ファイアウォール デバイスでのルーティング ポリシーの設定

Security Manager のルーティング セクションには、セキュリティ アプライアンスのルーティング設定を定義および管理するためのページがあります。

この章は次のトピックで構成されています。

[No Proxy ARP] の設定

あるホストから同じイーサネット ネットワーク上の別のデバイスに IP トラフィックを送信する場合、そのホストは送信先のデバイスの MAC アドレスを知る必要があります。Address Resolution Protocol（ARP）は、IP アドレスを MAC アドレスに解決するレイヤ 2 プロトコルです。ホストは、「この IP アドレスはだれですか」と質問する ARP 要求を送信します。その IP アドレスを所有するデバイスは、自分が所有者であることを自分の MAC アドレスで返答します。

プロキシ ARP を使用すると、デバイスは IP アドレスを持っていない場合でも、ARP 要求に対して MAC アドレスを返信します。別のホストの ARP プロキシとして機能することにより、

ネットワーク トラフィックをプロキシ（この場合は、セキュリティ アプライアンス）に転送できます。アプライアンスを通過するトラフィックは、適切な宛先にルーティングされます。

たとえば、NAT を設定し、同じネットワーク上のグローバル アドレスをアプライアンスのインターフェイスとして指定すると、セキュリティ アプライアンスではプロキシ ARP が使用されます。アプライアンスがトラフィックを要求してから宛先グローバルアドレスにルーティングする場合にだけ、トラフィックは宛先ホストに到達できます。

デフォルトでは、プロキシARPはすべてのインターフェイスに対してイネーブルです。グローバル アドレスに対してプロキシ ARP をディセーブルにするには、[No Proxy ARP] ページを使用します。

- 1 つ以上のインターフェイスに対してプロキシARPをディセーブルにするには、[Interfaces] フィールドに名前を入力します。複数のインターフェイスを指定する場合は、カンマで区切ります。[Select] をクリックして、デバイス上に定義されているインターフェイスおよび Security Manager で定義されているインターフェイス ロールのリストから、インターフェイスを選択できます。

（注） ルーテッドモードで動作するASA 8.4.2以降のデバイスでは、手動NATルールの出力インターフェイスで Proxy ARP をディセーブルできます。詳細については、テーブル 24-15 の「宛先インターフェイスで*ARP*をプロキシしない」を参照してください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、[プラットフォーム（Platform）] > [ルーティング（Routing）] > [プロキシARPなし（No Proxy ARP）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [プロキシARPなし（No Proxy ARP）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- スタティック ルートの設定 （208 ページ）
- RIP の設定 （196 ページ）
- OSPF の設定 （129 ページ）

BGP の設定

Border Gateway Protocol（BGP）は相互自律システム 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 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。

（注） BGP 設定は、ASA 9.2(1)+ でのみサポートされています。また、ASA 9.3(1) 以降、BGP は L2（EtherChannel タイプ）および L3（個別インターフェイスタイプ）クラスタリングモードでのみサポートされています。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [ルーティング（Routing）] > [BGP]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [BGP]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

[BGP] ページには、ファイアウォールデバイス上の BGP ルーティングを設定するための 2 つのタブ付きパネルがあります。次に、BGP プロセスを設定するための基本的な手順を示します。

1. [BGP] ページの [GBPの有効化（Enable BGP）] チェックボックスをオンにして、BGP ルーティングプロセスをイネーブルにします。
2. [AS Number] フィールドに、BGP プロセスの自律システム（AS）番号を入力します。AS 番号内部には、複数の自律番号が含まれます。AS 番号には、1 ～ 4294967295 または 1.0 ～ 65535.65535 を指定できます。
3. [General] タブ （7 ページ） で、次の手順を実行します。
   - （オプション）[受信されたルートのAS_PATH属性に含まれるAS番号の数を制限する（Limit the number of AS numbers in the AS_PATH attribute of received routes）] チェックボックスをオンにして、AS_PATH 属性の AS 番号の数を特定数に制限します。有効値は 1 ～ 254 です。
   - （オプション）[ネイバーの変更の記録（Log Neighbor Changes）] チェックボックスをオンにして、BGP ネイバーの変更（アップ状態またはダウン状態）およびリセットのロギングをイネーブルにします。これは、ネットワーク接続の問題をトラブルシューティングしたり、ネットワークの安定性を評価する際に役に立ちます。
   - （オプション）[TCPパスMTUディスカバリを使用する（Use TCP path MTU discovery）] チェックボックスをオンにし、パス MTU ディスカバリ手法を使用して 2 つの IP ホスト間のネットワークパスにおける最大伝送単位（MTU）のサイズを決定します。これにより、IP フラグメンテーションが回避されます。
   - （オプション）[Enable fast external failover] チェックボックスをオンにして、リンク障害の発生時に外部 BGP セッションをただちにリセットします。

- （オプション）[最初のASをEBGPルートのピアのASとして実行（Enforce that first AS is peer's AS for EBGP routes）] チェックボックスをオンにして、そのAS番号をAS_path属性の1つ目のセグメントとしてリストしていない外部BGPピアから受信した着信アップデートを破棄します。これにより、誤って設定されたピアや許可されていないピアが、別の自律システムから送信されたかのようにルートをアドバイタイズしてトラフィックを誤った宛先に送信することがなくなります。
- （オプション）[Use dot notation for AS numbers] チェックボックスをオンにして、完全なバイナリ4バイトのAS番号を、ドットで区切られた16ビットの2文字ずつに分割します。0 ～ 65553 の AS 番号は10進数で表され、65535を超えるAS番号はドット付き表記を使用して表されます。
- BGPルーティングの最適なパスの選択プロセスに関連する設定を定義します（[General] タブ （7 ページ）を参照）。
- [ネイバータイマー（Neighbor timers）] 領域でタイマー情報を指定します（[General] タブ （7 ページ）を参照）。
- （オプション）グレースフルリスタートを設定します（[General] タブ （7 ページ）を参照）。

4. [IPv4ファミリ（IPv4 Family）] タブで、[IPv4ファミリの有効化（Enable IPv4 Family）] チェックボックスをオンにし、提供されているタブを使用してIPv4アドレスファミリを設定します。詳細については、[IPv4ファミリ（IPv4 Family）] タブ （9 ページ）を参照してください。
5. [IPv6ファミリ（IPv6 Family）] タブで、[IPv6ファミリの有効化（Enable IPv6 Family）] チェックボックスをオンにし、提供されているタブを使用してIPv6アドレスファミリを設定します。詳細については、[IPv6ファミリ（IPv6 Family）] タブ （31 ページ）を参照してください。

関連項目

- BGP について （4 ページ）

BGP について

BGPは相互自律システム 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 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

大学や企業などの顧客ネットワークでは、その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などの内部ゲートウェイ プロトコル（IGP）を通常使用しています。顧客はISPに接続し、ISPはBGPを使用して顧客のルートとISPの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。

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。

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。これらのプロパティは 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。[重要度（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、[重要度（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 からの出力点を選択するために使用されます。[重要度（Weight）] 属性とは異なり、[ローカル プリファレンス（Local preference）] 属性は、ローカル AS 全体に伝搬されます。AS からの出力点が複数ある場合は、[ローカル プリファレンス（Local preference）] 属性値が最も高い出力点が特定のルートの出力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、アドバタイズしている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。
- Community：Community 属性は、ルーティングの決定（承認、優先度、再配布など）を適用できる宛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、[コミュニティ（Community）] 属性を設定するために使用されます。定義済みの [コミュニティ（Community）] 属性は次のとおりです。
  - no-export：EBGP ピアにこのルートを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の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。このパスを選択すると、BGP は IP ルーティング テーブルに選択したパスを格納し、そのネイバーにパスを伝搬します。BGP は次の基準を使用して（示されている順序で）、宛先へ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、この更新はドロップされます。
- ウェイトが最大のパスが優先されます。
- ウェイトが同じである場合、ローカルの優先順位が最大のパスが優先されます。
- ローカルの優先順位が同じである場合、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 の長さが同じである場合、起点タイプが最下位のパス（[IGP] は [EGP] よりも低く、[EGP] は [不完全（Incomplete）] よりも低い）が優先されます。
- 起点コードが同じである場合、最も小さい MED 属性を持つパスが優先されます。
- パスの MED が同じである場合、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である場合、最も近い IGP ネイバーを経由するパスが優先されます。
- 両方のパスが外部の場合、最初に受信したパス（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。
- 送信元またはルータ ID が複数のパスで同じである場合、クラスタ リストの長さが最小の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。

[General] タブ

[全般（General）] タブを使用して、[ベストパス選択（Best Path Selection）]、[ネイバータイマー（Neighbor Timers）]、[グレースフルリスタート（Graceful Restart）] などの BGP 設定を構成します。

ナビゲーション パス

[ネイバー（Neighbors）] タブには、[OSPF] ページからアクセスできます（BGP の設定 （2 ページ）を参照）。

関連項目

- BGP の設定 （2 ページ）
- BGP について （4 ページ）
- [IPv4ファミリ（IPv4 Family）] タブ （9 ページ）

フィールド リファレンス

表 1 : [General] タブ

要素	説明
[受信されたルートのAS_PATH属性に含まれるAS番号の数（Limit the number of AS numbers in AS_PATH attribute of received routes）]	AS_PATH 属性に含まれる AS 番号の数を特定の数に制限します。有効値は 1 ～ 254 です。
ネイバーの変更を記録（Log Neighbor Changes）	BGP ネイバーの変更（アップまたはダウン）のロギングを有効にします。これは、ネットワーク接続の問題をトラブルシューティングしたり、ネットワークの安定性を評価する際に役に立ちます。
[TCPパスMTUディスカバリを使用する（Use TCP Path MTU Discovery）]	パス MTU ディスカバリ手法を使用して、2 つの IP ホスト間のネットワークパスにおける最大伝送ユニット（MTU）のサイズを決定します。これにより、IP フラグメンテーションが回避されます。
[高速外部フェールオーバーの有効化（Enable fast external failover）]	リンク障害の発生時、外部 BGP セッションを即時にリセットします。

要素	説明
[最初のASをEBGPルートのピアのASとして実行（Enforce that the first AS is peer's AS for EBGP routes）]	AS 番号を AS_path 属性の 1 つ目のセグメントとしてリストに表示していない外部 BGP ピアから受信した着信アップデートを破棄します。これにより、誤って設定されたピアや許可されていないピアが、別の自律システムから送信されたかのようにルートをアドバイタイズしてトラフィックを誤った宛先に送信することがなくなります。
[AS番号にドット表記を使用（Use dot notation for AS numbers）]	完全なバイナリ 4 バイトの AS 番号を、ドットで区切られた 16 ビットの 2 文字ずつに分割します。0 ～ 65553 の AS 番号は 10 進数で表され、65535 を超える AS 番号はドット付き表記を使用して表されます。
[ベストパスの選択（Best Path Selection）]	
Default local preference	0 ～ 4294967295 の数値を指定します。デフォルト値は 100 です。値が大きいほど、優先度が高いことを示します。この優先度は、ローカル自律システム内のすべてのルータおよびアクセス サーバーに送信されます。
[異なるネイバーのMEDの比較を許可（Allow comparing MED from different neighbors）]	異なる自律システムにあるネイバーからのパスの Multi-Exit 識別子（MED）の比較を許可します。
[同一のBGPパスのルータIDを比較（Compare Router-id for identical EBGP paths）]	ベストパスの選択プロセス中に外部 BGP ピアから受信した類似パスを比較し、ベストパスをルータ ID が最も小さいルートに切り替えます。
[隣接ASからアドバタイズされたパスの間で最適なMEDパスを選択（Pick the best MED path among paths advertised from the neighboring AS）]	コンフェデレーション ピアから学習した複数のパスの間で MED 比較をイネーブルにします。MED 間の比較は、外部の自律システムがパスに存在しない場合にのみ行われます。
[欠落MEDを最低優先度として処理（Treat missing MED as the least preferred one）]	欠落している MED 属性は無限大の値を持つものとみなし、このパスを最も推奨度の低いパスにします。したがって、MED が欠落しているパスが最も優先度が低くなります。
[ネイバータイマー（Neighbor Timers）]	
[キープアライブ間隔（Keepalive Interval）]	キープアライブメッセージを送信しなかった場合に、その後 BGP ネイバーがアクティブな状態を継続する時間間隔を入力します。このキープアライブ インターバルが終わると、メッセージが送信されない場合、BGP ピアはデッドとして宣言されます。デフォルト値は 60 秒です。

要素	説明
保留時間（Hold Time）	BGP 接続が開始され設定されている間、BGP ネイバーがアクティブな状態を継続する時間間隔を入力します。デフォルト値は 180 秒です。
Min Hold Time	（任意）BGP 接続が開始され設定されている間、BGP ネイバーがアクティブな状態を継続する最小時間間隔を入力します。0 ～ 65535 の値を指定します。
[グレースフルリスタート（Graceful Restart）]（フェールオーバーまたはスパンドクラスタモードで使用） （ASA 9.3.1 以降のみ）	
グレースフル リスタートをイネーブルにします。	スイッチオーバー後のルーティングフラップを ASA ピアが回避できるようにします。
再起動時間	BGP オープンメッセージが受信される前に、ASA ピアが古いルートを削除するまでの待機時間を指定します。デフォルト値は 120 秒です。有効な値は 1 ～ 3600 秒です。
[Stalepath時間（Stalepath Time）]	再起動する ASA から End Of Record（EOR）メッセージを受信した後、ASA が古いルートを削除するまでの待機時間を入力します。デフォルト値は 360 秒です。有効な値は 1 ～ 3600 秒です。

