示されます。

```
Router# show ip bgp update-group

BGP version 4 update-group 1, internal, Address Family: IPv4 Unicast
  BGP Update version : 0, messages 0/0
  Route map for outgoing advertisements is COST1
  Update messages formatted 0, replicated 0
  Number of NLRIs in the update sent: max 0, min 0
  Minimum time between advertisement runs is 5 seconds
  Has 1 member:
  10.4.9.21

BGP version 4 update-group 2, internal, Address Family: IPv4 Unicast
```

```
BGP Update version : 0, messages 0/0
Update messages formatted 0, replicated 0
Number of NLRIs in the update sent: max 0, min 0
Minimum time between advertisement runs is 5 seconds
Has 2 members:
10.4.9.5 10.4.9.8
```

次の作業

- 外部サービス プロバイダーへの接続については、「Connecting to a Service Provider Using External BGP」モジュールを参照してください。
- BGP ネイバー セッション オプションの設定については、「Configuring BGP Neighbor Session Options」モジュールを参照してください。
- iBGP 機能の設定については、「Configuring Internal BGP Features」モジュールを参照してください。

参考資料

ここでは、基本的な BGP 作業の設定に関連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
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
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*』
IPv6 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、使用上の注意事項、および例	『*Cisco IOS IPv6 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 BGP Overview」モジュール
IPv4 VRF アドレス ファミリを使った Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）および BGP コンフィギュレーションの例	「Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels」モジュール
基本的な MPLS VPN および BGP コンフィギュレーションの例	「*Configuring MPLS Layer 3 VPNs*」モジュール

規格

規格	タイトル
MDT SAFI	MDT SAFI

MIB

MIB	MIB リンク
CISCO-BGP4-MIB	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
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
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/cisco/web/support/index.html

基本 BGP ネットワーク設定の機能情報

表 6 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。

このテクノロジーの機能でここに記載されていないものについては、『Cisco BGP Features Roadmap』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、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、機能セット、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 からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 6 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。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。

表 6　基本 BGP ネットワーク設定の機能情報

機能名	リリース	機能の設定情報
BGP バージョン 4	Cisco IOS XE 3.1.0SG	BGP は、独自のルーティング ポリシー（自律システム）を持つ異なるルーティング ドメイン間に、ループのないルーティングを行うように設計されたドメイン間ルーティング プロトコルです。BGP バージョン 4 の Cisco IOS ソフトウェア実装には、BGP が IP マルチキャスト ルートに関するルーティング情報を伝送できるようにするマルチプロトコル拡張機能と、IP Version 4（IPv4; IP バージョン 4）、IP Version 6（IPv6; IP バージョン 6）、Virtual Private Networks Version 4（VPNv4; バーチャル プライベート ネットワーク バージョン 4）、および Connectionless Network Services（CLNS; コネクションレス型ネットワーク サービス）を含む複数のレイヤ 3 プロトコル アドレス ファミリが組み込まれています。 この機能については、次の項に説明があります。 • 「BGP バージョン 4」（P.2）
BGP 条件付きルートの挿入	12.0(22)S 12.2(4)T 12.2(14)S 15.0(1)S Cisco IOS XE 3.1.0SG	BGP 条件付きルート挿入機能を使用すると、通常のルート集約を通じて選択されたあまり具体的ではないプレフィクスよりも、より具体的なプレフィクスを BGP ルーティング テーブルに挿入することができます。より具体的なプレフィクスを使用すると、集約されたルートを使う場合よりも、よりきめ細かなトラフィック エンジニアリングや管理制御を行うことができます。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP ルート集約」（P.8） • 「BGP ルートの条件付き挿入」（P.52）

表 6　基本 BGP ネットワーク設定の機能情報 （続き）

機能名	リリース	機能の設定情報
ピア テンプレートを使用した BGP コンフィギュレーション	12.0(24)S 12.2(18)S 12.2(27)SBC 12.3(4)T 15.0(1)S	ピア テンプレートを使用した BGP コンフィギュレーション機能により、ポリシーを共有する BGP ネイバーに対して、ネイバー コンフィギュレーションをグループ化する新しいメカニズムが導入されます。このタイプのポリシー コンフィギュレーションは、伝統的に BGP ピア グループを使って設定されています。ただし、ピア グループ コンフィギュレーションは、アップデート グループと特定セッションの特性に左右されるため、ピア グループには何らかの制限があります。コンフィギュレーション テンプレートはピア グループ コンフィギュレーションに代わるものを提供し、ピア グループの制約の一部を解決します。 次のセクションで、この機能に関する情報を参照できます。 • 「ピア テンプレート」（P.10） • 「ピア セッション テンプレートの設定」（P.59） • 「ピア ポリシー テンプレートの設定」（P.67）
BGP ダイナミック アップデート ピア グループ	12.0(24)S 12.2(18)S 12.2(27)SBC 12.3(4)T 15.0(1)S Cisco IOS XE 3.1.0SG	BGP ダイナミック アップデート ピア グループ機能により、同じアウトバウンド ポリシーを共有し、同じアップデート メッセージを共有できるネイバーのアップデート グループをダイナミックに計算し、最適化する新しいアルゴリズムが導入されます。Cisco IOS ソフトウェアの古いバージョンでは、BGP アップデート メッセージは、ピア グループ コンフィギュレーションに基づいてグループ化されていました。このグループ化の方法により、限定されたアウトバウンド ポリシーと特定のセッション コンフィギュレーションがアップデートされます。BGP ダイナミック アップデート ピア グループ機能では、アップデート グループ レプリケーションはピア グループ コンフィギュレーションから分離されるため、ネイバー コンフィギュレーションのコンバージェンス時間が短縮され、柔軟性が高まります。 次のセクションで、この機能に関する情報を参照できます。 • 「ピア グループおよび BGP アップデート メッセージ」（P.9） • 「BGP アップデート グループ」（P.10） • 「BGP ダイナミック アップデート グループのモニタリングとメンテナンス」（P.75）

