BGP

この章では、Border Gateway Protocol（BGP）を使用してデータのルーティング、認証の実行、ルーティング情報の再配布を行うように ASA を設定する方法について説明します。

BGPについて

BGP は相互および内部の自律システムのルーティングプロトコルです。自律システムとは、共通の管理下にあり、共通のルーティングポリシーを使用するネットワークまたはネットワークのグループです。BGP は、インターネットのルーティング情報を交換するために、インターネット サービス プロバイダー（ISP）間で使用されるプロトコルです。

BGP を使用する状況

通常、大学や企業などの顧客ネットワークではネットワーク内でルーティング情報を交換するために OSPF などの Interior Gateway Protocol（IGP）を採用しています。カスタマーはISPに接続し、ISPはBGPを使用してカスタマーおよびISPルートを交換します。自律システム（AS）間でBGPを使用する場合、このプロトコルは外部BGP（EBGP）と呼ばれます。サービスプロバイダーがBGPを使用してAS内のルートを交換する場合、このプロトコルは内部BGP（IBGP）と呼ばれます。

BGPは、IPv6ネットワーク上でIPv6プレフィックスのルーティング情報を伝送するためにも使用することができます。

（注） BGPv6 デバイスがクラスタに参加すると、ロギング レベル 7 が有効の場合、ソフト トレースバックを生成します。

ルーティング テーブルの変更

BGP ネイバーは、ネイバー間で最初に TCP 接続を確立する際に、完全なルーティング情報を交換します。ルーティングテーブルで変更が検出された場合、BGPルータはネイバーに対し、変更されたルートのみを送信します。BGP ルータは、定期的にルーティング アップデートを送信しません。また BGP ルーティング アップデートは、宛先ネットワークに対する最適パスのアドバタイズのみを行います。

（注） AS ループの検出は、完全な AS パス（AS_PATH 属性で指定される）をスキャンし、ローカル システムの AS 番号が AS パスに現れないことを確認することによって実行されます。デフォルトでは、EBGP は学習したルートを同じピアにアドバタイズすることで、ループチェックを実行するときにデバイスで追加の CPU サイクルが発生することを防ぐとともに、既存の発信更新タスクの遅延を防ぎます。

BGPにより学習されたルートには、特定の宛先に対して複数のパスが存在する場合、宛先に対する最適なルートを決定するために使用されるプロパティが設定されています。次のプロパティはBGP属性と呼ばれ、ルート選択プロセスで使用されます。

- Weight: これはシスコ定義の属性で、ルータに対してローカルです。Weight属性は、隣接ルータにアドバタイズされません。ルータが同じ宛先への複数のルートがあることを学習すると、[重み（Weight）] 属性値が最も大きいルートが優先されます。
- Local preference: Local preference属性は、ローカルASからの出口点を選択するために使用されます。Weight属性とは異なり、Local preference属性は、ローカルAS全体に伝搬されます。ASからの出口点が複数ある場合は、Local preference属性が最も高い出口点が特定のルートの出口点として使用されます。
- Multi-exit discriminator: メトリック属性であるMulti-exit discriminator (MED)は、メトリックをアドバタイズしているASへの優先ルートに関して、外部ASへの提案として使用されます。これが提案と呼ばれるのは、MEDを受信している外部ASがルート選択の際に他のBGP属性も使用している可能性があるためです。MEDメトリックが小さい方のルートが優先されます。
- Origin: Origin属性は、BGPが特定のルートについてどのように学習したかを示します。Origin属性は、次の3つの値のいずれかに設定することができ、ルート選択に使用されます。
  - IGP: ルートは発信側ASの内部にあります。この値は、ネットワークルータコンフィギュレーションコマンドを使用してBGPにルートを挿入する場合に設定されます。
  - EGP: ルートはExterior Border Gateway Protocol (EBGP)を使用して学習されます。
  - Incomplete: ルートの送信元が不明であるか、他の方法で学習されています。IncompleteのOriginは、ルートがBGPに再配布されるときに発生します。

- AS_path：ルートアドバタイズメントが自律システムを通過すると、ルートアドバタイズメントが通過した AS 番号が AS 番号の順序付きリストに追加されます。AS_path リストが最も短いルートのみ、IP ルーティングテーブルにインストールされます。
- Next hop: EBGPのnext-hop属性は、アドバタイジングルータに到達するために使用されるIPアドレスです。EBGP ピアの場合、ネクストホップアドレスは、ピア間の接続の IP アドレスです。IBGP の場合、EBGP のネクストホップアドレスがローカル AS に伝送されます。ただし、ネクストホップが eBGP ピアのピアリングアドレスと同じサブネットにある場合、ネクストホップは変更されません。この動作は、サードパーティのネクストホップと呼ばれます。

  VPN でアドバタイズされたルートを iBGP ピアに再配布する場合は、**next-hop-self** コマンドを使用して、ルートが正しいネクストホップ IP で再配布されるようにします。
- Community: Community属性は、ルーティングの決定(承認、優先順位、再配布など)を適用できる接続先をグループ化する方法、つまりコミュニティを提供します。ルートマップは、Community 属性を設定するために使用されます。事前定義済みのCommunity属性は次のとおりです。
  - no-export: EBGPピアにアドバタイズしません。
  - no-advertise: どのピアにもこのルートをアドバイタイズしません。
  - internet：インターネット コミュニティにこのルートをアドバタイズします。ネットワーク内のすべてのルートがこのコミュニティに属します。

BGP パスの選択

BGPは、異なる送信元から同じルートに対する複数のアドバタイズメントを受信する場合があります。BGP はベストパスとして 1 つのパスだけを選択します。ベストパスを選択すると、BGPは選択したパスをIPルーティングテーブルに格納し、そのネイバーにパスを伝達します。BGP は、次に示す順序で次の条件を使用して、宛先のパスを選択します。

- パスで指定されているネクストホップが到達不能な場合、更新はドロップされます。
- 重みが最大のパスが優先されます。
- 重みが同じ場合、ローカルプリファレンスが最大のパスが優先されます。
- ローカルプリファレンスが同じ場合、このルータで動作している BGP により発信されたパスが優先されます。
- ルートが発信されていない場合、AS_pathが最短のルートが優先されます。
- すべてのパスの AS_path の長さが同じ場合、Origin タイプが最下位のパス（IGP は EGP よりも低く、EGP は Incomplete よりも低い）が優先されます。
- Origin コードが同じ場合、最も小さい MED 属性を持つパスが優先されます。
- パスの MED が同じ場合、内部パスより外部パスが優先されます。

- それでもパスが同じ場合、最も近い IGP ネイバーを経由するパスが優先されます。
- BGP マルチパス （4 ページ） 用のルーティングテーブルに複数のパスをインストールする必要があるか判断します。
- 両方のパスが外部のときは、先に受信したパス(最も古いパス)が優先されます。
- BGPルータIDで指定された、IPアドレスが最も小さいパスが優先されます。
- 発信元 ID またはルータ ID が複数のパスで同じ場合は、最小のクラスタ リスト長を持つパスが優先されます。
- 最も小さいネイバー アドレスから発信されたパスが優先されます。

BGP マルチパス

BGP マルチパスでは、同じ宛先プレフィックスへの複数の等コスト BGP パスの IP ルーティングテーブルへのインストールが許可されます。その場合、宛先プレフィックスへのトラフィックは、インストールされたすべてのパス間で共有されます。

これらのパスは、ロードシェアリング用にベストパスとともにテーブルにインストールされます。BGPマルチパスはベストパスの選択には影響しません。たとえば、ルータではアルゴリズムに従って、ベストパスとしてパスの 1 つが引き続き指定され、そのベストパスが BGP ピアにアドバタイズされます。

マルチパスの候補になるためには、同じ宛先へのパスに、最適パスの特性に等しいこれらの特性が備わっている必要があります。

- 重量
- ローカル プリファレンス
- AS-PATH length
- オリジン コード
- Multi Exit識別子(MED)
- 次のいずれか。
  - ネイバー AS または sub-AS（BGP マルチパス機能が追加される前）
  - AS-PATH（BGP マルチパス機能が追加された後）

一部の BGP マルチパス機能により、マルチパス候補に関する追加要件が加わりました。

- パスは、外部またはコンフェデレーション外部の近接ルータ（eBGP）から学習されます。
- BGP ネクストホップへの IGP メトリックは、最適パスの IGP メトリックと等しくなる必要があります。

内部 BGP（iBGP）マルチパスの候補には次の追加要件があります。

- パスは、内部の近接ルータ（iBGP）から学習されます。

- ルータが不等コスト iBGP マルチパスで設定されない限り、BGP ネクストホップへの IGP メトリックは、最適パスの IGP メトリックと等しくなる必要があります。