[IPv4ファミリ（IPv4 Family）] タブ

[BGP] ページの [IPv4ファミリ（IPv4 Family）] タブを使用して、BGP の IPv4 設定を有効にして構成します。

ナビゲーション パス

[BGP] ページから [IPv4ファミリ（IPv4 Family）] タブにアクセスできます。[BGP] ページの詳細については、BGP の設定 （2 ページ）を参照してください。

関連項目

- BGP について （4 ページ）
- [General] タブ （7 ページ）

フィールド リファレンス

表 *2 : IPv4* ファミリ：*[*集約アドレス（*Aggregate Address*）*]* タブ

要素	説明
IPv4ファミリの有効化（Enable IPv4 Family）	標準の 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の設定を有効にします。
一般	このパネルを使用して、[ベストパス選択（Best Path Selection）]、[ネイバータイマー（Neighbor Timers）]、[グレースフルリスタート（Graceful Restart）] などの一般的な IPv4 設定を設定します。これらの定義の詳細については、IPv4 Family - [全般（General）] タブ （11 ページ）を参照してください。
[Aggregate Address]	このパネルを使用して、特定のルートから 1 つのルートへの集約を定義します。 [Aggregate Timer] フィールドで、集約タイマーの値（秒）を指定します。有効な値は、0 または 6 ～ 60 の値です。デフォルト値は 30 です。 これらの定義の詳細については、[集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス （34 ページ）を参照してください。
フィルタリング	このパネルを使用して、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をフィルタ処理します。これらの定義の詳細については、[Add Filter]/[Edit Filter] ダイアログボックス （15 ページ）を参照してください。
ネイバー	このパネルを使用して、BGP ネイバーとネイバーの設定を定義します。これらの定義の詳細については、[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （16 ページ）を参照してください。
ネットワーク	このパネルを使用して、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します。これらの定義の詳細については、[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （27 ページ）を参照してください。
再配布	このパネルを使用して、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します。これらの定義の詳細については、[Add Redistribution]/[Edit Redistribution] ダイアログボックス （28 ページ）を参照してください。
ルートの挿入	このパネルを使用して、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します。これらの定義の詳細については、[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （29 ページ）を参照してください。

IPv4 Family - [全般（General）] タブ

[IPv4 ファミリ] - [全般（General）] タブを使用して、全般的な IPv4 設定を行います。

ナビゲーション パス

[全般（General）] タブには、[BGP] ページの [IPv4ファミリ（IPv4 Family）] タブからアクセスできます。[IPv4ファミリ（IPv4 Family）] タブの詳細については、[IPv4ファミリ（IPv4 Family）] タブ （9 ページ）を参照してください。

関連項目

- BGP の設定 （2 ページ）
- BGP について （4 ページ）

フィールド リファレンス

表 3 : IPv4 Family - [全般（General）] タブ

要素	説明
ルータ ID（Router ID）	単一のデバイスで、[自動（Automatic）] または [IPアドレス（IP Address）] を選択します。（IP アドレスを選択すると、[アドレス（address）] フィールドが表示されます。） [自動（Automatic）] を選択すると、セキュリティアプライアンス上で最上位の IP アドレスがルータ ID として使用されます。固定ルータ ID を使用するには、[IPアドレス（IP Address）] を選択して、[ルータ ID（Router ID）] フィールドに IPv4 アドレスを入力します。 デバイスクラスタで、[自動（Automatic）] または [クラスタプール（Cluster Pool）] を選択します。（[クラスタプール（ Cluster Pool）] を選択すると、[IPv4プールオブジェクトID（ IPv4 Pool object ID）] フィールドが表示されます）。 [クラスタプール（Cluster Pool）] を選択した場合は、ルータの ID アドレスを提供する IPv4 プールオブジェクトの名前を入力または選択します。詳細については、[IPv4プールの追加または編集（Add or Edit IPv4 Pool）] ダイアログボックスを参照してください。

要素	説明
学習したルートマップ	ルートマップオブジェクトの名前を入力または選択します。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。
スキャン間隔	ネクストホップの検証用に BGP ルータのスキャン間隔（秒）を入力します。有効な値は 5 ～ 60 秒です。デフォルト値は 60 です。
ルートと同期	
デフォルトルートの生成	（任意）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。
サブネットルートをネットワークレベルのルートに集約します。	（任意）サブネットルートのネットワークレベルルートへの自動集約を設定します。
非アクティブのルートのアドバタイズ	（任意）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をアドバタイズします。
BGP と内部ゲートウェイプロトコル（IGP）システム間の同期	BGP と内部ゲートウェイプロトコル（IGP）システム間の同期をイネーブルにします。Cisco IOS ソフトウェアが IGP を待機せずにネットワークルートをアドバタイズできるようにするには、このオプションの選択を解除します。 通常、ルートがローカルであるか IGP に存在する場合を除き、BGP スピーカーは外部ネイバーにルートをアドバタイズしません。デフォルトでは BGP と IGP 間の同期はオフになっており、Cisco IOS ソフトウェアが IGP を待機せずにネットワーク ルートをアドバタイズできるようになっています。この機能により、自律システム内のルータおよびアクセス サーバーは、BGP が他の自律システムでルートを使用可能にする前にルートを確保できるようになります。自律システム内のルータが BGP を実行していない場合は、synchronization を使用します。
IBGPのIGPへの再配布	（任意）IS-IS や OSPF などの内部ゲートウェイプロトコル（IGP）への iBGP の再配布を設定します。
Administrative Route Distances	

要素	説明
外部	外部 BGP ルートのアドミニストレーティブ ディスタンスを指定します。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。デフォルト値は 20 です。
内線	内部 BGP ルートのアドミニストレーティブ ディスタンスを指定します。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。デフォルト値は 200 です。
ローカル（Local）	ローカルの BGP ルートのアドミニストレーティブ ディスタンスを指定します。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。デフォルト値は 200 です。
ネクスト ホップ	
アドレストラッキングの有効化	（任意）BGP ネクストホップ アドレス トラッキングをイネーブルにします。
遅延間隔	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指定します。
マルチパス上のフォワードパケット	
パス数	（任意）ルーティングテーブルにインストールできる外部 BGP ルートの最大数を指定します。
IBGP のパス数	（任意）ルーティングテーブルにインストールできる内部 BGP ルートの最大数を指定します。

[集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス

[集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックスで、特定のルートの 1 つのルートへの集約を定義します。

ナビゲーション パス

[集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックスには、[IPv4ファミリ（IPv4 Family）] タブ （9 ページ）からアクセスできます。

関連項目

- BGP の設定 （2 ページ）
- BGP について （4 ページ）

- IPv4 Family - [全般（General）] タブ （11 ページ）
- [Add Filter]/[Edit Filter] ダイアログボックス （15 ページ）
- [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （16 ページ）
- [ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （27 ページ）
- [Add Redistribution]/[Edit Redistribution] ダイアログボックス （28 ページ）
- [ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （29 ページ）

フィールド リファレンス

表 *4 : [*集約アドレスの追加/編集（*Add/Edit Summary Address***）*]* ダイアログボックス**

要素	説明
ネットワーク	IP アドレスを入力するか、目的のネットワーク/ホストオブジェクトを入力または選択します。
属性マップ	（オプション）集約ルートの属性の設定に使用されるルート マップを入力または選択します。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。
アドバタイズマップ（Advertise Map）	（オプション）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を入力または選択します。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。

要素	説明
抑制マップ（Suppress Map）	（オプション）抑制するルートの選択に使用されるルートマップを入力または選択します。 ヒント　[選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。
AS 設定パス情報の生成（Generate AS Set Path Information）	自律システム設定パス情報の生成を有効にします。
アップデートからのすべてのより具体的なルートをフィルタ処理（Filter all more-specific routes from updates）	アップデートからのすべてのより具体的なルートをフィルタ処理します。

[Add Filter]/[Edit Filter] ダイアログボックス

[フィルタの追加（Add Filter）]/[フィルタの編集（Edit Filter）] ダイアログボックスを使用して、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をフィルタ処理します。

ナビゲーション パス

[フィルタの追加（Add Filter）]/[フィルタの編集（Edit Filter）] ダイアログボックスには、[IPv4 ファミリ（IPv4 Family）] タブ （9 ページ）からアクセスできます。

関連項目

- BGP の設定 （2 ページ）
- BGP について （4 ページ）
- [IPv4ファミリ（IPv4 Family）] タブ：[全般（General）]タブ （94 ページ）
- [集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス （34 ページ）
- [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （36 ページ）
- [ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （46 ページ）
- [Add Redistribution]/[Edit Redistribution] ダイアログボックス （47 ページ）

- [ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス（48 ページ）

フィールド リファレンス

表 *5 : [Add Filter]/[Edit Filter]* ダイアログボックス

要素	説明
ACL	受信されるネットワークとルーティングアップデートで抑制されるネットワークを定義するアクセス制御リストを選択します。
方向	[Direction] ドロップダウン リストから方向を選択します。方向は、フィルタを着信アップデートに適用するか、または発信アップデートに適用するかを指定します。
プロトコル	[なし（None）]、[BGP]、[接続（Connected）]、[EIGRP]、[OSPF]、[RIP]、または [静的（Static）] のルーティングプロセスのうち、フィルタ処理するものを選択します。
AS 番号（AS Number）	BGP ルーティングプロセスの自律システム番号を表示します。この値は、BGP ページで指定されます（ BGP の設定 （2 ページ）を参照）。
プロセス ID（Process ID）	ルーティングプロセスの識別子を入力します。EIGRP および OSPF ルーティングプロトコルに適用されます。

[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス

[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックスを使用して、BGP ネイバーとネイバーの設定を定義します。

ナビゲーション パス

[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックスには、 [IPv4ファミリ（IPv4 Family）] タブ （9 ページ）からアクセスできます。

関連項目

- BGP の設定 （2 ページ）
- BGP について （4 ページ）
- IPv4 Family - [全般（General）] タブ （11 ページ）
- [集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス （13 ページ）
- [ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （27 ページ）

- [Add Redistribution]/[Edit Redistribution] ダイアログボックス （28 ページ）
- [ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （29 ページ）

フィールド リファレンス

表 *6 : [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス*

要素	説明
一般	
[IPアドレス（IP Address）]	BGP ネイバーの IP アドレスを入力します。この IP アドレスは、BGP ネイバー テーブルに追加されます。
リモート AS	BGP ネイバーが属する自律システムを入力します。
更新の送信元（Update Source） （ASA 9.19.1+ のみ）	（任意）BGP ネイバーシップの送信元インターフェイスを更新するには、適切なインターフェイスを選択します。 **ヒント** [選択（Select）] をクリックして、インターフェイスを選択できるインターフェイスセレクタを開きます。インターフェイスの詳細については、使用可能なインターフェイス タイプを参照してください。 **（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。
アドレスファミリの有効化（Enable Address Family）	（任意）BGP ネイバーとの通信を有効にします。
ネイバーを管理的にシャットダウンする（Shutdown neighbor administratively）	（任意）ネイバーまたはピアグループを無効にします。

要素	説明
ネイバーごとのBGPグレースフルリスタートの設定（Configure Graceful Restart per neighbor） （ASA 9.3.1 以降のみ）	（任意）ネイバーのボーダー ゲートウェイ プロトコル（BGP）グレースフルリスタート機能の設定を有効にします。このオプションを選択した後、[グレースフルリスタート（フェールオーバーまたはスパンドクラスタモードで使用）（Graceful Restart (Use in failover or spanned cluster mode)）] オプションを使用して、このネイバーに対してグレースフルリスタートを有効にするか、無効にするかを指定する必要があります。
[グレースフルリスタート（Graceful Restart）]（フェールオーバーまたはスパンドクラスタモードで使用） （ASA 9.3.1 以降のみ）	（任意）ネイバーのボーダー ゲートウェイ プロトコル（BGP）グレースフルリスタート機能を有効にします。
説明	（任意）BGP ネイバーの説明を入力します。
フォールオーバーBFD（fall-over BFD）	(オプション) BGP ネイバーのフォールオーバーに対する BFD サポートを有効にします。
BFDホップ（BFD-Hop）	（任意）BFD の送信元と宛先の間に単一の IP ホップがあるか、複数の IP ホップがあるかを指定します。
フィルタリング	
アクセスリストを使用してルートをフィルタ処理する（Filter routes using an access list）	（任意）適切な着信または発信アクセス制御リストを入力または選択して、BGP ネイバー情報を配布します。
ルートマップを使用してルートをフィルタ処理する（Filter routes using route map）	（任意）適切な着信または発信ルートマップを入力または選択して、着信または発信ルートにルートマップを適用します。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。