表 6　基本 BGP ネットワーク設定の機能情報 （続き）

機能名	リリース	機能の設定情報
BGP ハイブリッド CLI	12.0(22)S 12.2(15)T 15.0(1)S	BGP ハイブリッド CLI 機能は、BGP ネットワークと既存のコンフィギュレーションの NLRI 形式から AFI 形式への 移行を簡素化します。この新しい機能により、ネットワーク オペレータは、AFI 形式でコマンドを設定し、この設定を既存の NLRI 形式の設定に保存することができます。この機能により、ネットワーク オペレータは、新しい機能を活用し、NLRI 形式から AFI 形式への移行をサポートできるようになります。 次のセクションで、この機能に関する情報を参照できます。 • 「シスコシステムズが採用している BGP グローバル コマンドとアドレス ファミリ コンフィギュレーション コマンド」（P.6） • 「NLRI から AFI へのコンフィギュレーション：例」（P.82）
BGP ネイバー ポリシー	12.2(33)SB 12.2(33)SRB 12.4(11)T Cisco IOS XE 3.1.0SG	BGP ネイバー ポリシー機能により、ローカル ポリシー、および継承されたポリシーに関する情報を表示するための既存の 2 つのコマンドに新しいキーワードが導入されます。BGP ネイバーが複数レベルのピア テンプレートを使用する場合、ネイバーに適用されているポリシーを判断するのが難しいことがあります。継承されたポリシーは、ピア グループ、またはピア ポリシー テンプレートからネイバーが継承したポリシーです。 次のセクションで、この機能に関する情報を参照できます。 • 「ピア ポリシー テンプレートの設定」（P.67） • 「ピア ポリシー テンプレートの設定：例」（P.88） この機能では、**show ip bgp neighbors**、および **show ip bgp template peer-policy** 機能が変更されました。

表 6　基本 BGP ネットワーク設定の機能情報 （続き）

機能名	リリース	機能の設定情報
4 バイト ASN に対する BGP サポート	12.0(32)S12 12.0(32)SY8 12.0(33)S3 12.2(33)SRE 12.2(33)XNE 12.2(33)SXI1 、 12.4(24)T 15.0(1)S Cisco IOS XE 3.1.0SG	4 バイト ASN に対する BGP サポート機能により、4 バイト自律システム番号がサポートされるようになりました。自律システム番号の要求の増加に伴い、IANA は 2009 年 1 月から 65536 ～ 4294967295 の範囲の 4 バイト自律システム番号の割り当てを開始します。 Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、およびそれ以降のリリースでは、シスコシステムズが採用している 4 バイト自律システム番号は、自律システム番号の正規表現のマッチングおよび出力表示形式のデフォルトとして asplain を使用していますが、RFC 5396 に記載されているとおり、4 バイト自律システム番号を asplain 形式および asdot 形式の両方で設定できます。4 バイト自律システム番号の正規表現マッチングと出力表示のデフォルトを asdot 形式に変更するには、**bgp asnotation dot** コマンドを使用します。 Cisco IOS Release 12.0(32)S12 および 12.4(24)T では、4 バイト自律システム番号の設定形式、正規表現マッチング、出力表示の実装として、シスコは asdot だけを使用しており、asplain はサポートされていません。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP 自律システム番号の形式」（P.3） • 「BGP ルーティング プロセスと 4 バイト自律システム番号を使用したピアの設定」（P.18） • 「4 バイト自律システム番号で使用される出力および正規表現とのマッチング形式のデフォルトを変更」（P.22） • 「BGP ルーティング プロセスと 4 バイト自律システム番号を使用したピアの設定：例」（P.78） • 「4 バイトの BGP 自律システム番号を使用した VRF および拡張コミュニティの設定：例」（P.81） • 「4 バイト自律システム番号を使用する BGP ピアのリセット：例」（P.85） この機能により、次の各コマンドが追加または変更されています。**bgp asnotation dot**、**bgp confederation identifier**、**bgp confederation peers**、自律システム番号を設定するすべての **clear ip bgp** コマンド、**ip as-path access-list**、**ip extcommunity-list**、**match source-protocol**、**neighbor local-as**、**neighbor remote-as**、**neighbor soo**、**redistribute** (IP)、**router bgp**、**route-target**、**set as-path**、**set extcommunity**、**set origin**、**soo**、自律システム番号を表示するすべての **show ip bgp** コマンド、および **show ip extcommunity-list**。

表 6　基本 BGP ネットワーク設定の機能情報 （続き）

機能名	リリース	機能の設定情報
非アクティブなルートに対する BGP アドバタイズメントの抑制	12.2(25)S 12.2(33)SXH 15.0(1)M 15.0(1)S	非アクティブなルートに対する BGP アドバタイズメントの抑制機能では、ルーティング情報ベース（RIB）にインストールされていないルートに対するアドバタイズメントが行われないように設定できます。この機能を設定すると、ボーダー ゲートウェイ プロトコル（BGP）の更新と、トラフィックの転送に使用されるデータとの整合性がより高まります。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP ルート集約」（P.8） • 「BGP を使用した非アクティブなルート アドバタイズメントの抑制」（P.46） • 「BGP を使用したプレフィクスの集約：例」（P.86）