BGP は、マルチパス候補から最近受信した最大 *n* 個のパスを IP ルーティングテーブルに挿入します。ここで、*n* は、BGP マルチパスを設定するときに指定した、ルーティングテーブルにインストールするルートの数です。マルチパスがディセーブルになっている場合のデフォルト値は 1 です。

不等コスト ロード バランシングでは、BGP リンク帯域幅も使用できます。

（注） 内部ピアへの転送前に、eBGP マルチパスで選択されたベストパスに対し、同等の next-hop-self が実行されます。

BGP のガイドライン

コンテキスト モードのガイドライン

- シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。
- すべてのコンテキストでサポートされる自律システム（AS）番号は 1 つだけです。

ファイアウォール モードのガイドライン

トランスペアレント ファイアウォール モードはサポートされません。BGP は、ルーテッドモードでのみサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。

その他のガイドライン

- システムは、PPPoE 経由で受信した IP アドレスのルートエントリを CP ルートテーブルに追加しません。BGP は常に CP ルートテーブルを調べて TCP セッションを開始するため、BGP は TCP セッションを形成しません。

  つまり、PPPoE 経由の BGP はサポートされません。

- 管理専用または BVI インターフェイスでは、BGP はサポートされません
- ルートアップデートがリンク上の最小 MTU より大きい場合に、ルートアップデートがドロップされることによる隣接フラップを回避するには、リンクの両側のインターフェイスで同じ MTU を設定する必要があります。
- PATH MTU（PMTU）を使用した BGP は、特に ECMP ルーティングで MTU ディスカバリが失敗した場合に、隣接関係（アジャセンシー）フラップを引き起こす可能性がありま

す。したがって、何らかの理由で MTU ディスカバリが失敗した場合にパケットドロップが発生する可能性があるため、BGP、PMTU、および ECMP の使用時には注意が必要です。

- メンバーユニットの BGP テーブルは、制御ユニットテーブルと同期されません。ルーティングテーブルだけが、制御ユニットのルーティングテーブルと同期されます。

BGP の設定

ここでは、システムで BGP プロセスをイネーブルにして設定する方法について説明します。

手順

ステップ 1 BGP の有効化 （6 ページ）。
ステップ 2 BGP ルーティング プロセスの最適なパスの定義 （8 ページ）。
ステップ 3 ポリシー リストの設定 （9 ページ）。
ステップ 4 AS パス フィルタの設定 （10 ページ）。
ステップ 5 コミュニティ ルールの設定 （11 ページ）。
ステップ 6 IPv4 アドレス ファミリの設定 （12 ページ）。
ステップ 7 IPv6 アドレス ファミリの設定 （27 ページ）。

BGP の有効化

ここでは、BGP の有効化、BGP ルーティング プロセスの確立、一般的な BGP パラメータの設定に必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

autonomous-num の有効値は 1 ～ 4294967295 および 1.0 ～ XX.YY です。

ステップ 2 指定値を超えている AS パス セグメントを含むルートを破棄します。

bgp maxas-limit number

例：

```
ciscoasa(config-router)# bgp maxas-limit 15
```

number 引数には、自律システム セグメントの最大許容数を指定します。有効値は 1 ～ 254 です。

ステップ 3 BGP ネイバーのリセットをログに記録します。

bgp log-neighbor-changes

ステップ 4 BGP で各 BGP セッションの最適な TCP パス MTU を自動検出できるようにします。

bgp transport path-mtu-discovery

ステップ 5 BGP が、ピアに到達するために使用されているリンクがダウンした場合に、ホールドダウン タイマーが期限切れになるのを待たずに、直接隣接するいずれかのピアの外部 BGP セッションを終了できるようにします。

bgp fast-external-fallover

ステップ 6 BGP ルーティング プロセスで、自律システム（AS）番号を着信ルートの AS_path 属性の 1 つ目の AS パス セグメントとしてリストしていない外部 BGP（eBGP）ピアから受信したアップデートを破棄できるようにします。

bgp enforce-first-as

ステップ 7 デフォルトの表示を変更し、BGP 4 バイト自律システム番号の正規表現一致形式を、asplain（10 進数の値）からドット付き表記にします。

bgp asnotation dot

ステップ 8 BGP ネットワーク タイマーを調整します。

timers bgp keepalive holdtime [min-holdtime]

例：

```
ciscoasa(config-router)# timers bgp 80 120
```

- keepalive：ASA がキープアライブ メッセージをピアに送信する頻度（秒）。デフォルト値は 60 秒です。
- holdtime：キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの時間（秒）。デフォルト値は 180 秒です。
- （オプション）min-holdtime：ネイバーからキープアライブ メッセージを受信できない状態が継続して、ネイバーがデッドであると ASA が宣言するまでの時間（秒）。

（注）
ホールドタイムが 20 秒未満の場合、ピアフラッピングの可能性が高くなります。

ステップ 9 BGP グレースフル リスタート機能をイネーブルにします。

bgp graceful-restart [restart-time seconds|stalepath-time seconds][all]

例：

```
ciscoasa(config-router)# bgp graceful-restart restart-time 200
```

- restart-time：リスタートイベントが発生した後、グレースフル リスタート対応ネイバーが通常の動作に戻るまで ASA が待機する最大時間（秒）。デフォルトは 120 秒です。有効な値は 1 ～ 3600 秒です。
- stalepath-time：リスタートしているピアの古いパスを ASA が保持する最大時間（秒）。すべての古いパスは、このタイマーが期限切れになった後に削除されます。デフォルト値は 360 秒です。有効な値は 1 ～ 3600 秒です。

BGP ルーティング プロセスの最適なパスの定義

ここでは、BGP の最適なパスを設定するために必要な手順について説明します。最適なパスの詳細については、BGP パスの選択 （3 ページ）を参照してください。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 デフォルトの Local preference 値を変更します。

bgp default local-preference number

例：

```
ciscoasa(config-router)# bgp default local-preference 500
```

number 引数は、0 ～ 4294967295 の値です。値が大きいほど、優先度が高いことを示します。

デフォルト値は 100 です。

ステップ 3 さまざまな自律システムのネイバーから学習したパス間での Multi-exit discriminator（MED）比較をイネーブルにします。

bgp always-compare-med

ステップ 4 最適なパスの選択プロセス中に外部 BGP（eBGP）ピアから受信した類似ルートを比較し、最適なパスをルータ ID が最も小さいルートに切り替えます。

bgp bestpath compare-routerid

ステップ 5 隣接 AS からアドバタイズされた最適な MED パスを選択します。

bgp deterministic-med

ステップ 6 MED 属性が欠落しているパスを最も優先度の低いパスとして設定します。

bgp bestpath med missing-as-worst

ポリシー リストの設定

ルート マップ内でポリシー リストが参照されると、ポリシー リスト内の match 文すべてが評価され、処理されます。1 つのルート マップに 2 つ以上のポリシー リストを設定できる。ポリシー リストは、同じルート マップ内にあるがポリシー リストの外で設定されている他の既存の match および set 文とも共存できます。ここでは、ポリシー リストを設定するために必要な手順について説明します。

手順

ステップ 1 BGP ポリシーリストを作成します。

policy-list *policy_list_name* {**permit** | **deny**}

permit キーワードを指定すると、条件が一致した場合にアクセスが許可されます。

deny キーワードを指定すると、条件が一致した場合にアクセスが拒否されます。

例：

```
ciscoasa(config)# policy-list Example-policy-list1 permit
```

ステップ 2 指定したいずれかのインターフェイスの外部にネクスト ホップを持つルートを配布します。

match interface [*interface_name* [*interface_name*] […]]

例：

```
ciscoasa(config-policy-list)# match interface outside
```

ステップ 3 宛先アドレス、ネクスト ホップ ルータ アドレス、ルータ/アクセス サーバ ソースのいずれかまたはすべてを一致させてルートを再配布します。

match ip {**address** | **next-hop** | **route-source**}

ステップ 4 BGP 自律システム パスを一致させます。

match as-path

ステップ 5 BGP コミュニティを一致させます。

match community {*community-list_name* | **exact-match**}

- *community-list_name* ：1 つ以上のコミュニティ リスト。
- **exact-match**：完全一致が必要であることを示します。指定されたすべてのコミュニティのみが存在する必要があります。

例：

```
ciscoasa(config-policy-list)# match community ExampleCommunity1
```

ステップ 6 指定したメトリックを持つルートを再配布します。

match metric *metric* [*metric* […]]

ステップ 7 指定されたタグと一致するルーティング テーブルのルートを再配布します。

match tag *tag* [*tag* […]]

AS パス フィルタの設定

AS パス フィルタで、アクセス リストを使用してルーティング アップデート メッセージをフィルタリングし、アップデート メッセージ内の個々のプレフィックスを確認できます。アップデート メッセージ内のプレフィックスがフィルタ基準に一致すると、フィルタ エントリで実行するように設定されているアクションに応じて、個々のプレフィックスは除外されるか受け入れられます。ここでは、AS パス フィルタを設定するために必要な手順について説明します。