要素	説明
プレフィックスリストを使用してルートをフィルタ処理する（Filter routes using a Prefix list）	（任意）適切な着信または発信プレフィックスリストを入力または選択して、BGP ネイバー情報を配布します。 ヒント　[選択（Select）] をクリックして、プレフィックス リスト オブジェクトを選択できるプレフィックス リスト オブジェクト セレクタを開きます。オブジェクト プレフィックス リスト オブジェクト セレクタから新しいオブジェクトを作成することもできます。詳細については、[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （235 ページ）を参照してください。
ASパスフィルタを使用してルートをフィルタ処理する（Filter routes using AS Path filter）	（任意）適切な着信または発信ASパスフィルタを入力または選択して、BGP ネイバー情報を配布します。 ヒント　[選択（Select）] をクリックして、AS パスオブジェクトを選択できる AS パスオブジェクトセレクタを開きます。ASパスオブジェクトセレクタから新しいASパスオブジェクトを作成することもできます。詳細については、[ASパスオブジェクトの追加（（Add AS Path Object））]/[ASパスオブジェクトの編集（Edit AS Path Object）] ダイアログボックス （242 ページ）を参照してください。

要素	説明
ネイバーから許可されるプレフィックスの数を制限する（Limit the number of prefixes allowed from the neighbor）	（任意）選択して、ネイバーから受信できるプレフィックスの数を制御ます。 • [最大プレフィックス数（Maximum Prefixes）] フィールドに、特定のネイバーからの許可される最大プレフィックス数を入力します。 • [しきい値レベル（Threshold Level）] フィールドに、ルータが警告メッセージの生成を開始するパーセンテージ（最大数に対する割合）を入力します。有効な値は1～100の整数です。デフォルト値は 75 です。 • （任意）[ピアから受信したプレフィックスの制御（Control prefixes received from the peer）] チェックボックスをオンにし、ピアから受信したプレフィックスに対する追加の制御を指定します。次のいずれかを実行します。 • プレフィックス数の制限値に到達したときに BGP ネイバーを停止するには、[プレフィックス数の制限値を超えたときにピアリングを停止する（Terminate peering when prefix limit is exceeded）] を選択します。[Restart interval] フィールドで、BGP ネイバーが再起動するまでの時間を指定します。 • 最大プレフィックス数の制限値を超えたときにログメッセージを生成するには、[プレフィックス数の制限値を超えたときに警告メッセージのみを表示する（Give only warning message when prefix limit is exceeded）] を選択します。この場合、BGP ネイバーは終了しません。
ルート	
アドバタイズメント間隔	BGP ルーティング更新が送信される最小間隔（秒単位）を入力します。有効な値は、1 ～ 600 です。
アウトバウンドルーティング更新からプライベートAS番号を削除します。	（任意）プライベートAS番号をアウトバウンドルートでアドバタイズしないようにします。

要素	説明
デフォルトルートの生成（Generate Default route）	（任意）選択して、ネイバーへのデフォルトルート 0.0.0.0 の送信をローカルルータに許可して、デフォルトルートとして使用します。[ルートマップ（Route map）] フィールドで、ルート 0.0.0.0 が条件に応じて注入されるように許可するルート マップを入力または選択します。 ヒント [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。

ルートの条件付きアドバタイズ（Conditionally Advertised Routes）	（任意）条件付きでアドバタイズされるルートを追加または編集するには、[行の追加（Add Row）]（+）ボタンをクリックするか、テーブル内の行を選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。
	[アドバタイズ対象ルートの追加/編集（Add/Edit Advertised Route）] ダイアログボックスで、次の手順を実行します。
	• [選択（Select）] をクリックして [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。このセレクタから、存在マップまたは非存在マップの条件が満たされた場合にアドバタイズされるルートマップを選択できます。ルートマップの詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。
	• 次のいずれかを実行します。
	  • [存在マップの設定（Set Exist Map）] を選択し、[ルートマップオブジェクトセレクタ（Route Map Object Selector）] からルートマップを選択します。このルートマップは、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ます。
	  • [非存在マップ（Non-Exist Map）] を選択し、[ルートマップオブジェクトセレクタ（Route Map Object Selector）] からルートマップを選択します。このルートマップは、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ます。

要素	説明
タイマー	
BGPピアにタイマーを設定する（Set timers for the BGP peer）	（任意）選択して、キープアライブ頻度、ホールド時間、最小ホールド時間を設定します。
キープアライブ間隔（Keepalive Interval）	ASA がキープアライブ メッセージをネイバーに送信する頻度（秒）を有効な値は、0 ～ 65535 です。デフォルト値は 60 秒です。
保留時間（Hold Time）	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 が宣言するまでの間隔（秒単位）を入力します。有効な値は、0 ～ 65535 です。デフォルト値は 180 秒です。
Min Hold Time	（任意）キープアライブメッセージを受信できずに、ピアがデッドであると ASA が宣言するまでの最小間隔（秒単位）を入力します。有効な値は、0 ～ 65535 です。デフォルト値は 0 秒です。
詳細設定（Advanced）	
Enable Authentication	（任意）選択して、2 つの BGP ピア間の TCP 接続で MD5 認証を有効にします。 • [暗号化を有効にする（Enable Encryption）] ドロップダウンリストから暗号化タイプを選択します。 • パスワードを [Password] フィールドに入力します。[Confirm] フィールドにパスワードを再入力します。 パスワードは大文字と小文字を区別し、service password-encryption コマンドが有効な場合は最大 25 文字、service password-encryption コマンドが有効でない場合は最大 81 文字まで指定できます。最初の文字を数値にはできません。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） 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。
コミュニティ属性をこのネイバーに送信します	（任意）コミュニティ属性を BGP ネイバーに送信する必要があることを指定します。
ネイバーのネクストホップとしてASAを使用する（Use ASA as next hop for neighbor）	（任意）選択して、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ルータを設定します。

要素	説明
接続検証の無効化（Disable connection verification）	（任意）選択して、シングルホップで到達可能だが、ループバックインターフェイス上に設定されている、あるいは直接接続されない IP アドレスで設定されている eBGP ピアリングセッションの接続検証プロセスを無効にします。 このコマンドが必要になるのは、neighbor ebgp-multihop コマンドで TTL 値を 1 に設定している場合だけです。シングル ホップ eBGP ピアのアドレスに到達できる必要があります。neighbor update-source コマンドを使用して、BGP ルーティングプロセスでピアリングセッションにループバック インターフェイスを使用できるように設定する必要があります。 オフ（デフォルト）にすると、シングルホップ eBGP ピアリングセッション（TTL=254）について、BGP ルーティング プロセスで接続が検証され、eBGP ピアが同じネットワーク セグメントに直接接続されているかどうか確認されます。ピアが同じネットワーク セグメントに直接接続されていない場合、ピアリングセッションは確立されません。
直接接続されていないネイバーとの接続を許可する（Allow connections with neighbor that is not directly connected）	選択して、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、そのピアへの BGP 接続を試みます。 （オプション）[TTL hops] フィールドに存続可能時間を入力します。有効な値は、1 ～ 255 です。 （注） この機能は、シスコテクニカルサポート担当者の指示のもとでのみ使用してください。ルートが一定でないことによるループの発生を回避するために、マルチホップピアのルートがデフォルトルート（0.0.0.0）だけの場合はマルチホップは確立されません。

要素	説明
ネイバーへのTTLホップ数を制限する（Limit number of TTL hops to neighbor）	

要素	説明
	BGP ピアリングセッションを保護するには、このオプションを選択します。[TTL hops] フィールドに、eBGP ピアを区切るホップの最大数を入力します。有効な値は、1 ～ 254 です。 この機能は、CPU 利用率に基づく攻撃から BGP ピアリングセッションを保護するための簡単なセキュリティメカニズムを提供します。この種の攻撃は、通常、パケット ヘッダーの送信元と宛先の IP アドレスを偽造した大量の IP パケットでネットワークをあふれさせてネットワークをディセーブルにしようとする典型的な力任せのサービス拒否（DoS）攻撃です。 この機能は、TTL カウントがローカルの設定値以上である IP パケットだけを受け入れるという IP パケットの設計上の動作を利用したものです。IP パケットの TTL カウントを完全に偽造することは一般には不可能であると考えられます。内部の送信元ネットワークまたは宛先ネットワークにアクセスしない限り、信頼できるピアからの TTL カウントに完全に一致するパケットを偽造することはできません。 この機能は、参加している各ルータで設定する必要があります。この機能では、eBGP セッションが受信方向だけ保護され、送信 IP パケットまたはリモート ルータは影響を受けません。この機能がイネーブルの場合、BGP は、IP パケット ヘッダーの TTL 値がピアリング セッション用に設定された TTL 値以上の場合だけセッションを確立または維持します。この機能は BGP ピアリング セッションには影響しません。この機能がイネーブルの場合でも、キープアライブ パケットを受信しなければピアリングセッションは期限切れになります。受信パケットの TTL 値が、ローカルで設定された値未満の場合、パケットはサイレントに廃棄され、インターネット制御メッセージ プロトコル（ICMP）メッセージは生成されません。これは設計された動作です。偽造パケットへの応答は必要ありません。 この機能の効果を最大化するには、ローカルネットワークと外部ネットワーク間のホップ数が一致するように hop-count の値を正確に設定する必要があります。また、この機能をマルチホップ ピアリング セッションに対して設定する場合は、パスがそれぞれで異なる点についても考慮する必要があります。 このコマンドの設定には、次の制限が適用されます。 • この機能は、内部 BGP（iBGP）ピアではサポートされません。 • 大きい直径のマルチホップ ピアリングでは、この機能の効果は下がります。大きい直径のピアリング用に設定された BGP ルータに対する CPU 利用率に基づく攻撃の場合は、影

要素	説明
	響を受けたピアリング セッションをシャットダウンして、この攻撃に対処する必要がある場合があります。 • この機能は、ネットワーク内部が損なわれているピアからの攻撃には効果的ではありません。この制約事項には、送信元ネットワークと宛先ネットワークの間のネットワーク セグメント上のピアも含まれます。
TCPパスMTUディスカバリを使用する（Use TCP Path MTU Discovery）	（任意）選択して、BGP セッションの TCP トランスポートセッションを有効にします。
TCPトランスポートモード（TCP transport mode）	ドロップダウンリストから TCP 接続モードを選択します。オプションは [デフォルト（Default）]、[アクティブ（Active）]、または [パッシブ（Passive）] です。
重量	（任意）BGP ネイバー接続の重みを入力します。
BGPバージョン（BGP Version）	ドロップダウンリストから、ASA が受け入れる BGP バージョンを選択します。[4 のみ（4-Only）] に設定すると、指定されたネイバーとの間でバージョン 4 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。
移行 （注） このカスタマイズは、AS 移行にのみ使用し、移行完了後に削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のみ実行する必要があります。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。	
ネイバーから受信したルートのAS番号をカスタマイズする（Customize the AS number for routes received from the neighbor）	（任意）選択して、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。
ローカルAS番号（Local AS Number）	ローカル自律システム番号を入力します。有効な値は、1 ～ 4294967295 または 1.0 ～ 65535.65535 の有効な自律システム番号です。
ネイバーから受信したルートの先頭にローカルAS番号を追加しない（Do not prepend local AS number to routes received from neighbor）	（任意）選択して、ローカル AS 番号が eBGP ピアから受信したルートの先頭に追加されないようにします。

要素	説明
実際のAS番号をネイバーから受信したルート内のローカルAS番号と置き換える（Replace real AS number with local AS number in routes received from neighbor）	（任意）選択して、実際の自律システム番号をeBGPアップデートのローカル自律システム番号で置き換えます。ローカル BGP ルーティング プロセスからの自律システム番号は、追加されません。
ネイバーから学習したルートで実際のAS番号かローカルAS番号を受け入れる（Accept either real AS number or local AS number in routes received from neighbor）	（任意）（ローカル BGP ルーティングプロセスの）実際の自律システム番号を使用するか、ローカル自律システム番号を使用してピアリングセッションを確立するようにeBGP ネイバーを設定します。

[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス

[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックスを使用して、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します。

ナビゲーション パス

[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックスには、[IPv4ファミリ（IPv4 Family）] タブ （9 ページ）からアクセスできます。

関連項目

- BGP の設定 （2 ページ）
- BGP について （4 ページ）
- IPv4 Family - [全般（General）] タブ （11 ページ）
- [集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス （13 ページ）
- [Add Filter]/[Edit Filter] ダイアログボックス （15 ページ）
- [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （16 ページ）
- [Add Redistribution]/[Edit Redistribution] ダイアログボックス （28 ページ）
- [ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （29 ページ）

フィールド リファレンス

表 *7: [*ネットワークの追加/編集（*Add/Edit Network*）*]* ダイアログボックス

要素	説明
ネットワーク	BGP ルーティングプロセスでアドバタイズするネットワークを指定します。
ルート マップ	（任意）アドバタイズされるネットワークをフィルタ処理するために調べる必要があるルートマップを入力または選択します。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。 ヒント [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。

[Add Redistribution]/[Edit Redistribution] ダイアログボックス

[再配布の追加（Add Redistribution）]/[再配布の編集（Edit Redistribution）] ダイアログボックスを使用して、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します。

ナビゲーション パス

[再配布の追加（Add Redistribution）]/[再配布の編集（Edit Redistribution）] ダイアログボックスには、[IPv4ファミリ（IPv4 Family）] タブ （9 ページ）からアクセスできます。