（注） AS パス アクセス リストは、通常のファイアウォール ACL とは異なります。

手順

グローバル コンフィギュレーション モードで正規表現を使用して自律システム パス フィルタを設定します。

as-path access-list acl-number {permit|deny} regexp

例：

```
ciscoasa(config)# as-path access-list 35 permit testaspath
```

- *acl-number*：AS パス アクセスリストの番号。有効な値は、1 ～ 500 です。
- regexp：AS パス フィルタを定義する正規表現。自律システム番号は 1 ～ 65535 の範囲で表します。

コミュニティ ルールの設定

コミュニティは、共通するいくつかの属性を共有する宛先のグループです。コミュニティ リストを使用すると、ルート マップの match 句で使用されるコミュニティ グループを作成できます。アクセス リストと同様に、一連のコミュニティ リストを作成できます。ステートメントは一致が見つかるまでチェックされ、1 つのステートメントが満たされると、テストは終了します。ここでは、コミュニティ ルールを設定するために必要な手順について説明します。

手順

BGP コミュニティ リストを作成または設定して、そのリストへのアクセスを制御します。

community-list {standard| community list-name {deny|permit} [community-number] [AA:NN] [internet] [no-advertise][no-export]}| {expanded|expanded list-name {deny| permit}regexp}

例：

```
ciscoasa(config)# community-list standard excomm1 permit 100 internet no-advertise
no-export
```

- standard：1 ～ 99 の数字を使用して標準のコミュニティ リストを設定し、1 つ以上の許可または拒否コミュニティ グループを識別します。
- （オプション）community-number：1 ～ 4294967200 の 32 ビットの数値で表わされたコミュニティ。1 つのコミュニティ、または複数のコミュニティをそれぞれスペースで区切って入力できます。
- AA:NN：4 バイトの新コミュニティ形式で入力された自律システム番号およびネットワーク番号。この値は、コロンで区切られた 2 バイトの数 2 つで設定されます。2 バイトの数ごとに 1 ～ 65535 の数を入力できます。1 つのコミュニティ、または複数のコミュニティをそれぞれスペースで区切って入力できます。
- （オプション）internet：インターネット コミュニティを指定します。このコミュニティのルートは、すべてのピア（内部および外部）にアドバタイズされます。
- （オプション）no-advertise：no-advertise コミュニティを指定します。このコミュニティのあるルートはピア（内部または外部）にはアドバタイズされません。

- （オプション）no-export：no-export コミュニティを指定します。このコミュニティのあるルートは、同じ自律システム内のピアへのみ、または連合内の他のサブ自律システムへのみアドバタイズされます。これらのルートは外部ピアにはアドバタイズされません。
- （オプション）expanded：100 ～ 500 の拡張コミュニティ リスト番号を設定し、1 つ以上の許可または拒否コミュニティ グループを識別します。
- regexp：AS パス フィルタを定義する正規表現。自律システム番号は 1 ～ 65535 の範囲で表します。

（注）
正規表現を使用できるのは拡張コミュニティ リストだけです。

IPv4 アドレス ファミリの設定

BGP の IPv4 設定は、BGP 設定セットアップ内の IPv4 ファミリ オプションから指定できます。IPv4 ファミリ セクションには、一般設定、集約アドレスの設定、フィルタリング設定、ネイバー 設定のサブセクションが含まれます。これらの各サブセクションを使用して、IPv4 ファミリに固有のパラメータをカスタマイズすることができます。

IPv4 ファミリの一般設定

ここでは、一般的な IPv4 の設定に必要な手順を説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ルータをルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 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、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [unicast]

キーワード unicast では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3 （オプション）ローカル BGP ルーティング プロセスの固定ルータ ID を設定します。

bgp router-id A.B.C.D

例：

```
ciscoasa(config-router-af)# bgp router-id 10.86.118.3
```

引数 A.B.C.D には、ルータ ID を IP アドレス形式で指定します。ルータ ID を指定しない場合、自動的に割り当てられます。

ステップ 4 （オプション）個別インターフェイス（L3）モードで IP アドレスのクラスタ プールを設定します。

bgp router-id cluster-pool

例：

```
ciscoasa(config-router-af)# bgp router-id cp
```

（注）
L3 クラスタでは、BGP ネイバーをクラスタ プールの IP アドレスの 1 つとして定義できません。

ステップ 5 BGP ルートのアドミニストレーティブ ディスタンスを設定します。

distance bgp external-distance internal-distance local-distance

例：

```
ciscoasa(config-router-af)# distance bgp 80 180 180
```

- external-distance：外部 BGP ルートのアドミニストレーティブ ディスタンス。外部自律システムから学習されたルートは、外部ルートです。この引数の値の範囲は 1 ～ 255 です。
- internal-distance：内部 BGP ルートのアドミニストレーティブ ディスタンス。ローカル自律システムのピアから学習されたルートは、内部ルートです。この引数の値の範囲は 1 ～ 255 です。
- local-distance：ローカル BGP ルートのアドミニストレーティブ ディスタンス。ローカル ルートは、別のプロセスから再配布されているルータまたはネットワークの、多くの場合バック ドアとして、ネットワーク ルータ コンフィギュレーション コマンドによりリストされるネットワークです。この引数の値の範囲は 1 ～ 255 です。

ステップ 6 BGP で学習されたルートを使用して IP ルーティング テーブルが更新されたときに、メトリックおよびタグ値を変更します。

table-map {WORD|route-map_name}

例：

```
ciscoasa(config-router-af)# table-map example1
```

引数 route-map_name には route-map コマンドのルート マップ名を指定します。

ステップ 7 BGP ルーティング プロセスを設定し、デフォルト ルート（ネットワーク 0.0.0.0）を配布します。

default-information originate

ステップ 8 ネットワーク レベルのルートへのサブネット ルートの自動集約を設定します。

auto-summary

ステップ 9 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のアドバタイズメントを抑制します。

bgp suppress-inactive

ステップ 10 BGP と Interior Gateway Protocol（IGP）システム間で同期します。

同期

ステップ 11 OSPF などの IGP への iBGP の再配布を設定します。

bgp redistribute-internal

ステップ 12 ネクスト ホップの検証用に BGP ルータのスキャン間隔を設定します。

bgp scan-time scanner-interval

例：

```
ciscoasa(config-router-af)# bgp scan-time 15
```

引数 scanner-interval には BGP ルーティング情報のスキャン間隔を指定します。有効な値は 5 ～ 60 秒です。デフォルトは 60 秒です。

ステップ 13 BGP ネクスト ホップ アドレス トラッキングを設定します。

bgp nexthop trigger {delay seconds|enable}

例：

```
ciscoasa(config-router-af)# bgp nexthop trigger delay 15
```

- trigger：BGP ネクスト ホップ アドレス トレッキングの使用を指定します。ネクスト ホップ トラッキングの遅延を変更するには、このキーワードを delay キーワードとともに使用します。ネクスト ホップ アドレス トラッキングを有効にするには、このキーワードを enable キーワードとともに使用します。
- delay：ルーティング テーブルにインストールされている更新済みのネクスト ホップ ルートのチェック間の遅延間隔を変更します。
- seconds：遅延を秒数で指定します。指定できる値の範囲は 0 ～ 100 です。デフォルトは 5 です。
- enable：BGP ネクスト ホップ アドレス トラッキングをすぐに有効化します。

ステップ 14 ルーティング テーブルにインストールできる並列 iBGP ルートの最大数を制御します。

maximum-paths {number_of_paths|ibgp number_of_paths}

例：

```
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

（注）
ibgp キーワードを使用しない場合、number_of_paths 引数は、並列 EBGP ルートの最大数を制御します。

number_of_paths 引数には、ルーティング テーブルにインストールするルートの数を指定します。有効な値は、1 ～ 8 です。

IPv4 ファミリ集約アドレスの設定

ここでは、特定のルートの 1 つのルートへの集約を定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 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、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [unicast]

キーワード unicast では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3 BGP データベースで集約エントリを作成します。

aggregate-address address mask [as-set][summary-only][suppress-map map-name][advertise-map map-name][attribute-map map-name]

例：