関連項目

- BGP の設定 （2 ページ）
- BGP について （4 ページ）
- IPv4 Family - [全般（General）] タブ （11 ページ）
- [集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス （13 ページ）
- [集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス （34 ページ）
- [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （16 ページ）
- [ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （27 ページ）
- [ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （29 ページ）

フィールド リファレンス

表 8 : [Add Redistribution]/[Edit Redistribution] ダイアログボックス

要素	説明
ソース プロトコル	[Source Protocol] ドロップダウンリストから、どのプロトコルからルートを BGP ドメインに再配布するかを選択します。
プロセス ID（Process ID）	ルーティングプロセスの識別子を入力します。EIGRP および OSPF ルーティングプロトコルに適用されます。
メトリック（Metric）	（オプション）：再配布されているルートのメトリックを入力します。
ルート マップ	再配布されるネットワークをフィルタ処理するために調べる必要のあるルートマップを入力または選択します。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。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。
一致（Match）	1 つのルーティング プロトコルから別のルーティング プロトコルへのルート再配布に使用される条件。ルートが再配布されるには、選択した条件と一致している必要があります。次の一致条件から 1 つ以上を選択できます。これらのオプションは、OSPF が送信元プロトコルとして選択されているときにのみ有効になります。 • 内線 • 外部 1 • 外部 2 • NSSA 外部 1 • NSSA 外部 2

[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス

[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックスを使用して、条件に応じて BGP ルーティングテーブルに挿入されるルートを定義できます。

ナビゲーション パス

[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックスには、[IPv4ファミリ（IPv4 Family）] タブ （9 ページ）からアクセスできます。

関連項目

- BGP の設定 （2 ページ）
- BGP について （4 ページ）
- IPv4 Family - [全般（General）] タブ （11 ページ）
- [集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス （13 ページ）
- [Add Filter]/[Edit Filter] ダイアログボックス （15 ページ）
- [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （16 ページ）
- [ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （27 ページ）
- [Add Redistribution]/[Edit Redistribution] ダイアログボックス （28 ページ）

フィールド リファレンス

表 *9 : [*ルートインジェクションの追加/編集（*Add/Edit Route Injection***）*]* ダイアログボックス**

要素	説明
インジェクトマップ	ローカル BGP ルーティングテーブルに挿入するプレフィックスを指定するルートマップを入力または選択します。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。
存在マップ	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を入力または選択します。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。

要素	説明
挿入されたルートは、集約ルートの属性を継承します。	挿入されたルートが集約ルートの属性を継承するように設定します。

[IPv6ファミリ（IPv6 Family）] タブ

[BGP] ページの [IPv6 ファミリ（IPv6 Family）] タブを使用して、BGP の IPv6 設定を有効にして設定します。

ナビゲーション パス

[BGP] ページから [IPv6 ファミリ（IPv6 Family）] タブにアクセスできます。[BGP] ページの詳細については、BGP の設定 （2 ページ）を参照してください。

関連項目

- BGP について （4 ページ）
- [General] タブ （7 ページ）

フィールド リファレンス

表 *10 : IPv6* ファミリ：*[*集約アドレス（*Aggregate Address*）*]* タブ

要素	説明
[IPv6 ファミリの有効化（Enable IPv6 Family）]	標準の 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の設定を有効にします。
一般	このパネルを使用して、一般的な IPv6 設定を指定します。これらの定義の詳細については、[IPv6 ファミリ（IPv6 Family）] : [全般（General）] タブ （32 ページ）を参照してください。
[Aggregate Address]	このパネルを使用して、特定のルートから 1 つのルートへの集約を定義します。 [Aggregate Timer] フィールドで、集約タイマーの値（秒）を指定します。有効な値は、0 または 6 ～ 60 の値です。デフォルト値は 30 です。 これらの定義の詳細については、[集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス （34 ページ）を参照してください。

要素	説明
ネイバー	このパネルを使用して、BGP ネイバーとネイバーの設定を定義します。これらの定義の詳細については、[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （36 ページ）を参照してください。
ネットワーク	このパネルを使用して、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します。これらの定義の詳細については、[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （46 ページ）を参照してください。
再配布	このパネルを使用して、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します。これらの定義の詳細については、[Add Redistribution]/[Edit Redistribution] ダイアログボックス （47 ページ）を参照してください。
ルートの挿入	このパネルを使用して、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します。これらの定義の詳細については、[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （48 ページ）を参照してください。

[IPv6 ファミリ（IPv6 Family）]：[全般（General）] タブ

全般的な IPv6 設定を指定するには、[IPv6 ファミリ（IPv6 Family）]：[全般（General）] タブを使用します。

ナビゲーション パス

[全般（General）] タブには、[BGP] ページの [IPv6ファミリ（IPv6 Family）] タブからアクセスできます。[IPv6ファミリ（IPv6 Family）] タブの詳細については、[IPv6ファミリ（IPv6 Family）] タブ （31 ページ）を参照してください。

関連項目

- BGP の設定 （2 ページ）
- BGP について （4 ページ）

フィールド リファレンス

表 *11 : [IPv6* ファミリ（*IPv6 Family*）*]*：*[*全般（*General*）*]* タブ

要素	説明
スキャン間隔	ネクストホップの検証用に BGP ルータのスキャン間隔（秒）を入力します。有効な値は 5 ～ 60 秒です。デフォルト値は 60 です。
ルートと同期	

要素	説明
デフォルトルートの生成	（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。
非アクティブのルートのアドバタイズ	（任意）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をアドバタイズします。
BGP と内部ゲートウェイプロトコル（IGP）システム間の同期	BGP と内部ゲートウェイプロトコル（IGP）システム間の同期をイネーブルにします。Cisco IOS ソフトウェアが IGP を待機せずにネットワークルートをアドバタイズできるようにするには、このオプションの選択を解除します。 通常、ルートがローカルであるかIGPに存在する場合を除き、BGP スピーカーは外部ネイバーにルートをアドバタイズしません。デフォルトではBGP と IGP 間の同期はオフになっており、Cisco IOS ソフトウェアが IGP を待機せずにネットワーク ルートをアドバタイズできるようになっています。この機能により、自律システム内のルータおよびアクセス サーバーは、BGP が他の自律システムでルートを使用可能にする前にルートを確保できるようになります。自律システム内のルータが BGP を実行していない場合は、synchronization を使用します。
[iBGP の IGP への再配布（Redistribute iBGP into an IGP）]（再配布されるプレフィックスの数を制限するため、フィルタリングを使用します）	（任意）IS-IS やOSPF などの内部ゲートウェイプロトコル（IGP）への iBGP の再配布を設定します。
Administrative Route Distances	
外部	外部BGPルートのアドミニストレーティブディスタンスを指定します。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。デフォルト値は 20 です。
内線	内部BGPルートのアドミニストレーティブディスタンスを指定します。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。デフォルト値は 200 です。
ローカル（Local）	ローカルのBGPルートのアドミニストレーティブディスタンスを指定します。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。デフォルト値は 200 です。

要素	説明
マルチパス上のフォワードパケット	
パス数	（任意）ルーティングテーブルにインストール可能な Border Gateway Protocol ルートの最大数を指定します。値の範囲は 1 ～ 8 です。デフォルト値は 1 です。
IBGP のパス数	（任意）ルーティングテーブルにインストール可能な並行内部ボーダー ゲート ウェイプロトコル（IBGP）ルートの最大数を指定します。値の範囲は 1 ～ 8 です。デフォルト値は 1 です。

[集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス

[集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックスで、特定のルートの 1 つのルートへの集約を定義します。

ナビゲーション パス

[集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックスには、[IPv6ファミリ（IPv6 Family）] タブ （31 ページ）からアクセスできます。[行の追加（Add Row）]（+）ボタンをクリックするか、テーブルから行を選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。

関連項目

- BGP の設定 （2 ページ）
- BGP について （4 ページ）
- [IPv6 ファミリ（IPv6 Family）] : [全般（General）] タブ （32 ページ）
- [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （36 ページ）
- [ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （46 ページ）
- [Add Redistribution]/[Edit Redistribution] ダイアログボックス （47 ページ）
- [ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （48 ページ）

フィールド リファレンス

表 *12 : [*集約アドレスの追加/編集（*Add/Edit Summary Address*）*]* ダイアログボックス

要素	説明
ネットワーク	IP アドレスを入力するか、目的のネットワーク/ホストオブジェクトを入力または選択します。

要素	説明
属性マップ	（オプション）集約ルートの属性の設定に使用されるルート マップを入力または選択します。 ヒント [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。
アドバタイズマップ（Advertise Map）	（オプション）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を入力または選択します。 ヒント [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。
抑制マップ（Suppress Map）	（オプション）抑制するルートの選択に使用されるルートマップを入力または選択します。 ヒント [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。
AS 設定パス情報の生成（Generate AS Set Path Information）	自律システム設定パス情報の生成を有効にします。
アップデートからのすべてのより具体的なルートをフィルタ処理（Filter all more-specific routes from updates）	アップデートからのすべてのより具体的なルートをフィルタ処理します。

[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス

[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックスを使用して、BGP ネイバーとネイバーの設定を定義します。

ナビゲーション パス

[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックスには、[IPv6ファミリ（IPv6 Family）] タブ （31 ページ）からアクセスできます。[行の追加（Add Row）]（+）ボタンをクリックするか、テーブルから行を選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。

関連項目

- BGP の設定 （2 ページ）
- BGP について （4 ページ）
- [IPv6 ファミリ（IPv6 Family）] : [全般（General）] タブ （32 ページ）
- [集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス （34 ページ）
- [ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （46 ページ）
- [Add Redistribution]/[Edit Redistribution] ダイアログボックス （47 ページ）
- [ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （48 ページ）

フィールド リファレンス

表 *13 : [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス*

要素	説明
一般	
[IPアドレス（IP Address）]	BGP ネイバーの IP アドレスを入力します。この IP アドレスは、BGP ネイバー テーブルに追加されます。
リモート AS	BGP ネイバーが属する自律システムを入力します。

要素	説明
更新の送信元（Update Source） （ASA 9.19.1+ のみ）	（任意）BGP ネイバーシップの送信元インターフェイスを更新するには、適切なインターフェイスを選択します。 ヒント [選択（Select）] をクリックして、インターフェイスを選択できるインターフェイスセレクタを開きます。インターフェイスの詳細については、使用可能なインターフェイス タイプを参照してください。 （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。
アドレスファミリの有効化（Enable Address Family）	（任意）BGP ネイバーとの通信を有効にします。
ネイバーを管理的にシャットダウンする（Shutdown neighbor administratively）	（任意）ネイバーまたはピアグループを無効にします。
ネイバーごとのBGPグレースフルリスタートの設定（Configure Graceful Restart per neighbor） （ASA 9.3.1 以降のみ）	（任意）ネイバーのボーダー ゲートウェイ プロトコル（BGP）グレースフルリスタート機能の設定を有効にします。このオプションを選択した後、[グレースフルリスタート（フェールオーバーまたはスパンドクラスタモードで使用）（Graceful Restart (Use in failover or spanned cluster mode)）] オプションを使用して、このネイバーに対してグレースフルリスタートを有効にするか、無効にするかを指定する必要があります。
[グレースフルリスタート（Graceful Restart）]（フェールオーバーまたはスパンドクラスタモードで使用） （ASA 9.3.1 以降のみ）	（任意）ネイバーのボーダー ゲートウェイ プロトコル（BGP）グレースフルリスタート機能を有効にします。
説明	（任意）BGP ネイバーの説明を入力します。
フォールオーバーBFD（fall-over BFD）	(オプション) BGP ネイバーのフォールオーバーに対する BFD サポートを有効にします。

要素	説明
BFDホップ（BFD-Hop）	（任意）BFD の送信元と宛先の間に単一の IP ホップがあるか、複数の IP ホップがあるかを指定します。
フィルタリング	
アクセスリストを使用してルートをフィルタ処理する（Filter routes using an access list）	（任意）適切な着信または発信アクセス制御リストを入力または選択して、BGP ネイバー情報を配布します。
ルートマップを使用してルートをフィルタ処理する（Filter routes using route map）	（任意）適切な着信または発信ルートマップを入力または選択して、着信または発信ルートにルートマップを適用します。 ヒント [選択（Select）]をクリックして、ルートマップオブジェクトを選択できる[ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。
プレフィックスリストを使用してルートをフィルタ処理する（Filter routes using a Prefix list）	（任意）適切な着信または発信プレフィックスリストを入力または選択して、BGP ネイバー情報を配布します。 ヒント [選択（Select）]をクリックして、プレフィックスリストオブジェクトを選択できるプレフィックスリストオブジェクトセレクタを開きます。オブジェクト プレフィックス リスト オブジェクト セレクタから新しいオブジェクトを作成することもできます。詳細については、[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （235 ページ）を参照してください。
ASパスフィルタを使用してルートをフィルタ処理する（Filter routes using AS Path filter）	（任意）適切な着信または発信 AS パスフィルタを入力または選択して、BGP ネイバー情報を配布します。 ヒント [選択（Select）] をクリックして、AS パスオブジェクトを選択できる AS パスオブジェクトセレクタを開きます。ASパスオブジェクトセレクタから新しいASパスオブジェクトを作成することもできます。詳細については、[ASパスオブジェクトの追加（（Add AS Path Object））]/[ASパスオブジェクトの編集（Edit AS Path Object）] ダイアログボックス （242 ページ）を参照してください。