```
ciscoasa(config-router-af) aggregate-address 10.86.118.0 255.255.255.0 as-set summary-only
 suppress-map example1 advertise-map example1 attribute-map example1
```

- address：集約アドレス。
- mask：集約マスク。
- map-name：ルート マップ。
- （オプション）as-set：自律システムの設定パス情報を生成します。
- （オプション）summary-only：アップデートから固有性の強いルートをすべてフィルタリングします。
- （オプション）Suppress-map map-name：抑制するルートを選択するために使用するルートマップの名前を指定します。
- （オプション）Advertise-map map-name：AS_SET 発信コミュニティを作成するためのルートを選択するために使用するルート マップの名前を指定します。
- （オプション）Attribute-map map-name：集約ルートの属性を設定するために使用するルート マップの名前を指定します。

IPv4 ファミリのフィルタリング設定

ここでは、着信 BGP アップデートで受信したルートまたはネットワークをフィルタリングするために必要な手順について説明します。

手順

ステップ 1 BGPP ルーティング プロセスを有効にし、ルータ コンフィギュレーション モードを開始します。

router bgp *autonomous-num*

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 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、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [**unicast**]

キーワード unicast では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3 着信 BGP アップデートで受信したルータまたはネットワーク、あるいは発信 BGP アップデートでアドバタイズされたルータまたはネットワークをフィルタリングします。

distribute-list *acl-number* {**in** | **out**} [*protocol process-number* | **connected** | **static**]

引数 *acl-number* には、IP アクセス リストの番号を指定します。アクセス リストは、ルーティング アップデートで受信されるネットワークと抑制されるネットワークを定義します。

キーワード **in** はフィルタを着信 BGP アップデートに適用する必要があることを指定し、**out** はフィルタを発信 BGP アップデートに適用する必要があることを指定します。

アウトバウンド フィルタの場合、必要に応じて、配布リストに適用するプロトコル（**bgp**、**eigrp**、**ospf**、または **rip**）をプロセス番号付き（RIP を除く）で指定できます。ピアおよびネットワークが **connected** または **static** ルート経由で学習されたかどうかでフィルタすることもできます。

例：

```
ciscoasa(config-router-af)# distribute-list ExampleAcl in bgp 2
```

IPv4 ファミリの BGP ネイバーの設定

ここでは、BGP ネイバーおよびネイバー設定を定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ルータをルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 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、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [unicast]

キーワード unicast では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3 エントリを BGP ネイバー テーブルに追加します。

neighbor ip-address remote-as autonomous-number

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 remote-as 3
```

ステップ 4 （オプション）ネイバーまたはピア グループをディセーブルにします。

neighbor ip-address shutdown

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 shutdown 3
```

ステップ 5 BGP ネイバーと情報を交換します。

neighbor ip-address activate

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 activate
```

ステップ 6 BGP ネイバーの Border Gateway Protocol（BGP）グレースフル リスタート機能をイネーブルまたはディセーブルにします。

neighbor ip-address ha-mode graceful-restart [disable]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ha-mode graceful-restart
```

（オプション）disable キーワードを指定すると、ネイバーの BGP グレースフル リスタート機能が無効化されます。

ステップ 7 アクセス リストで指定された BGP ネイバー情報を配布します。

neighbor {ip-address} distribute-list {access-list-name}{in|out}

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 distribute-list ExampleAcl in
```

- access-list-number：標準アクセス リストまたは拡張アクセス リストの番号。標準アクセス リストの番号の範囲は 1 ～ 99 です。拡張アクセス リストの番号の範囲は 100 ～ 199 です。
- expanded-list-number：拡張アクセス リストの番号。拡張アクセス リストの範囲は 1300 ～ 2699 です。
- access-list-name：標準アクセス リストまたは拡張アクセス リストの名前。
- prefix-list-name：BGP プレフィックス リストの名前。
- in：アクセス リストはそのネイバーへの着信アドバタイズメントに適用されます。
- out：アクセス リストはそのネイバーへの発信アドバタイズメントに適用されます。

ステップ 8 着信ルートまたは発信ルートにルート マップを適用します。

neighbor {ip-address} route-map map-name {in|out}

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 route-map example1 in
```

キーワード in を指定すると、ルート マップは着信ルートに適用されます。

キーワード out を指定すると、ルート マップは発信ルートに適用されます。

ステップ 9 プレフィックス リストで指定された BGP ネイバー情報を配布します。

neighbor {ip-address} prefix-list prefix-list-name {in|out}

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 prefix-list NewPrefixList in
```

キーワード in は、プレフィックス リストがそのネイバーからの着信アドバタイズメントに適用されることを意味します。

キーワード out は、プレフィックス リストがそのネイバーへの発信アドバタイズメントに適用されることを意味します。

ステップ 10 フィルタ リストを設定します。

neighbor {ip-address} filter-list access-list-number {in|out}

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 filter-list 5 in
```

- access-list-name：自律システム パスのアクセス リストの番号を指定します。ip as-path access-list コマンドを使用して、このアクセス リストを定義します。
- in：アクセス リストはそのネイバーからの着信アドバタイズメントに適用されます。
- out：アクセス リストはそのネイバーへの発信アドバタイズメントに適用されます。

ステップ 11 ネイバーから受信できるプレフィックスの数を制御します。

neighbor {ip-address} maximum-prefix maximum [threshold][restart restart interval][warning-only]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 maximum-prefix 7 75 restart 12
```

- maximum：このネイバーからの許可される最大プレフィックス数。
- （オプション）threshold：最大数の何パーセントになったらルータが警告メッセージの生成を開始するかを指定する整数。指定できる範囲は 1 ～ 100 です。デフォルト値は 75（%）です。
- （オプション）restart interval：BGP ネイバーが再起動するまでの時間を指定する整数値（分）。

- （オプション）warning-only：プレフィックスの最大数を超えた場合に、ピアリングを終了する代わりに、ルータでログ メッセージを生成できます。

ステップ 12 BGP スピーカー（ローカル ルータ）にネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。

neighbor {ip-address} default-originate [route-map map-name]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 default-originate route-map example1
```

引数 map-name は、ルートマップの名前です。ルート マップでは、条件に応じてルート 0.0.0.0 を挿入できます。

ステップ 13 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。

neighbor {ip-address} advertisement-interval seconds

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 advertisement-interval 15
```

引数 seconds は時間（秒）です。0 ～ 600 の範囲の値を指定できます。

ステップ 14 設定されているルート マップと一致する BGP テーブル内のルートをアドバタイズします。

neighbor {ip-address} advertise-map map-name {exist-map map-name |non-exist-map map-name}[check-all-paths]

例：

```
ciscoasa(config-router-af)# neighbor 10.2.1.1 advertise-map MAP1 exist-map MAP2
```

- advertise-map map name：exist-map または non-exist-map の条件に一致した場合にアドバタイズされるルート マップの名前。
- exist-map map name：advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較される exist-map の名前。
- non-exist-map map name：advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較される non-exist-map の名前。
- （オプション）check all paths：BGP テーブル内のプレフィックスを持つ exist-map によるすべてのパスのチェックを有効化します。

ステップ 15 プライベート自律システム番号を発信ルーティング アップデートから削除します。

neighbor {ip-address} remove-private-as

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 remove-private-as
```

ステップ 16 特定の BGP ピアまたは BGP ピア グループのタイマーを設定します。

neighbor {ip-address} timers keepalive holdtime min holdtime

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 timers 15 20 12
```

- keepalive：ASA がキープアライブ メッセージをピアに送信する頻度（秒）。デフォルトは 60 秒です。有効値は、0 ～ 65535 です。
- holdtime：キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの時間（秒）。デフォルト値は 180 秒です。
- min holdtime：キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの最小時間（秒）。

（注）
ホールドタイムが 20 秒未満の場合、ピアフラッピングの可能性が高くなります。

ステップ 17 2 つの BGP ピア間の TCP 接続で Message Digest 5（MD5）認証をイネーブルにします。

neighbor {ip-address} password string

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 password test
```

引数 string は大文字と小文字を区別するパスワードで、service password-encryption コマンドが有効化されている場合は最大 25 文字、service password-encryption コマンドが有効化されていない場合は最大 81 文字を指定できます。この文字列には、スペースも含め、あらゆる英数字を使用できます。

（注）
パスワードの最初の文字を数字にする場合、数字の直後にスペースを入れないでください。つまり、数字-スペース-任意の文字の形式でパスワードを指定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。

ステップ 18 BGP ネイバーに送信する Community 属性を指定します。

neighbor {ip-address} send-community

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 send-community
```

ステップ 19 ルータを BGP スピーキング ネイバーまたはピア グループのネクスト ホップとして設定します。

neighbor {ip-address}next-hop-self

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 next-hop-self
```

ステップ 20 直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。

neighbor {ip-address} ebgp-multihop [ttl]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ebgp-multihop 5
```

引数 ttl には、1 ～ 255 ホップの範囲の存続可能時間を指定します。

ステップ 21 ループバック インターフェイスを使用するシングル ホップ ピアと eBGP ピアリング セッションを確立するための接続確認をディセーブルにします。

neighbor {ip-address} disable-connected-check

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 disable-connected-check
```

ステップ 22 BGP ピアリング セッションを保護し、2 つの外部 BGP （eBGP）ピアを区切るホップの最大数を設定します。

neighbor ip-addressttl-security hops hop-count

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ttl-security hops 15
```