要素	説明
ネイバーから許可されるプレフィックスの数を制限する（Limit the number of prefixes allowed from the neighbor）	（任意）選択して、ネイバーから受信できるプレフィックスの数を制御ます。 • [最大プレフィックス数（Maximum Prefixes）] フィールドに、特定のネイバーからの許可される最大プレフィックス数を入力します。 • [しきい値レベル（Threshold Level）] フィールドに、ルータが警告メッセージの生成を開始するパーセンテージ（最大数に対する割合）を入力します。有効な値は1～100の整数です。デフォルト値は 75 です。 • （任意）[ピアから受信したプレフィックスの制御（Control prefixes received from the peer）] チェックボックスをオンにし、ピアから受信したプレフィックスに対する追加の制御を指定します。次のいずれかを実行します。 • プレフィックス数の制限値に到達したときに BGP ネイバーを停止するには、[プレフィックス数の制限値を超えたときにピアリングを停止する（Terminate peering when prefix limit is exceeded）] を選択します。[Restart interval] フィールドで、BGP ネイバーが再起動するまでの時間を指定します。 • 最大プレフィックス数の制限値を超えたときにログメッセージを生成するには、[プレフィックス数の制限値を超えたときに警告メッセージのみを表示する（Give only warning message when prefix limit is exceeded）] を選択します。この場合、BGP ネイバーは終了しません。
ルート	
アドバタイズメント間隔	BGP ルーティング更新が送信される最小間隔（秒単位）を入力します。有効な値は、1 ～ 600 です。
アウトバウンドルーティング更新からプライベートAS番号を削除します。	（任意）プライベートAS番号をアウトバウンドルートでアドバタイズしないようにします。

要素	説明
デフォルトルートの生成（Generate Default route）	（任意）選択して、ネイバーへのデフォルトルート 0.0.0.0 の送信をローカルルータに許可して、デフォルトルートとして使用します。[ルートマップ（Route map）] フィールドで、ルート 0.0.0.0 が条件に応じて注入されるように許可するルート マップを入力または選択します。 ヒント [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。
ルートの条件付きアドバタイズ（Conditionally Advertised Routes）	（任意）条件付きでアドバタイズされるルートを追加または編集するには、[行の追加（Add Row）]（+）ボタンをクリックするか、テーブル内の行を選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。 [アドバタイズ対象ルートの追加/編集（Add/Edit Advertised Route）] ダイアログボックスで、次の手順を実行します。 • [選択（Select）] をクリックして [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。このセレクタから、存在マップまたは非存在マップの条件が満たされた場合にアドバタイズされるルートマップを選択できます。ルートマップの詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。 • 次のいずれかを実行します。 • [存在マップの設定（Set Exist Map）] を選択し、[ルートマップオブジェクトセレクタ（Route Map Object Selector）] からルートマップを選択します。このルートマップは、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ます。 • [非存在マップ（Non-Exist Map）] を選択し、[ルートマップオブジェクトセレクタ（Route Map Object Selector）] からルートマップを選択します。このルートマップは、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ます。

要素	説明
タイマー	
BGPピアにタイマーを設定する（Set timers for the BGP peer）	（任意）選択して、キープアライブ頻度、ホールド時間、最小ホールド時間を設定します。
キープアライブ間隔（Keepalive Interval）	ASA がキープアライブ メッセージをネイバーに送信する頻度（秒）を有効な値は、0 ～ 65535 です。デフォルト値は 60 秒です。
保留時間（Hold Time）	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 が宣言するまでの間隔（秒単位）を入力します。有効な値は、0 ～ 65535 です。デフォルト値は 180 秒です。
Min Hold Time	（任意）キープアライブメッセージを受信できずに、ピアがデッドであると ASA が宣言するまでの最小間隔（秒単位）を入力します。有効な値は、0 ～ 65535 です。デフォルト値は 0 秒です。
詳細設定（Advanced）	
Enable Authentication	（任意）選択して、2 つの BGP ピア間の TCP 接続で MD5 認証を有効にします。 • [暗号化を有効にする（Enable Encryption）] ドロップダウンリストから暗号化タイプを選択します。 • パスワードを [Password] フィールドに入力します。[Confirm] フィールドにパスワードを再入力します。 パスワードは大文字と小文字を区別し、service password-encryption コマンドが有効な場合は最大 25 文字、service password-encryption コマンドが有効でない場合は最大 81 文字まで指定できます。最初の文字を数値にはできません。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） 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。
コミュニティ属性をこのネイバーに送信します	（任意）コミュニティ属性を BGP ネイバーに送信する必要があることを指定します。
ネイバーのネクストホップとしてASAを使用する（Use ASA as next hop for neighbor）	（任意）選択して、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ルータを設定します。

要素	説明
接続検証の無効化（Disable connection verification）	（任意）選択して、シングルホップで到達可能だが、ループバックインターフェイス上に設定されている、あるいは直接接続されない IP アドレスで設定されている eBGP ピアリングセッションの接続検証プロセスを無効にします。 このコマンドが必要になるのは、neighbor ebgp-multihop コマンドで TTL 値を 1 に設定している場合だけです。シングル ホップ eBGP ピアのアドレスに到達できる必要があります。neighbor update-source コマンドを使用して、BGP ルーティングプロセスでピアリングセッションにループバック インターフェイスを使用できるように設定する必要があります。 オフ（デフォルト）にすると、シングルホップ eBGP ピアリングセッション（TTL=254）について、BGP ルーティング プロセスで接続が検証され、eBGP ピアが同じネットワーク セグメントに直接接続されているかどうか確認されます。ピアが同じネットワーク セグメントに直接接続されていない場合、ピアリングセッションは確立されません。
直接接続されていないネイバーとの接続を許可する（Allow connections with neighbor that is not directly connected）	選択して、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、そのピアへの BGP 接続を試みます。 （オプション）[TTL hops] フィールドに存続可能時間を入力します。有効な値は、1 ～ 255 です。 （注） この機能は、シスコテクニカルサポート担当者の指示のもとでのみ使用してください。ルートが一定でないことによるループの発生を回避するために、マルチホップピアのルートがデフォルトルート（0.0.0.0）だけの場合はマルチホップは確立されません。

要素	説明
ネイバーへのTTLホップ数を制限する（Limit number of TTL hops to neighbor）	

要素	説明
	BGP ピアリングセッションを保護するには、このオプションを選択します。[TTL hops] フィールドに、eBGP ピアを区切るホップの最大数を入力します。有効な値は、1 ～ 254 です。 この機能は、CPU 利用率に基づく攻撃から BGP ピアリングセッションを保護するための簡単なセキュリティメカニズムを提供します。この種の攻撃は、通常、パケット ヘッダーの送信元と宛先の IP アドレスを偽造した大量の IP パケットでネットワークをあふれさせてネットワークをディセーブルにしようとする典型的な力任せのサービス拒否（DoS）攻撃です。 この機能は、TTL カウントがローカルの設定値以上である IP パケットだけを受け入れるという IP パケットの設計上の動作を利用したものです。IP パケットの TTL カウントを完全に偽造することは一般には不可能であると考えられます。内部の送信元ネットワークまたは宛先ネットワークにアクセスしない限り、信頼できるピアからの TTL カウントに完全に一致するパケットを偽造することはできません。 この機能は、参加している各ルータで設定する必要があります。この機能では、eBGP セッションが受信方向だけ保護され、送信 IP パケットまたはリモート ルータは影響を受けません。この機能がイネーブルの場合、BGP は、IP パケット ヘッダーの TTL 値がピアリング セッション用に設定された TTL 値以上の場合だけセッションを確立または維持します。この機能は BGP ピアリング セッションには影響しません。この機能がイネーブルの場合でも、キープアライブ パケットを受信しなければピアリングセッションは期限切れになります。受信パケットの TTL 値が、ローカルで設定された値未満の場合、パケットはサイレントに廃棄され、インターネット制御メッセージ プロトコル（ICMP）メッセージは生成されません。これは設計された動作です。偽造パケットへの応答は必要ありません。 この機能の効果を最大化するには、ローカルネットワークと外部ネットワーク間のホップ数が一致するように hop-count の値を正確に設定する必要があります。また、この機能をマルチホップ ピアリング セッションに対して設定する場合は、パスがそれぞれで異なる点についても考慮する必要があります。 このコマンドの設定には、次の制限が適用されます。 • この機能は、内部 BGP（iBGP）ピアではサポートされません。 • 大きい直径のマルチホップ ピアリングでは、この機能の効果は下がります。大きい直径のピアリング用に設定された BGP ルータに対する CPU 利用率に基づく攻撃の場合は、影

要素	説明
	響を受けたピアリング セッションをシャットダウンして、この攻撃に対処する必要がある場合があります。 • この機能は、ネットワーク内部が損なわれているピアからの攻撃には効果的ではありません。この制約事項には、送信元ネットワークと宛先ネットワークの間のネットワーク セグメント上のピアも含まれます。
TCPパスMTUディスカバリを使用する（Use TCP Path MTU Discovery）	（任意）選択して、BGP セッションの TCP トランスポートセッションを有効にします。
TCPトランスポートモード（TCP transport mode）	ドロップダウンリストから TCP 接続モードを選択します。オプションは [デフォルト（Default）]、[アクティブ（Active）]、または [パッシブ（Passive）] です。
重量	（任意）BGP ネイバー接続の重みを入力します。
BGPバージョン（BGP Version）	ドロップダウンリストから、ASA が受け入れる BGP バージョンを選択します。[4 のみ（4-Only）] に設定すると、指定されたネイバーとの間でバージョン4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。
移行 （注） このカスタマイズは、AS 移行にのみ使用し、移行完了後に削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のみ実行する必要があります。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。	
ネイバーから受信したルートのAS番号をカスタマイズする（Customize the AS number for routes received from the neighbor）	（任意）選択して、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。
ローカルAS番号（Local AS Number）	ローカル自律システム番号を入力します。有効な値は、1 ～ 4294967295 または 1.0 ～ 65535.65535 の有効な自律システム番号です。
ネイバーから受信したルートの先頭にローカルAS番号を追加しない（Do not prepend local AS number to routes received from neighbor）	（任意）選択して、ローカル AS 番号が eBGP ピアから受信したルートの先頭に追加されないようにします。

要素	説明
実際のAS番号をネイバーから受信したルート内のローカルAS番号と置き換える（Replace real AS number with local AS number in routes received from neighbor）	（任意）選択して、実際の自律システム番号をeBGPアップデートのローカル自律システム番号で置き換えます。ローカルBGPルーティング プロセスからの自律システム番号は、追加されません。
ネイバーから学習したルートで実際のAS番号かローカルAS番号を受け入れる（Accept either real AS number or local AS number in routes received from neighbor）	（任意）（ローカルBGPルーティングプロセスの）実際の自律システム番号を使用するか、ローカル自律システム番号を使用してピアリングセッションを確立するようにeBGPネイバーを設定します。

[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス

[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックスを使用して、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します。

ナビゲーション パス

[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックスには、[IPv6ファミリ（IPv6 Family）] タブ （31 ページ）からアクセスできます。[行の追加（Add Row）]（+）ボタンをクリックするか、テーブルから行を選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。

関連項目

- BGP の設定 （2 ページ）
- BGP について （4 ページ）
- [IPv6 ファミリ（IPv6 Family）]：[全般（General）] タブ （32 ページ）
- [集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス （34 ページ）
- [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （36 ページ）
- [Add Redistribution]/[Edit Redistribution] ダイアログボックス （47 ページ）
- [ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （48 ページ）

フィールド リファレンス

表 *14 : [*ネットワークの追加/編集（*Add/Edit Network*）*]* ダイアログボックス

要素	説明
ネットワーク	BGP ルーティングプロセスでアドバタイズするネットワークを指定します。
ルート マップ	（任意）アドバタイズされるネットワークをフィルタ処理するために調べる必要があるルートマップを入力または選択します。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。 ヒント　[選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。

[Add Redistribution]/[Edit Redistribution] ダイアログボックス

[再配布の追加（Add Redistribution）]/[再配布の編集（Edit Redistribution）] ダイアログボックスを使用して、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します。

ナビゲーション パス

[再配布の追加（Add Redistribution）]/[再配布の編集（Edit Redistribution）] ダイアログボックスには、[IPv6ファミリ（IPv6 Family）] タブ （31 ページ）からアクセスできます。[行の追加（Add Row）]（+）ボタンをクリックするか、テーブルから行を選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。

関連項目

- BGP の設定 （2 ページ）
- BGP について （4 ページ）
- [IPv6 ファミリ（IPv6 Family）] : [全般（General）] タブ （32 ページ）
- [集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス （34 ページ）
- [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （36 ページ）
- [ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （46 ページ）
- [ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （48 ページ）

フィールド リファレンス

表 15 : [Add Redistribution]/[Edit Redistribution] ダイアログボックス

要素	説明
ソース プロトコル	[Source Protocol] ドロップダウンリストから、どのプロトコルからルートを BGP ドメインに再配布するかを選択します。
プロセス ID（Process ID）	ルーティングプロセスの識別子を入力します。EIGRP および OSPF ルーティングプロトコルに適用されます。
メトリック（Metric）	（オプション）：再配布されているルートのメトリックを入力します。
ルート マップ	再配布されるネットワークをフィルタ処理するために調べる必要のあるルートマップを入力または選択します。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。 ヒント [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。
一致（Match）	1 つのルーティング プロトコルから別のルーティング プロトコルへのルート再配布に使用される条件。ルートが再配布されるには、選択した条件と一致している必要があります。次の一致条件から 1 つ以上を選択できます。これらのオプションは、OSPF が送信元プロトコルとして選択されているときにのみ有効になります。 • 内線 • 外部 1 • 外部 2 • NSSA 外部 1 • NSSA 外部 2

[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス

[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックスを使用して、条件に応じて BGP ルーティングテーブルに挿入されるルートを定義できます。

ナビゲーション パス

[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックスには、[IPv6ファミリ（IPv6 Family）] タブ （31 ページ）からアクセスできます。[行の追加（Add Row）]（+）ボタンをクリックするか、テーブルから行を選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。

関連項目

- BGP の設定 （2 ページ）
- BGP について （4 ページ）
- [IPv6 ファミリ（IPv6 Family）] : [全般（General）] タブ （32 ページ）
- [集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス （34 ページ）
- [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （36 ページ）
- [ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （46 ページ）
- [Add Redistribution]/[Edit Redistribution] ダイアログボックス （47 ページ）

フィールド リファレンス

表 *16 : [ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス*

要素	説明
インジェクトマップ	ローカル BGP ルーティングテーブルに挿入するプレフィックスを指定するルートマップを入力または選択します。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。

要素	説明
存在マップ	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を入力または選択します。 ヒント [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。
挿入されたルートは、集約ルートの属性を継承します。	挿入されたルートが集約ルートの属性を継承するように設定します。

EIGRP の設定

[EIGRP] ページには、ファイアウォールデバイスで Enhanced Interior Gateway Routing Protocol（EIGRP）ルーティングを設定するための 6 つのタブ付きパネルがあります。以下のトピックでは、EIGRP の有効化および設定について詳しく説明します。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [ルーティング（Routing）] > [EIGRP]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [EIGRP]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 *17 : [EIGRP]* ページ

要素	説明
EIGRP のイネーブル化	EIGRP ルーティングプロセスを有効にするには、このチェックボックスをオンにします。
AS 番号（AS Number）	EIGRP プロセスの自律システム（AS）番号を入力します。指定できる AS 番号の範囲は 1 ～ 65535 です。
[Advanced] ボタン	EIGRP 詳細ダイアログボックス （53 ページ）を開きます。ここでは、ルータ ID、スタブルーティング、隣接関係の変更など、追加の EIGRP プロセス設定を設定できます。
[Setup] タブ	[セットアップ（Setup）] タブを使用して、EIGRP ルーティングプロセスで使用されるネットワーク、パッシブインターフェイス、デフォルトルート情報、アドミニストレーティブ ディスタンス、およびデフォルトメトリックを設定します。 詳細については、[Setup] タブ （56 ページ）を参照してください。
[フィルタルール（Filter Rules）] タブ	[フィルタルール（Filter Rules）] タブを使用してフィルタルールを定義すると、EIGRP ルーティングプロセスで受け入れ、またはアドバタイズされるルートを制御することができます。 詳細については、[フィルタルール（Filter Rules）] タブ （59 ページ）を参照してください。
[ネイバー（Neighbors）] タブ	[ネイバー（Neighbors）] タブを使用して、EIGRP ネイバーを手動で定義します。 詳細については、[Neighbors] タブ （61 ページ）を参照してください。
[再配布（Redistribution）] タブ	[再配布（Redistribution）] タブを使用して、他のルーティングプロトコルから EIGRP ルーティングプロセスにルートを再配布するためのルールを定義します。 詳細については、[Redistribution] タブ （63 ページ）を参照してください。
[サマリーアドレス（Summary Address）] タブ	[サマリーアドレス（Summary Address）] タブを使用して、スタティックに定義された EIGRP サマリーアドレスを作成します。 詳細については、[サマリーアドレス（Summary Address）] タブ （67 ページ）を参照してください。

要素	説明
[インターフェイス（Interfaces）] タブ	[インターフェイス（Interfaces）] タブを使用して、EIGRP のインターフェイスを設定します。 詳細については、 [Interfaces] タブ （69 ページ）を参照してください。

EIGRP について

EIGRP は、シスコが開発した、IGRP の拡張バージョンです。IGRP や RIP と異なり、EIGRP が定期的にルート アップデートを送信することはありません。EIGRP アップデートは、ネットワーク トポロジが変更された場合にだけ送信されます。EIGRP を他のルーティング プロトコルと区別する主な機能には、迅速なコンバージェンス、可変長サブネット マスクのサポート、部分的アップデートのサポート、複数のネットワーク レイヤ プロトコルのサポートなどがあります。バージョン 4.27 より、EIGRPv6 もサポートされます。EIGRPV6 は IPv6 サポートを使用した EIGRP の拡張機能です。

EIGRP を実行するルータでは、すべてのネイバー ルーティング テーブルが格納されているため、代替ルートに迅速に適応できます。適切なルートが存在しない場合、EIGRP はそのネイバーにクエリーを送信して代替のルートを検出します。これらのクエリーは、代替ルートが検出されるまで伝搬します。EIGRP では可変長サブネット マスクがサポートされているため、ルートはネットワーク番号の境界で自動的に集約されます。さらに、任意のインターフェイスの任意のビット境界で集約を行うように EIGRP を設定することもできます。EIGRP は定期的なアップデートを行いません。その代わり、ルートのメトリックが変更されたときだけ、部分的なアップデートを送信します。部分的アップデートの伝搬では、境界が自動的に設定されるため、その情報を必要とするルータだけがアップデートされます。これらの 2 つの機能により、EIGRP の帯域幅消費量は IGRP に比べて大幅に減少します。

ネイバー探索は、ASA が直接接続されているネットワーク上にある他のルータをダイナミックに把握するために使用するプロセスです。EIGRP ルータは、マルチキャスト hello パケットを送信して、ネットワーク上に自分が存在していることを通知します。ASA は、新しいネイバーから hello パケットを受信すると、トポロジ テーブルに初期化ビットを設定してそのネイバーに送信します。ネイバーは、初期化ビットが設定されたトポロジアップデートを受信すると、自分のトポロジ テーブルを ASA に返送します。

hello パケットはマルチキャスト メッセージとして送信されます。hello メッセージへの応答は想定されていません。ただし、スタティックに定義されたネイバーの場合は例外です。ネイバーを手動で設定した場合、そのネイバーに送信される hello メッセージはユニキャストメッセージとして送信されます。ルーティングアップデートと確認応答が、ユニキャストメッセージとして送信されます。

このネイバー関係が確立した後は、ネットワーク トポロジが変更された場合にだけ、ルーティング アップデートが交換されます。ネイバー関係は、hello パケットによって維持されます。ネイバーから受信した各 hello パケットには、保持時間が含まれています。ASA は、この時間内にそのネイバーから hello パケットを受信すると想定できます。ASA が保持時間内にそのネ

イバーからアドバタイズされた hello パケットを受信しない場合、ASA はそのネイバーを使用不能と見なします。

EIGRP プロトコルは、ネイバーの検出、ネイバーの回復、Reliable Transport Protocol（RTP）、およびルート計算に重要な DUAL を含む、4 の主要なアルゴリズム テクノロジーと 4 つの主要なテクノロジーを使用します。DUAL は、最小コストのルートだけでなく、宛先へのすべてのルートをトポロジ テーブルに保存します。最小コストのルートはルーティング テーブルに挿入されます。その他のルートは、トポロジテーブルに残ります。メインのルートに障害が発生したら、フィジブル サクセサから別のルートが選択されます。サクセサとは、宛先への最小コスト パスを持ち、パケット転送に使用される隣接ルータです。フィジビリティ計算によって、パスがルーティング ループを形成しないことが保証されます。

フィジブル サクセサがトポロジ テーブル内にない場合、必ずルート計算が発生します。ルートの再計算中、DUAL は EIGRP ネイバーにルートを求めるクエリーを送信して、次に EIGRP ネイバーがそのネイバーにクエリーを送信します。ルートのフィジブル サクセサがないルータは、到達不能メッセージを返します。

ルートの再計算中、DUAL は、ルートをアクティブとマークします。デフォルトでは、ASA は、ネイバーから応答が返ってくるのを 3 分間待ちます。ASA がネイバーから応答を受信しないと、そのルートは stuck-in-active とマークされます。トポロジ テーブル内のルートのうち、応答しないネイバーをフィジブル サクセサとして指しているものはすべて削除されます。

（注） EIGRP ネイバー関係では、GRE トンネルを使用しない IPsec トンネルの通過はサポートされていません。

関連項目

- EIGRP の設定 （50 ページ）
- EIGRPv6 の設定 （71 ページ）

EIGRP 詳細ダイアログボックス

EIGRP 詳細ダイアログボックスを使用して、ルータ ID、スタブ ルーティング、隣接関係の変更などの設定を行います。

ナビゲーション パス

[EIGRP] ページから [EIGRP詳細（EIGRP Advanced）] ダイアログボックスにアクセスできます（ EIGRP の設定 （50 ページ）を参照）。

関連項目

- EIGRP の設定 （50 ページ）

フィールド リファレンス

表 *18 : EIGRP* 詳細ダイアログボックス

要素	説明
ルータ ID（Router ID）	ルータ IDは、外部ルートの発信元ルータを識別するために使用されます。外部ルートがローカルのルータ ID で受信された場合、このルートは廃棄されます。これを回避するには、ルータ ID のグローバルアドレスを指定します。各 EIGRP ルータには、一意の値を設定する必要があります。 単一のデバイスで、[自動（Automatic）] または [IPアドレス（IP Address）] を選択します。（IP アドレスを選択すると、[アドレス（address）] フィールドが表示されます。） [自動（Automatic）] を選択すると、セキュリティアプライアンス上で最上位の IP アドレスがルータ ID として使用されます。固定ルータ ID を使用するには、[IPアドレス（IP Address）] を選択して、[ルータID（Router ID）] フィールドに IPv4 アドレスを入力します。 デバイスクラスタで、[自動（Automatic）] または [クラスタプール（Cluster Pool）] を選択します。（[クラスタプール（ Cluster Pool）] を選択すると、[IPv4プールオブジェクトID（ IPv4 Pool object ID）] フィールドが表示されます）。 [クラスタプール（Cluster Pool）] を選択した場合は、ルータの ID アドレスを提供する IPv4 プールオブジェクトの名前を入力または選択します。詳細については、を参照してください。

要素	説明
Stub	ASA を EIGRP スタブ ルータとしてイネーブル化し、設定することができます。スタブルーティングは、ASA でメモリと[IPv4プールの追加または編集（Add or Edit IPv4 Pool）] ダイアログボックスの処理要件を減らす場合があります。ASA をスタブ ルータとして設定すると、ローカル以外のトラフィックがすべて配布ルータに転送されるようになり、完全な EIGRP ルーティング テーブルを維持する必要がなくなります。一般に、配布ルータからスタブ ルートに送信する必要があるのは、デフォルト ルートだけです。 スタブ ルータから配布ルータには、指定されたルートだけが伝搬されます。スタブ ルータである ASA は、サマリー、接続されているルート、再配布されたスタティック ルート、外部ルート、および内部ルートに対するクエリーすべてに、応答として「inaccessible」というメッセージを返します。ASA がスタブとして設定されているときは、自身のスタブ ルータとしてのステータスを報告するために、特殊なピア情報パケットをすべての隣接ルータに送信します。スタブ ステータスの情報を伝えるパケットを受信したネイバーはすべて、スタブ ルータにルートのクエリーを送信しなくなり、スタブ ピアを持つルータはそのピアのクエリーを送信しなくなります。スタブ ルータが正しいアップデートをすべてのピアに送信するには、配布ルータが必要です。 ASA を EIGRP スタブルーティングプロセスとして有効にするには、次の EIGRP スタブルーティングプロセスから 1 つ以上を選択します。 • Receive only：隣接ルータからルート情報を受信しても、その隣接ルータにルート情報を送信しないために、EIGRP スタブルーティングプロセスを設定します。このオプションを選択する場合は、他のスタブ ルーティング オプションを選択できません。 • [接続済み（Connected）]：接続済みルートをアドバタイズします。 • [再配布済み（Redistributed）]：再配布済みルートをアドバタイズします。 • [スタティック（Static）]：スタティックルートをアドバタイズします。 • [サマリ - （Summary）]：サマリールートをアドバタイズします。

要素	説明
隣接関係の変更	これらのオプションでは、隣接関係の変更が発生したときに送信される syslog メッセージを指定します。 • [ログネイバーの変更（Log Neighbor Changes）]：EIGRP ネイバーの隣接関係に関する変更のロギングを有効にします。このオプションは、デフォルトで選択されます。 • [ログネイバーの警告（Log Neighbor Warnings）]：EIGRP ネイバーの警告メッセージのロギングを有効にします。このオプションは、デフォルトで選択されます。 （任意）ネイバー警告メッセージの反復間隔（秒数）。有効値は 1 ～ 65535 です。この間隔内に警告が繰り返し発生した場合、それらの警告はログに記録されません。