引数 hop-count は、eBGP ピアを区切るホップの数です。TTL 値は、設定された hop-count 引数に基づいてルータにより計算されます。有効値は 1 ～ 254 です。

ステップ 23 ネイバー接続に重みを割り当てます。

neighbor {ip-address} weight number

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 weight 30
```

引数 number は、ネイバー接続に割り当てる重みです。有効値は、0 ～ 65535 です。

ステップ 24 特定の BGP バージョンだけを受け入れるように ASA を設定します。

neighbor {ip-address} version number

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 version 4
```

引数 number には、BGP バージョン番号を指定します。バージョンを 2 に設定すると、指定されたネイバーとの間でバージョン 2 だけが使用されます。デフォルトでは、バージョン 4 が使用され、要求された場合は動的にネゴシエートしてバージョン 2 に下がります。

ステップ 25 BGP セッションの TCP トランスポート セッション オプションをイネーブルにします。

neighbor {ip-address} transport {connection-mode{active|passive}| path-mtu-discovery[disable]}

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 transport path-mtu-discovery
```

- connection-mode：接続のタイプ（active または passive）。
- path-mtu-discovery：TCP トランスポート パスの最大伝送ユニット（MTU）ディスカバリを有効にします。TCP パス MTU ディスカバリは、デフォルトではイネーブルです。
- （オプション）disable：TCP パス MTU ディスカバリを無効にします。

ステップ 26 External Border Gateway Protocol（eBGP）ネイバーから受信したルートの AS_path 属性をカスタマイズします。

neighbor {ip-address} local-as [autonomous-system-number[no-prepend]]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 local-as 5 no-prepend replace-as
```

- （オプション）autonomous-system-number：AS_path 属性の前に追加する自律システムの番号。この引数の値の範囲は、1 ～ 4294967295 または 1.0 ～ XX.YY の有効な任意の自律システム番号です。
- （オプション）no-prepend：eBGP ネイバーから受信したルートの前にローカル自律システム番号を追加しません。

ステップ 27 BGP ネイバーシップの送信元としてインターフェイスを更新する場合：

neighbor *ip_address* **update-source** *interface_name*

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 update-source loop1
```

引数 *interface_name* は、BGP ネイバーが BGP ルーティングの送信元として使用するインターフェイスの名前です。

（注）
BGP ネイバーシップの送信元としてループバック インターフェイスを更新すると、ループバック インターフェイスの IP アドレスがネットワーク全体にアドバタイズされます。ループバック インターフェイスは eBGP ピアとして機能し、ルーティングに参加します。ループバック

インターフェイスは有効にすると安定し、管理上のシャットダウンまで使用可能な状態になるため、ループバック インターフェイスの IP アドレスで常に ASA に到達できます。

IPv4 ネットワークの設定

ここでは、BGP ルーティング プロセスによってアドバタイズされるネットワークを定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 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、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [unicast]

キーワード unicast では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3 BGP ルーティング プロセスによってアドバタイズされるネットワークを指定します。

network {network-number [mask network-mask]}[route-map map-tag]

例：

```
ciscoasa(config-router-af)# network 10.86.118.13 mask 255.255.255.255 route-map example1
```

（注）
ネットワークプレフィックスをアドバタイズするには、デバイスへのルートがルーティングテーブルに存在する必要があります。

- network-number：BGP がアドバタイズするネットワーク。
- （オプション）network-mask：マスク アドレスを持つネットワーク マスクまたはサブネットワーク マスク。

- （オプション）map-tag：設定されているルートマップのID。ルートマップは、アドバタイズされるネットワークをフィルタリングするために調べる必要があります。この値を指定しない場合、すべてのネットワークがアドバタイズされます。

IPv4 再配布の設定

ここでは、別のルーティング ドメインから BGP にルートを再配布する条件を定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 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、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [unicast]

例：

```
ciscoasa(config-router)# address-family ipv4[unicast]
```

キーワード unicast では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3 別のルーティング ドメインから BGP 自律システムにルートを再配布します。

redistribute protocol [process-id] [metric] [route-map [map-tag]]

例：

```
ciscoasa(config-router-af)# redistribute ospf 2 route-map example1 match external
```

- protocol：ルートの再配布元となるソース プロトコル。Connected、EIGRP、OSPF、RIP または Static のいずれかを指定できます。
- （オプション）process-id：特定のルーティング プロセスの名前。
- （オプション）metric：再配布されるルートのメトリック。
- （オプション）map-tag：設定されているルート マップの ID。

（注）
ルートマップは、再配布されるネットワークをフィルタリングするために調べる必要があります。この値を指定しない場合、すべてのネットワークが再配布されます。

IPv4 ルート注入の設定

ここでは、条件に応じて BGP ルーティング テーブルに注入されるルートを定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 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、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [unicast]

例：

```
ciscoasa(config-router)# address-family ipv4[unicast]
```

キーワード unicast では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3 BGP ルーティング テーブルに固有性の強いルートを注入するよう条件付きルート注入を設定します。

bgp inject-map inject-map exist-map exist-map [copy-attributes]

例：

```
ciscoasa(config-router-af)# bgp inject-map example1 exist-map example2 copy-attributes
```

- inject-map：ローカル BGP ルーティング テーブルに注入するプレフィックスを指定するルート マップの名前。
- exist-map：BGP スピーカーが追跡するプレフィックスを含むルート マップの名前。

- （オプション）copy-attributes：集約ルートの属性を継承するよう注入されたルートを設定します。

IPv6 アドレス ファミリの設定

BGP の IPv6 設定は、BGP 設定セットアップ内の IPv6 ファミリ オプションから指定できます。IPv6 ファミリ セクションには、一般設定、集約アドレスの設定、ネイバー設定のサブセクションが含まれます。これらの各サブセクションを使用して、IPv6 ファミリに固有のパラメータをカスタマイズすることができます。

ここでは、BGP IPv6 ファミリの設定をカスタマイズする方法について説明します。

IPv6 ファミリの一般設定

ここでは、一般的な IPv6 の設定に必要な手順を説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ルータをルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 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、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv6 [unicast]

ステップ 3 BGP ルートのアドミニストレーティブ ディスタンスを設定します。

distance bgp external-distance internal-distance local-distance

例：

```
ciscoasa(config-router-af)# distance bgp 80 180 180
```

- external-distance：外部 BGP ルートのアドミニストレーティブ ディスタンス。外部自律システムから学習されたルートは、外部ルートです。この引数の値の範囲は 1 ～ 255 です。
- internal-distance：内部 BGP ルートのアドミニストレーティブ ディスタンス。ローカル自律システムのピアから学習されたルートは、内部ルートです。この引数の値の範囲は 1 ～ 255 です。

- local-distance：ローカル BGP ルートのアドミニストレーティブ ディスタンス。ローカル ルートは、別のプロセスから再配布されているルータまたはネットワークの、多くの場合バック ドアとして、ネットワーク ルータ コンフィギュレーション コマンドによりリストされるネットワークです。この引数の値の範囲は 1 ～ 255 です。

ステップ 4 （オプション）デフォルト ルート（ネットワーク 0.0.0.0）を配布するように BGP ルーティング プロセスを設定します。

default-information originate

ステップ 5 （オプション）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のアドバタイズメントを抑制します。

bgp suppress-inactive

ステップ 6 BGP と Interior Gateway Protocol（IGP）システム間で同期します。

同期

ステップ 7 OSPF などの IGP への iBGP の再配布を設定します。

bgp redistribute-internal

ステップ 8 ネクスト ホップの検証用に BGP ルータのスキャン間隔を設定します。

bgp scan-time scanner-interval

例：

```
ciscoasa(config-router-af)# bgp scan-time 15
```

scanner-interval 引数の有効な値は 5 ～ 60 秒です。デフォルトは 60 秒です。

ステップ 9 ルーティング テーブルにインストールできる並列 iBGP ルートの最大数を制御します。

maximum-paths {number_of_paths|ibgp number_of_paths}

例：

```
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

number_of_paths 引数の有効な値は 1 ～ 8 です。

ibgp キーワードを使用しない場合、number_of_paths 引数は、並列 EBGP ルートの最大数を制御します。

IPv6 ファミリ集約アドレスの設定

ここでは、特定のルートの 1 つのルートへの集約を定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 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、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv6 unicast

ステップ 3 BGP データベースで集約エントリを作成します。

aggregate-address ipv6-address/cidr [as-set][summary-only][suppress-map map-name][advertise-map ipv6-map-name][attribute-map map-name]

例：

```
ciscoasa(config-router-af) aggregate-address 2000::1/8 summary-only
```

- address：集約 IPv6 アドレス。
- （オプション）as-set：自律システムの設定パス情報を生成します。
- （オプション）summary-only：アップデートから固有性の強いルートをすべてフィルタリングします。
- （オプション）suppress-map map-name：抑制するルートを選択するために使用するルートマップの名前を指定します。
- （オプション）advertise-map map-name：AS_SET 発信コミュニティを作成するためのルートを選択するために使用するルート マップの名前を指定します。
- （オプション）attribute-map map-name：集約ルートの属性を設定するために使用するルート マップの名前を指定します。

ステップ 4 BGP ルートが集約される間隔を設定します。

bgp aggregate-timer seconds

例：

```
ciscoasa(config-router-af)bgp aggregate-timer 20
```

IPv6 ファミリの BGP ネイバーの設定

ここでは、BGP ネイバーおよびネイバー設定を定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ルータをルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 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、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv6 [unicast]

ステップ 3 エントリを BGP ネイバー テーブルに追加します。

neighbor ipv6-address remote-as autonomous-number

例：

```
ciscoasa(config-router-af)# neighbor 2000::1/8 remote-as 3
```

引数 ipv6-address には、指定したネットワークに到達するために使用できるネクスト ホップの IPv6 アドレスを指定します。ネクスト ホップの IPv6 アドレスは直接接続しないようにする必要があります。直接接続されたネクスト ホップの IPv6 アドレスを検出するために再帰が実行されるためです。インターフェイス タイプおよびインターフェイス番号を指定すると、パケットの出力先のネクスト ホップの IPv6 アドレスを指定できます（オプション）。リンクローカルアドレスをネクストホップとして使用する場合は、インターフェイス タイプおよびインターフェイス番号を指定する必要があります（また、リンクローカル ネクスト ホップが隣接デバイスである必要があります）。

（注）
この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。

ステップ 4 （オプション）ネイバーまたはピア グループをディセーブルにします。

neighbor ipv6-address shutdown

例：

```
ciscoasa(config-router-af)# neighbor 2000::1/8 shutdown 3
```

ステップ 5 BGP ネイバーと情報を交換します。

neighbor ipv6-address activate

例：

```
ciscoasa(config-router-af)# neighbor 2000::1/8 activate
```

ステップ 6 BGP ネイバーの Border Gateway Protocol（BGP）グレースフル リスタート機能をイネーブルまたはディセーブルにします。

neighbor {ip-address} ha-mode graceful-restart [disable]

例：

```
ciscoasa(config-router-af)# neighbor 2000::1/8 ha-mode graceful-restart
```

（オプション）disable キーワードを指定すると、ネイバーの BGP グレースフル リスタート機能が無効化されます。

ステップ 7 着信ルートまたは発信ルートにルート マップを適用します。

neighbor {ipv6-address} route-map map-name {in|out}

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 route-map example1 in
```

キーワード in を指定すると、ルート マップは着信ルートに適用されます。

キーワード out を指定すると、ルート マップは発信ルートに適用されます。

ステップ 8 プレフィックス リストで指定された BGP ネイバー情報を配布します。

neighbor {ipv6-address} prefix-list prefix-list-name {in|out}

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 prefix-list NewPrefixList in
```

キーワード in は、プレフィックス リストがそのネイバーからの着信アドバタイズメントに適用されることを意味します。

キーワード out は、プレフィックス リストがそのネイバーへの発信アドバタイズメントに適用されることを意味します。

ステップ 9 フィルタ リストを設定します。

neighbor {ipv6-address} filter-list access-list-name {in|out}

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 filter-list 5 in
```

- access-list-name：自律システム パスのアクセス リストの番号を指定します。ip as-path access-list コマンドを使用して、このアクセス リストを定義します。
- in：アクセス リストはそのネイバーからの着信アドバタイズメントに適用されます。
- out：アクセス リストはそのネイバーへの発信アドバタイズメントに適用されます。

ステップ 10 ネイバーから受信できるプレフィックスの数を制御します。

neighbor {ipv6-address} maximum-prefix maximum [threshold][restart restart interval][warning-only]

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 maximum-prefix 7 75 restart 12
```

- maximum：このネイバーからの許可される最大プレフィックス数。
- （オプション）threshold：最大数の何パーセントになったらルータが警告メッセージの生成を開始するかを指定する整数。指定できる範囲は1～100です。デフォルト値は75（%）です。
- （オプション）restart interval：BGP ネイバーが再起動するまでの時間を指定する整数値（分）。
- （オプション）warning-only：プレフィックスの最大数を超えた場合に、ピアリングを終了する代わりに、ルータでログ メッセージを生成できます。

ステップ 11 BGP スピーカー（ローカル ルータ）にネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。

neighbor {ipv6-address} default-originate [route-map map-name]

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 default-originate route-map example1
```

引数 map-name はルート マップの名前です。ルート マップにより、ルート 0.0.0.0 が条件に応じて注入されます。

ステップ 12 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。

neighbor {ipv6-address} advertisement-interval seconds

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 advertisement-interval 15
```

引数 seconds は時間（秒）です。0 ～ 600 の範囲の値を指定できます。

ステップ 13 プライベート自律システム番号を発信ルーティング アップデートから削除します。

neighbor {ipv6-address} remove-private-as

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 remove-private-as
```

ステップ 14 設定されているルート マップと一致する BGP テーブル内のルートをアドバタイズします。

neighbor {ipv6-address} advertise-map map-name {exist-map map-name |non-exist-map map-name}[check-all-paths]

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 advertise-map MAP1 exist-map MAP2
```

- advertise-map map name：exist-map または non-exist-map の条件に一致した場合にアドバタイズされるルート マップの名前。
- exist-map map name：advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較される exist-map の名前。
- non-exist-map map name：advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較される non-exist-map の名前。
- （オプション）check all paths：BGP テーブル内のプレフィックスを持つ exist-map によるすべてのパスのチェックを有効化します。

ステップ 15 特定の BGP ピアまたは BGP ピア グループのタイマーを設定します。

neighbor {ipv6-address} timers keepalive holdtime min holdtime

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 timers 15 20 12
```

- keepalive：ASA がキープアライブ メッセージをピアに送信する頻度（秒）。デフォルトは 60 秒です。有効値は、0 ～ 65535 です。
- holdtime：キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの時間（秒）。デフォルト値は 180 秒です。
- min holdtime：キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの最小時間（秒）。

  （注）
  ホールドタイムが 20 秒未満の場合、ピアフラッピングの可能性が高くなります。

ステップ 16 2 つの BGP ピア間の TCP 接続で Message Digest 5（MD5）認証をイネーブルにします。

neighbor {ipv6-address} password string

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 password test
```

引数 string は大文字と小文字を区別するパスワードで、service password-encryption コマンドが有効化されている場合は最大25 文字、service password-encryption コマンドが有効化されていない場合は最大 81 文字を指定できます。この文字列には、スペースも含め、あらゆる英数字を使用できます。

（注）
パスワードの最初の文字を数字にする場合、数字の直後にスペースを入れないでください。つまり、数字-スペース-任意の文字の形式でパスワードを指定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。

ステップ 17 BGP ネイバーに送信する Community 属性を指定します。

neighbor {ipv6-address} send-community [standard]

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 send-community
```

（オプション）standard キーワード：標準コミュニティのみ送信されます。

ステップ 18 ルータを BGP スピーキング ネイバーまたはピア グループのネクスト ホップとして設定します。

neighbor {ipv6-address}next-hop-self

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 next-hop-self
```

ステップ 19 直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。

neighbor {ipv6-address} ebgp-multihop [ttl]

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 ebgp-multihop 5
```

引数 ttl には、1 ～ 255 ホップの範囲の存続可能時間を指定します。

ステップ 20 ループバック インターフェイスを使用するシングル ホップ ピアと eBGP ピアリング セッションを確立するための接続確認をディセーブルにします。

neighbor {ipv6-address} disable-connected-check

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 disable-connected-check
```

ステップ 21 BGP ピアリング セッションを保護し、2 つの外部 BGP （eBGP）ピアを区切るホップの最大数を設定します。

neighbor {ipv6-address} ttl-security hops hop-count

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ttl-security hops 15
```

引数 hop-count は、eBGP ピアを区切るホップの数です。TTL 値は、設定された hop-count 引数に基づいてルータにより計算されます。有効値は 1 ～ 254 です。

ステップ 22 ネイバー接続に重みを割り当てます。

neighbor {ipv6-address} weight number

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 weight 30
```

引数 number は、ネイバー接続に割り当てる重みです。有効値は、0 ～ 65535 です。

ステップ 23 特定の BGP バージョンだけを受け入れるように ASA を設定します。

neighbor {ipv6-address} version number

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 version 4
```

引数 number には、BGP バージョン番号を指定します。デフォルトはバージョン 4 です。現在は、BGP バージョン 4 のみがサポートされます。

ステップ 24 BGP セッションの TCP トランスポート セッション オプションをイネーブルにします。

neighbor {ipv6-address} transport {connection-mode{active|passive}| path-mtu-discovery[disable]}

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 transport connection-mode active
```