[Setup] タブ

[EIGRP] ページの [セットアップ（Setup）] タブを使用して、EIGRP ルーティングプロセスで使用されるネットワーク、パッシブインターフェイス、デフォルトルート情報、アドミニストレーティブ ディスタンス、およびデフォルトメトリックを設定します。

ナビゲーション パス

[EIGRP] ページから [セットアップ（Setup）] タブにアクセスできます。詳細については、EIGRP の設定 （50 ページ）を参照してください。

関連項目

- EIGRP の設定 （50 ページ）
- EIGRP について （52 ページ）
- [Setup] タブ （56 ページ）
- [フィルタルール（Filter Rules）] タブ （59 ページ）
- [Neighbors] タブ （61 ページ）
- [Redistribution] タブ （63 ページ）
- [サマリーアドレス（Summary Address）] タブ （67 ページ）
- [Interfaces] タブ （69 ページ）

フィールド リファレンス

表 *19 : EIGRP*：*[*セットアップ（*Setup*）*]* タブ

要素	説明
自動サマリー	自動ルート集約を有効にするには、このチェックボックスをオンにします。自動サマリーは、9.2.1 より前の ASA バージョンではデフォルトで有効になっており、ASA 9.2(1) 以降ではデフォルトで無効になっています。 有効になっている場合、EIGRP ルーティングプロセスは、ネットワーク番号の境界で集約を行います。このことは、不連続ネットワークがある場合にルーティングの問題の原因となることがあります。 たとえば、ネットワーク 192.168.1.0、192.168.2.0、192.168.3.0 が接続されているルータがあり、それらのネットワークがすべて EIGRP に参加していると、EIGRP ルーティング プロセスはそれらのルートに対しサマリーアドレス 192.168.0.0 を作成します。さらにネットワーク 192.168.10.0 と 192.168.11.0 が接続されているルータがこのネットワークに追加され、それらのネットワークが EIGRP に参加すると、これらもまた 192.168.0.0 として集約されます。トラフィックが誤った場所にルーティングされる可能性をなくすために、競合するサマリーアドレスを作成するルータでの自動ルート集約をディセーブルにする必要があります。
ネットワーク	EIGRP ルーティングプロセスに参加するネットワークの IP アドレスを入力します。 **ヒント** [選択（Select）] をクリックすると、ネットワーク/ホストオブジェクトのリストからネットワークを選択できます。
パッシブ インターフェイス	1 つ以上のインターフェイスを受動インターフェイスとして設定できます。EIGRP の場合、受動インターフェイスではルーティング アップデートが送受信されません。 デフォルトでは、そのインターフェイスでルーティングが有効になると、アクティブルーティング（ルーティング更新の送受信）に対してすべてのインターフェイスが有効になります。 パッシブインターフェイスを設定するには、次のいずれかを実行します。 • そのインターフェイスに対してルーティングが有効な場合、アクティブルーティング（ルーティング更新の送受信）に対してすべてのインターフェイスを有効にするには、[なし（None）] を選択します。 • すべてのインターフェイスをパッシブとして設定するには、[すべてのインターフェイス（All Interfaces）] を選択します。 • 特定のインターフェイスをパッシブとして設定するには、[指定されたインターフェイス（Specified Interfaces）] を選択し、パッシブにするインターフェイスを入力または選択します。

要素	説明
デフォルトのルート情報	EIGRP アップデート内のデフォルト ルート情報の送受信を制御できます。デフォルトでは、デフォルト ルートが送信され、受け入れられます。デフォルト情報の受信を禁止するように ASA を設定すると、候補のデフォルト ルート ビットが受信ルート上でブロックされます。デフォルト情報の送信を禁止するように ASA を設定すると、アドバタイズされるルートのデフォルト ルート ビット設定が無効になります。 • デフォルトのルート情報を受け入れる：外部のデフォルト ルーティング情報を受け入れるように EIGRP を設定します。任意で、デフォルト ルート情報を受信するときに許可するネットワークと許可しないネットワークを定義する標準アクセス リストを指定できます。 • デフォルトのルート情報を送信する：外部ルーティング情報をアドバタイズするように EIGRP を設定します。任意で、デフォルト ルート情報を送信するときに許可するネットワークと許可しないネットワークを定義する標準アクセス リストを指定できます。
アドミニストレーティブ ディスタンス（Administrative Distance）	各ルーティング プロトコルには、他のルーティング プロトコルと異なるアルゴリズムに基づいたメトリックがあるため、異なるルーティング プロトコルによって生成された同じ宛先への 2 つのルートのいずれが「最適パス」であるかは、必ずしも判別できません。アドミニストレーティブ ディスタンスは、2 つの異なるルーティング プロトコルから同じ宛先への異なるルートが複数存在する場合に、ASA がベスト パスの選択に使用するルート パラメータです。 ASA で複数のルーティング プロトコルが実行されている場合、distance eigrp コマンドを使用して、EIGRP ルーティング プロトコルが検出するルートのデフォルト アドミニストレーティブ ディスタンスを、他のルーティング プロトコルと関連付けて調整できます。 [Internal Distance]：EIGRP 内部ルートのアドミニストレーティブ ディスタンスです。内部ルートとは、同じ自律システム内の別のエンティティから学習されるルートです。有効な値は、1 ～ 255 です。デフォルトは 90 です。 [External Distance]：EIGRP 外部ルートのアドミニストレーティブ ディスタンスです。外部ルートとは、最適パスを自律システムの外部にあるネイバーから学習するルートです。有効値の範囲は 1 ～ 255 で、デフォルト値は 170 です。

要素	説明
デフォルトメトリック	EIGRP ルーティングプロセスに再配布されるルートのデフォルトのメトリックを定義できます。 • [帯域幅（Bandwidth）]：ルートの最小帯域幅（キロビット/秒）。有効値の範囲は 1 ～ 4294967295 です。 • [遅延時間（Delay Time）]：ルートの遅延（10 マイクロ秒）。有効値の範囲は、0 ～ 4294967295 です。 • [信頼性（Reliability）]：0 ～ 255 の数値で表現した、パケットが正常に伝送される見込み。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを表します。 • [ローディング（Loading）]：ルートの実効帯域幅。有効値の範囲は 1 ～ 255 で、255 は負荷が 100 % であることを示します。 • [MTU]：パスの最大伝送単位の最小許容値。有効値の範囲は 1 ～ 65535 です。

[フィルタルール（Filter Rules）] タブ

[フィルタルール（Filter Rules）] タブには、EIGRP ルーティングプロセスに設定されているルート フィルタリング ルールを表示する [フィルタルール（Filter Rules）] テーブルが含まれています。フィルタ ルールによって、EIGRP ルーティング プロセスで受け入れまたはアドバタイズされるルートを制御できます。

ナビゲーション パス

[EIGRP] ページから [フィルタルール（Filter Rules）] タブにアクセスできます。詳細については、EIGRP の設定 （50 ページ）を参照してください。

関連項目

• [EIGRPフィルタルールの追加（Add EIGRP Filter Rule）]/[EIGRPフィルタルールの編集（Edit EIGRP Filter Rule）] ダイアログボックス （60 ページ）
• EIGRP の設定 （50 ページ）
• EIGRP について （52 ページ）
• [Setup] タブ （56 ページ）
• [Neighbors] タブ （61 ページ）
• [Redistribution] タブ （63 ページ）
• [サマリーアドレス（Summary Address）] タブ （67 ページ）

- [Interfaces] タブ （69 ページ）

フィールド リファレンス

表 *20 : EIGRP* : *[フィルタルール（Filter Rules）] タブ*

要素	説明
方向（Direction）	フィルタルールの方向： • [インバウンド（Inbound）]：このルールは、着信 EIGRP ルーティング アップデートからのデフォルトルート情報をフィルタリングします。 • [アウトバウンド（Outbound）]：このルールは、発信 EIGRP ルーティングアップデートからのデフォルトルート情報をフィルタリングします。
インターフェイス	（オプション）フィルタルールが適用されるインターフェース。
プロトコル	フィルタリングされるルーティングプロトコル：[BGP]、[接続（Connected）]、[OSPF]、[RIP]、または [スタティック（Static）]。
ACL	標準 IP アクセス リスト名。このリストは、受信されるネットワークとルーティング アップデートで抑制されるネットワークを定義します。

[EIGRPフィルタルールの追加（Add EIGRP Filter Rule）]/[EIGRPフィルタルールの編集（Edit EIGRP Filter Rule）] ダイアログボックス

[EIGRPフィルタルールの追加（Add EIGRP Filter Rule）]/[EIGRPフィルタルールの編集（Edit EIGRP Filter Rule）] ダイアログボックスを使用して、既存のフィルタルールテーブルに新しいフィルタルールを追加するか、または既存のフィルタルールを変更します。

ナビゲーション パス

[EIGRPフィルタルールの追加（Add EIGRP Filter Rule）]/[EIGRPフィルタルールの編集（Edit EIGRP Filter Rule）] ダイアログボックスには、[フィルタルール（Filter Rules）] タブ （59 ページ）からアクセスできます。

関連項目

- EIGRP の設定 （50 ページ）
- EIGRP について （52 ページ）
- [フィルタルール（Filter Rules）] タブ （59 ページ）

フィールド リファレンス

表 *21 : [EIGRP*フィルタルールの追加（*Add EIGRP Filter Rule***）*]/[EIGRP*フィルタルールの編集（***Edit EIGRP Filter Rule***）*]* ダイアログボックス**

要素	説明
EIGRP フィルタの方向	フィルタルールの方向を指定します。 • [インバウンド（Inbound）]：このルールは、着信 EIGRP ルーティングアップデートからのデフォルトルート情報をフィルタリングします。 • [アウトバウンド（Outbound）]：このルールは、発信 EIGRP ルーティングアップデートからのデフォルトルート情報をフィルタリングします。
タイプ（Type）	フィルタルールのタイプを指定します。 • （任意）インターフェイス：ルーティングアップデートを適用するインターフェイスを指定します。インターフェイスを指定すると、アクセスリストはそのインターフェイスのルーティングアップデートにのみ適用されます。インターフェイスが指定されていない場合、アクセスリストはすべてのアップデートに適用されます。 • （任意）ルーティングプロトコル：アウトバウンド EIGRP ルーティングアップデートでは、フィルタリングするルーティングプロトコル（BGP、接続済み、OSPF、RIP またはスタティック）を選択します。 ルーティングプロトコル ID：ルーティングプロセスの識別子を入力します。BGP および OSPF ルーティングプロトコルに適用されます。
ACL	受信されるネットワークとルーティングアップデートで抑制されるネットワークを定義するアクセス制御リストを選択します。

[Neighbors] タブ

[ネイバー（Neighbors）] タブには、スタティックネイバーを定義できるネイバーテーブルが含まれています。手動で EIGRP ネイバーを定義すると、hello パケットはユニキャスト メッセージとしてそのネイバーに送信されます。

ナビゲーション パス

[EIGRP] ページから [ネイバー（Neighbors）] タブにアクセスできます。詳細については、EIGRP の設定 （50 ページ）を参照してください。

関連項目

- [EIGRPネイバーの追加/編集（Add/Edit EIGRP Neighbor）] ダイアログボックス （62 ページ）

- EIGRP の設定 （50 ページ）
- EIGRP について （52 ページ）
- [Setup] タブ （56 ページ）
- [フィルタルール（Filter Rules）] タブ （59 ページ）
- [Redistribution] タブ （63 ページ）
- [サマリーアドレス（Summary Address）] タブ （67 ページ）
- [Interfaces] タブ （69 ページ）

フィールド リファレンス

表 *22 : EIGRP* : *[ネイバー（Neighbors）] タブ*

要素	説明
インターフェイス（Interface）	ネイバーが使用可能なインターフェイス。
ネイバー	スタティック ネイバーの IP アドレス。

[EIGRPネイバーの追加/編集（Add/Edit EIGRP Neighbor）] ダイアログボックス

EIGRP hello パケットはマルチキャスト パケットとして送信されます。EIGRP ネイバーが、トンネルなど、非ブロードキャスト ネットワークを越えた場所にある場合、手動でネイバーを定義する必要があります。手動で EIGRP ネイバーを定義すると、hello パケットはユニキャスト メッセージとしてそのネイバーに送信されます。

（注） インターフェイスに対して passive-interface コマンドを設定すると、そのインターフェイスではすべての発着信ルーティング更新および hello メッセージが表示されなくなります。EIGRP ネイバーとの隣接関係は、パッシブとして設定されるインターフェイス経由で確立および維持できません。

スタティックネイバーを定義するか、または既存のスタティックネイバーの情報を変更するには、[EIGRPネイバーの追加/編集（Add/Edit EIGRP Neighbor）] ダイアログボックスを使用します。

ナビゲーション パス

[EIGRPネイバーの追加/編集（Add/Edit EIGRP Neighbor）] ダイアログボックスには、[Neighbors] タブ （61 ページ）からアクセスできます。