- connection-mode：接続のタイプ（active または passive）。
- path-mtu-discovery：TCP トランスポート パスの最大伝送ユニット（MTU）ディスカバリを有効にします。TCP パス MTU ディスカバリは、デフォルトではイネーブルです。
- （オプション）disable：TCP パス MTU ディスカバリを無効にします。

ステップ 25 External Border Gateway Protocol（eBGP）ネイバーから受信したルートの AS_path 属性をカスタマイズします。

neighbor {ipv6-address} local-as [autonomous-system-number[no-prepend]]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 local-as 5 no-prepend replace-as
```

- （オプション）autonomous-system-number：AS_path 属性の前に追加する自律システムの番号。この引数の値の範囲は、1 ～ 4294967295 または 1.0 ～ XX.YY の有効な任意の自律システム番号です。
- （オプション）no-prepend：eBGP ネイバーから受信したルートの前にローカル自律システム番号を追加しません。

注意
BGP は、ネットワーク到着可能性情報を維持し、ルーティング ループを防ぐために、ルートが通過する各 BGP ネットワークから自律システム番号をプリペンドします。このコマンドは、自律システムの移行のためだけに設定する必要があり、遷移が完了した後設定解除する必要があります。この手順は、経験豊富なネットワーク オペレータだけが行うべきものです。不適切な設定によってルーティング ループが作成される可能性があります。

ステップ 26 BGP ネイバーシップの送信元としてインターフェイスを更新する場合：

neighbor {ipv6-address} update-source {interface name}

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 update-source loop1
```

引数 interface name は、BGP ネイバーが BGP ルーティングの送信元として使用するインターフェイスの名前を指定します。

（注）
BGP ネイバーシップの送信元としてループバック インターフェイスを更新すると、ループバック インターフェイスの IP アドレスがネットワーク全体にアドバタイズされます。ループバック インターフェイスは eBGP ピアとして機能し、ルーティングに参加します。ループバック インターフェイスは有効にすると安定し、管理上のシャットダウンまで使用可能な状態になるため、ループバック インターフェイスの IP アドレスで常に ASA に到達できます。

IPv6 ネットワークの設定

ここでは、BGP ルーティング プロセスによってアドバタイズされるネットワークを定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp *autonomous-num*

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 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、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv6 [unicast]

ステップ 3 BGP ルーティング プロセスによってアドバタイズされるネットワークを指定します。

network {*prefix_delegation_name* [*subnet_prefix*/*prefix_length*] | *ipv6_prefix*/*prefix_length*} [**route-map** *route_map_name*]

例：

```
ciscoasa(config-router-af)# network 2001:1/64 route-map test_route_map
ciscoasa(config-router-af)# network outside-prefix 1::/64
ciscoasa(config-router-af)# network outside-prefix 2::/64
```

- *prefix_delegation_name*：DHCPv6 プレフィクス委任クライアント（**ipv6 dhcp client pd**）を有効にすると、プレフィックスをアドバタイズできます。プレフィックスをサブネット化するには、*subnet_prefix*/*prefix_length* を指定します。
- *ipv6 network*/*prefix_length*：BGP がアドバタイズするネットワーク。
- （オプション）**route-map** *name*：設定されているルート マップの ID。ルート マップは、アドバタイズされるネットワークをフィルタリングするために調べる必要があります。この値を指定しない場合、すべてのネットワークがアドバタイズされます。

IPv6 再配布の設定

ここでは、別のルーティング ドメインから BGP にルートを再配布する条件を定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 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、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv6 [unicast]

例：

```
ciscoasa(config-router)# address-family ipv6[unicast]
```

ステップ 3 別のルーティング ドメインから BGP 自律システムにルートを再配布します。

```
redistribute protocol [process-id][autonomous-num][metric metric value][match{internal|
 external1|external2|NSSA external 1|NSSA external 2}][route-map [map-tag]][subnets]
```

例：

```
ciscoasa(config-router-af)# redistribute ospf 2 route-map example1 match external
```

- protocol：ルートの再配布元となるソース プロトコル。Connected、EIGRP、OSPF、RIP または Static のいずれかを指定できます。
- （オプション）process-id：OSPF プロトコルの場合は、ルートの再配布元となる適切な OSPF プロセス ID です。この値により、ルーティング プロセスを識別します。この値は 0 以外の 10 進数で指定します。

  （注）
  この値は、その他のプロトコルでは自動入力されます。

- （オプション）metric metric value：同じルータ上で 1 つの OSPF プロセスから別の OSPF プロセスに再配布する場合、メトリック値を指定しないと、メトリックは 1 つのプロセスから他のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。デフォルト値は 0 です
- （オプション）match internal | external1 | external2 | NSSA external 1 | NSSA external 2：OSPF ルートが他のルーティング ドメインに再配布される条件を表します。次のいずれかを指定できます。
  - internal：特定の自律システムの内部にあるルート。
  - external 1：自律システムの外部だが、BGP に OSPF タイプ 1 外部ルートとしてインポートされるルート。
  - external 2：自律システムの外部だが、BGP に OSPF タイプ 2 外部ルートとしてインポートされるルート。
  - NSSA external 1：自律システムの外部だが、BGP に OSPF NSSA タイプ 1 外部ルートとしてインポートされるルート。
  - NSSA external 2：自律システムの外部だが、BGP に OSPF NSSA タイプ 2 外部ルートとしてインポートされるルート。
- （オプション）map-tag：設定されているルート マップの ID。

（注）

ルートマップは、再配布されるネットワークをフィルタリングするために調べる必要があります。この値を指定しない場合、すべてのネットワークが再配布されます。

IPv6 ルート注入の設定

ここでは、条件に応じて BGP ルーティング テーブルに注入されるルートを定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 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、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv6 [unicast]

例：

```
ciscoasa(config-router)# address-family ipv6 [unicast]
```

ステップ 3 BGP ルーティング テーブルに固有性の強いルートを注入するよう条件付きルート注入を設定します。

bgp inject-map inject-map exist-map exist-map [copy-attributes]

例：

```
ciscoasa(config-router-af)# bgp inject-map example1 exist-map example2 copy-attributes
```

- inject-map：ローカル BGP ルーティング テーブルに注入するプレフィックスを指定するルート マップの名前。
- exist-map：BGP スピーカーが追跡するプレフィックスを含むルート マップの名前。
- （オプション）copy-attributes：集約ルートの属性を継承するよう注入されたルートを設定します。

BGP のモニタリング

次のコマンドを使用して、BGP ルーティング プロセスをモニターできます。コマンド出力の例と説明については、コマンド リファレンスを参照してください。また、ネイバー変更メッセージとネイバー警告メッセージのロギングをディセーブルにできます。

さまざまな BGP ルーティング統計情報をモニターするには、次のコマンドの 1 つを入力します。

- **show bgp** [ip-address [mask [longer-prefixes [injected] | shorter-prefixes [length]]]| prefix-list name | route-map name]

  BGP ルーティング テーブル内のエントリを表示します。

- **show bgp** cidr-only

  ナチュラル ネットワーク マスク以外を使用するルート（つまり、クラスレス ドメイン間ルーティング（CIDR））を表示します。

- **show bgp community community-number [exact-match][no-advertise][no-export]**

  指定された BGP コミュニティに属するルートを表示します。

- **show bgp community-list community-list-name [exact-match]**

  BGP コミュニティ リストによって許可されたルートを表示します。

- **show bgp filter-list** *access-list-number*

  指定されたフィルタ リストと一致するルートを表示します。

- **show bgp injected-paths**

  BGP ルーティング テーブルに注入されたすべてのパスを表示します。

- **show bgp ipv4 unicast**

  ユニキャスト セッションの IPv4 BGP ルーティング テーブルのエントリを表示します。

- show bgp ipv6 unicast

  IPv6 の Border Gateway Protocol（BGP）ルーティング テーブルのエントリを表示します。

- show bgp ipv6 community

  指定された IPv6 Border Gateway Protocol（BGP）コミュニティに属するルートを表示します。

- show bgp ipv6 community-list

  IPv6 Border Gateway Protocol（BGP）コミュニティ リストによって許可されたルートを表示します。

- show bgp ipv6 filter-list

  指定された IPv6 フィルタ リストと一致するルートを表示します。

- show bgp ipv6 inconsistent-as

  整合性のない発信自律システムを使用している IPv6 Border Gateway Protocol（BGP）ルートを表示します。

- show bgp ipv6 neighbors

  ネイバーへの IPv6 Border Gateway Protocol（BGP）接続に関する情報を表示します。

- show bgp ipv6 paths

  データベース内のすべての IPv6 Border Gateway Protocol（BGP）パスを表示します。

- show bgp ipv6 prefix-list

  プレフィックス リストに一致するルートを表示します。

- show bgp ipv6 quote-regexp

  自律システム パスの正規表現と一致する IPv6 Border Gateway Protocol（BGP）ルートを引用符で囲まれた文字列として表示します。

- show bgp ipv6 regexp

  自律システム パスの正規表現と一致する IPv6 Border Gateway Protocol（BGP）ルートを表示します。

- show bgp ipv6 route-map

  ルーティング テーブルにインストールできなかった IPv6 Border Gateway Protocol（BGP）ルートを表示します。

- show bgp ipv6 summary

  すべての IPv6 Border Gateway Protocol（BGP）接続のステータスを表示します。

- show bgp neighbors ip_address

  ネイバーに対する BGP 接続と TCP 接続に関する情報を表示します。

- show bgp paths [LINE]

  データベース内のすべての BGP パスを表示します。

- show bgp pending-prefixes

  削除が保留されているプレフィックスを表示します。

- show bgp prefix-list prefix_list_name [WORD]

  指定のプレフィックス リストに一致するルートを表示します。

- show bgp regexp regexp

  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。

- show bgp replication [index-group | ip-address]

  BGP アップデート グループのアップデートのレプリケーション統計情報を表示します。

- show bgp rib-failure

ルーティング情報ベース（RIB）テーブルにインストールできなかったBGPルートを表示します。

- show bgp route-map map-name

  指定されたルート マップに基づいて、BGP ルーティング テーブルのエントリを表示します。

- show bgp summary

  すべての BGP 接続のステータスを表示します。

- show bgp system-config

  マルチ コンテキスト モードでシステム コンテキスト固有の BGP 設定を表示します。

  このコマンドは、マルチ コンテキスト モードのすべてのユーザー コンテキストで使用できます。

- show bgp update-group

  BGP アップデート グループに関する情報を表示します。

（注） BGP ログ メッセージを無効にするには、ルータ コンフィギュレーション モードで **no bgp log-neighbor-changes** コマンドを入力します。これにより、ネイバー変更メッセージのロギングが無効になります。BGP 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 モードでこのコマンドを入力します。デフォルトでは、ネイバー変更はログに記録されます。

BGP の例

次の例に、さまざまなオプションのプロセスを使用して BGPv4 をイネーブルにし、設定する方法を示します。

1. ルーティング プロトコル間のルートの再配布に対する条件を定義します。または、ポリシー ルーティングをイネーブルにします。

```
ciscoasa(config)# route-map mymap2 permit 10
```

2. 指定されたアクセス リストのいずれかによって渡されるルートアドレスまたは一致パケットを持つルートを再配布します。

```
ciscoasa(config-route-map)# match ip address acl_dmz1 acl_dmz2
```

3. ポリシールーティング用のルートマップのmatch節を通過したパケットの送出先を指定します。

```
ciscoasa(config-route-map)# set ip next-hop peer address
```

4. グローバル コンフィギュレーション モードで BGP ルーティング プロセスをイネーブルにします。

```
ciscoasa(config)# router bgp 2
```

5. アドレス ファミリ コンフィギュレーション モードでローカル Border Gateway Protocol（BGP）ルーティング プロセスの固定ルータ ID を設定します。

```
ciscoasa(config)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

6. エントリを BGP ネイバー テーブルに追加します。

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 remote-as 65
```

7. 着信ルートまたは発信ルートにルート マップを適用します。

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 route-map mymap2 in
```

8. BGP スピーキングネイバーの送信元としてインターフェイスを更新する場合：

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 update-source loop1
```

次の例に、さまざまなオプションのプロセスを使用して BGPv6 を有効にし、設定する方法を示します。

1. ルーティング プロトコル間のルートの再配布に対する条件を定義します。または、ポリシー ルーティングをイネーブルにします。

```
ciscoasa(config)# route-map mymap1 permit 10
```

2. 指定されたアクセス リストのいずれかによって渡されるルート アドレスまたは一致パケットを持つルートを再配布します。

```
ciscoasa(config-route-map)# match ipv6 address acl_dmz1 acl_dmz2
```

3. ポリシー ルーティング用のルート マップの match 節を通過したパケットの送出先を指定します。

```
ciscoasa(config-route-map)# set ipv6 next-hop peer address
```

4. グローバル コンフィギュレーション モードで BGP ルーティング プロセスをイネーブルにします。

```
ciscoasa(config)# router bgp 2
```

5. アドレス ファミリ コンフィギュレーション モードでローカル Border Gateway Protocol（BGP）ルーティング プロセスの固定ルータ ID を設定します。

```
ciscoasa(config)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

6. 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、標準IPv6アドレス プレフィックスを使用するルーティング セッションを設定します。

```
address-family ipv6 [unicast]
```

7. エントリを BGP ネイバー テーブルに追加します。

```
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 remote-as 64600
```

8. 着信ルートまたは発信ルートにルート マップを適用します。

```
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 route-map mymap1 in
```

9. BGP スピーキング ネイバーの送信元としてインターフェイスを更新する場合：

```
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 update-source loop1
```

BGP の履歴

表 *1 : BGP* の各機能の履歴

機能名	プラットフォーム リリース	機能情報
BGP のサポート	9.2(1)	Border Gateway Protocol を使用した、データのルーティング、認証の実行、およびルーティング情報の再配布とモニターについて、サポートが追加されました。 次のコマンドが導入されました。**router bgp**、**bgp maxas-limitbgp maxas-limit**、**bgp log-neighbor-changes**、**bgp transport path-mtu-discovery**、**bgp fast-external-fallover**、**bgp enforce-first-as**、**bgp asnotation dot**、**timers bgp**、**bgp default local-preference**、**bgp always-compare-med**、**bgp bestpath compare-routerid**、**bgp deterministic-med**、**bgp bestpath med missing-as-worst**、**policy-list**、**match as-path**、**match community**、**match metric**、**match tag**、**as-path access-list**、**community-list**、**address-family ipv4**、**bgp router-id**、**distance bgp**、**table-map**、**bgp suppress-inactive**、**bgp redistribute-internal**、**bgp scan-time**、**bgp nexthop**、**aggregate-address**、**neighbor**、**bgp inject-map**、**show bgp**、**show bgp cidr-only**、**show bgp all community**、**show bgp all neighbors**、**show bgp community**、**show bgp community-list**、**show bgp filter-list**、**show bgp injected-paths**、**show bgp ipv4 unicast**、**show bgp neighbors**、**show bgp paths**、**show bgp pending-prefixes**、**show bgp prefix-list**、**show bgp regexp**、**show bgp replication**、**show bgp rib-failure**、 **show bgp route-map**、**show bgp summary**、**show bgp system-config**、**show bgp update-group**、**clear route network**、**maximum-path**、 **network**。 次のコマンドが変更されました。**show route**、**show route summary**、**show running-config router**、**clear config router**、**clear route all**、**timers lsa arrival**、**timers pacing**、**timers throttle**、**redistribute bgp**。
ASA クラスタリングに対する BGP のサポート	9.3(1)	L2 および L3 クラスタリングのサポートが追加されました。 次のコマンドが導入されました。bgp router-id clusterpool

機能名	プラットフォーム リリース	機能情報
ノンストップ フォワーディングに対する BGP のサポート	9.3(1)	ノンストップ フォワーディングのサポートが追加されました。 次のコマンドが導入されました。bgp graceful-restart、neighbor ha-mode graceful-restart
アドバタイズされたマップに対する BGP のサポート	9.3(1)	アドバタイズされたマップに対する BGPv4 のサポートが追加されました。 次のコマンドが導入されました。neighbor advertise-map
IPv6 に対する BGP のサポート	9.3(2)	IPv6 のサポートが追加されました。 次のコマンドが導入されました。address-family ipv6、ipv6 prefix-list、ipv6 prefix-list description、ipv6 prefix-list sequence-number、match ipv6 next-hop、match ipv6 route-source、match ipv6- address prefix-list、set ipv6-address prefix -list、set ipv6 next-hop、set ipv6 next-hop peer-address 次のコマンドが変更されました。bgp router-id
委任プレフィックスの IPv6 ネットワーク アドバタイズメント	9.6(2)	ASA は DHCPv6 プレフィックスの委任クライアントをサポートするようになりました。ASA は DHCPv6 サーバーから委任プレフィックスを取得します。ASA は、これらのプレフィックスを使用して他の ASA インターフェイスのアドレスを設定し、ステートレス アドレス自動設定（SLAAC）クライアントが同じネットワーク上で IPv6 アドレスを自動設定できるようにします。これらのプレフィックスをアドバタイズするように BGP ルータを設定できます。 次のコマンドが変更されました。**network**
BGP トラフィックのループバック インターフェイス サポート	9.18(2)	ループバック インターフェイスを追加して、BGP トラフィックに使用できるようになりました。 新規/変更されたコマンド：**interface loopback**、**neighbor update-source**
IPv6 のグレースフル リスタート	9.19(1)	IPv6 アドレス ファミリのグレースフル リスタート サポートを追加しました。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。