関連項目

- EIGRP の設定 （50 ページ）

- EIGRP について （52 ページ）
- [Neighbors] タブ （61 ページ）

フィールド リファレンス

表 *23 : [EIGRP*ネイバーの追加/編集（*Add/Edit EIGRP Neighbor*）*]* ダイアログボックス

要素	説明
インターフェイス（Interface）	ネイバーが使用可能なインターフェイス。 ヒント　[選択（Select）] をクリックして、インターフェイスオブジェクトのリストからインターフェイスを選択できます。
ネイバー	スタティック ネイバーの IP アドレス。 ヒント　[選択（Select）] をクリックすると、ホストオブジェクトのリストからネイバーを選択できます。

[Redistribution] タブ

[再配布（Redistribution）] タブを使用して、他のルーティングプロトコルから EIGRP ルーティングプロセスにルートを再配布するためのルールを定義します。

ナビゲーション パス

[EIGRP] ページから [再配布（Redistribution）] タブにアクセスできます。詳細については、EIGRP の設定 （50 ページ）を参照してください。

関連項目

- [EIGRP再配布の追加/編集（Add/Edit EIGRP Redistribution）] ダイアログボックス （65 ページ）
- EIGRP の設定 （50 ページ）
- EIGRP について （52 ページ）
- [Setup] タブ （56 ページ）
- [フィルタルール（Filter Rules）] タブ （59 ページ）
- [Neighbors] タブ （61 ページ）
- [サマリーアドレス（Summary Address）] タブ （67 ページ）
- [Interfaces] タブ （69 ページ）

フィールド リファレンス

表 *24 : EIGRP* : *[*再配布（*Redistribution***）*]* タブ**

要素	説明
プロトコル	ルートの再配布元の送信元プロトコル。 • [BGP]：BGP ルーティングプロセスによって検出されたルートを EIGRP に再配布します。 • [RIP]：RIP ルーティングプロセスによって検出されたルートを EIGRP に再配布します。 • [Static]：スタティックルートを EIGRP ルーティングプロセスに再配布します。ネットワーク設定の範囲内にあるスタティック ルートは EIGRP に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。 • [Connected]：接続されたルート（インターフェイス上で IP アドレスをイネーブルにすることによって自動的に確立されるルート）を EIGRP ルーティングプロセスに再配布します。ネットワーク設定の範囲内にある接続済みルートは EIGRP に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。 • [OSPF]：OSPF ルーティングプロセスで検出されたルートを EIGRP に再配布します。このプロトコルを選択すると、このダイアログボックスの [Match] のオプションが表示されます。これらのオプションは、スタティック、接続済み、RIP、または BGP ルートを再配布するときには使用できません。
ID	BGP または OSPF ルーティングプロセスの自律システム（AS）番号。
Bandwidth	ルートの最小帯域幅（キロビット/秒）。有効値の範囲は 1 ～ 4294967295 です。
遅延時間	ルート遅延（10 マイクロ秒単位）。有効値の範囲は、0 ～ 4294967295 です。
信頼性	正常なパケット伝送の可能性。0 ～ 255 の数値で表されます。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを表します。
読み込み中	ルートの実効帯域幅。有効値の範囲は 1 ～ 255 で、255 は負荷が 100 % であることを示します。
[MTU]	パスの最大伝送単位の最小許容値。有効値の範囲は 1 ～ 65535 です。
ルート マップ	再配布エントリに適用されるルートマップオブジェクトの名前。

[EIGRP再配布の追加/編集（Add/Edit EIGRP Redistribution）] ダイアログボックス

[再配布の追加/編集（Add/Edit Redistribution）] ダイアログボックスを使用して、再配布ルールを追加するか、[再配布（Redistribution）] テーブルの既存の再配布ルールを編集します。

ナビゲーション パス

[EIGRP再配布の追加/編集（Add/Edit EIGRP Redistribution）] ダイアログボックスには、[Redistribution] タブ （63 ページ）からアクセスできます。

関連項目

- EIGRP の設定 （50 ページ）
- EIGRP について （52 ページ）
- [Redistribution] タブ （63 ページ）

フィールド リファレンス

表 *25 : [EIGRP*再配布の追加/編集（*Add/Edit EIGRP Redistribution*）*]* ダイアログボックス

要素	説明
プロトコル	ルートが再配布されているソース プロトコルを選択します。次のいずれかのオプションを選択できます。 • [BGP]：BGP ルーティングプロセスによって検出されたルートを EIGRP に再配布します。 • [RIP]：RIP ルーティングプロセスによって検出されたルートを EIGRP に再配布します。 • [Static]：スタティックルートを EIGRP ルーティングプロセスに再配布します。ネットワーク設定の範囲内にあるスタティック ルートは EIGRP に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。 • [Connected]：接続されたルート（インターフェイス上で IP アドレスをイネーブルにすることによって自動的に確立されるルート）を EIGRP ルーティングプロセスに再配布します。ネットワーク設定の範囲内にある接続済みルートは EIGRP に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。 • [OSPF]：OSPF ルーティングプロセスで検出されたルートを EIGRP に再配布します。このプロトコルを選択すると、このダイアログボックスの [Match] のオプションが表示されます。これらのオプションは、スタティック、接続済み、RIP、または BGP ルートを再配布するときには使用できません。

要素	説明
ルーティングプロセス ID	BGP または OSPF ルーティングプロセスの自律システム（AS）番号。
オプションメトリック	EIGRP ルーティングプロセスに再配布されるルートの次のメトリックを定義できます。 • [帯域幅（Bandwidth）]：ルートの最小帯域幅（キロビット/秒）。有効値の範囲は 1 ～ 4294967295 です。 • [遅延時間（Delay Time）]：ルートの遅延（10 マイクロ秒）。有効値の範囲は、0 ～ 4294967295 です。 • [信頼性（Reliability）]：0 ～ 255 の数値で表現した、パケットが正常に伝送される見込み。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを表します。 • [ローディング（Loading）]：ルートの実効帯域幅。有効値の範囲は 1 ～ 255 で、255 は負荷が 100 % であることを示します。 • [MTU]：パスの最大伝送単位の最小許容値。有効値の範囲は 1 ～ 65535 です。
ルートマップ	EIGRP ルーティングプロセスに再配布されるルートを定義するには、ルートマップオブジェクトを選択または入力します。 **ヒント** [選択（Select）]をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）]を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。

要素	説明
オプションの OSPF 再配布	ルートタイプとして OSPF を選択した場合、1 つのルーティングプロトコルから別のルーティングプロトコルへのルート再配布に使用される条件を選択します。ルートが再配布されるには、選択した条件と一致している必要があります。次の一致条件から 1 つ以上を選択できます。 • [Internal]：ルートは特定の AS の内部です。 • [External 1]：自律システムの外部だが、OSPF にタイプ 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、OSPF にタイプ 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、OSPF にタイプ 2 NSSA 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、OSPF にタイプ 2 NSSA ルートとしてインポートされるルート。

[サマリーアドレス（Summary Address）] タブ

[サマリーアドレス（Summary Address）] タブを使用して、特定のインターフェイスの EIGRP のサマリーを設定します。サマリーアドレスはインターフェイスごとに設定できます。ネットワーク番号の境界以外でサマリーアドレスを作成する場合、または自動ルート集約がディセーブルになった ASA でサマリー アドレスを使用する場合は、手動でサマリー アドレスを定義する必要があります。ルーティング テーブルに他にも個別のルートがある場合、EIGRP は、他の個別ルートすべての中で最小のメトリックと等しいメトリックで、サマリーアドレスをインターフェイスからアドバタイズします。

ナビゲーション パス

[EIGRP] ページから [サマリーアドレス（Summary Address）] タブにアクセスできます。詳細については、EIGRP の設定 （50 ページ）を参照してください。

関連項目

• [EIGRPサマリーアドレスの追加/編集（Add/Edit EIGRP Summary Address）] ダイアログボックス （68 ページ）
• EIGRP の設定 （50 ページ）
• EIGRP について （52 ページ）
• [Setup] タブ （56 ページ）
• [フィルタルール（Filter Rules）] タブ （59 ページ）

- [Neighbors] タブ （61 ページ）
- [Redistribution] タブ （63 ページ）
- [Interfaces] タブ （69 ページ）

フィールド リファレンス

表 *26 : EIGRP* : *[*サマリーアドレス（*Summary Address*）*]* タブ

要素	説明
インターフェイス（Interface）	サマリーアドレスのアドバタイズ元となるインターフェイスです。
ネットワーク（Network）	サマリーアドレスの IP アドレスおよびネットワークマスク。
アドミニストレーティブ ディスタンス（Administrative Distance）	サマリールートのアドミニストレーティブ ディスタンス。

[EIGRPサマリーアドレスの追加/編集（Add/Edit EIGRP Summary Address）] ダイアログボックス

[EIGRPサマリーアドレスの追加/編集（Add/Edit EIGRP Summary Address）] ダイアログボックスを使用して、新しいエントリを追加するか、サマリーアドレステーブルの既存のエントリを変更します。サマリーアドレスはインターフェイスごとに設定できます。ネットワーク番号の境界以外でサマリーアドレスを作成する場合、または自動ルート集約がディセーブルになった ASA でサマリー アドレスを使用する場合は、手動でサマリー アドレスを定義する必要があります。ルーティング テーブルに他にも個別のルートがある場合、EIGRP は、他の個別ルートすべての中で最小のメトリックと等しいメトリックで、サマリーアドレスをインターフェイスからアドバタイズします。

ナビゲーション パス

[EIGRPサマリーアドレスの追加/編集（Add/Edit EIGRP Summary Address）] ダイアログボックスには、[サマリーアドレス（Summary Address）] タブ （67 ページ）からアクセスできます。

関連項目

- EIGRP の設定 （50 ページ）
- EIGRP について （52 ページ）
- [サマリーアドレス（Summary Address）] タブ （67 ページ）

フィールド リファレンス

表 *27 : [EIGRP*サマリーアドレスの追加/編集（*Add/Edit EIGRP Summary Address*）*]* ダイアログボックス

要素	説明
インターフェイス（Interface）	サマリーアドレスのアドバタイズ元となるインターフェイスです。 ヒント　[選択（Select）] をクリックして、インターフェイスオブジェクトのリストからインターフェイスを選択できます。
ネットワーク	サマリーアドレスの IP アドレスおよびネットワークマスク。 ヒント　[選択（Select）] をクリックすると、ネットワークオブジェクトのリストからネットワークを選択できます。
アドミニストレーティブディスタンス（Administrative Distance）	（任意）集約ルートのアドミニストレーティブディスタンス。有効な値は 1 ～ 255 です。デフォルト値は 5 です。

[Interfaces] タブ

[インターフェイス（Interface）] タブを使用して、インターフェイス固有の EIGRP ルーティングプロパティを設定します。

ナビゲーション パス

[EIGRP] ページから [インターフェイス（Interfaces）] タブにアクセスできます。詳細については、EIGRP の設定　（50 ページ）を参照してください。

関連項目

- [EIGRPインターフェイスの追加/編集（Add/Edit EIGRP Interface）] ダイアログボックス　（70 ページ）
- EIGRP の設定　（50 ページ）
- EIGRP について　（52 ページ）
- [Setup] タブ　（56 ページ）
- [フィルタルール（Filter Rules）] タブ　（59 ページ）
- [Neighbors] タブ　（61 ページ）
- [Redistribution] タブ　（63 ページ）
- [サマリーアドレス（Summary Address）] タブ　（67 ページ）

フィールド リファレンス

表 *28 : [EIGRP]* : *[インターフェイス（Interfaces）]* タブ

要素	説明
インターフェイス（Interface）	設定が適用されるインターフェイスの名前。
Hello 間隔（Hello Interval）	インターフェイス上で送信される EIGRP hello パケット間の間隔（秒数）。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 5 秒です。
保留時間（Hold Time）	EIGRP hello パケットで ASA によってアドバタイズされるホールドタイム。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 15 秒です。
Split Horizon	インターフェイスで EIGRP スプリットホライズンが有効になっているか（true）無効になっているか（false）を示します。
遅延	遅延時間（10 マイクロ秒単位）。有効な値は、1 ～ 16777215 です。このオプションは、マルチコンテキストモードのデバイスではサポートされています。
Key ID	EIGRP 更新の認証に使用されるキーの ID。

[EIGRPインターフェイスの追加/編集（Add/Edit EIGRP Interface）] ダイアログボックス

[EIGRPインターフェイスの追加/編集（Add/Edit EIGRP Interface）] ダイアログボックスを使用して、インターフェイス固有の EIGRP ルーティングパラメータを設定します。

ナビゲーション パス

[EIGRPインターフェイスの追加/編集（Add/Edit EIGRP Interface）] ダイアログボックスには、[Interfaces] タブ （69 ページ）からアクセスできます。

関連項目

- EIGRP の設定 （50 ページ）
- EIGRP について （52 ページ）
- [Interfaces] タブ （69 ページ）

フィールド リファレンス

表 *29 : [EIGRP*インターフェイスの追加（*Add EIGRP Interface***）*]/[EIGRP*インターフェイスの編集（***Edit EIGRP Interface***）*]* ダイアログボックス**

要素	説明
インターフェイス（Interface）	設定が適用されるインターフェイスの名前。
Hello 間隔（Hello Interval）	インターフェイス上で送信される EIGRP hello パケット間の間隔（秒数）。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 5 秒です。
保留時間（Hold Time）	EIGRP hello パケットで ASA によってアドバタイズされるホールドタイム。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 15 秒です。
Split Horizon	インターフェイスで EIGRP スプリットホライズンを有効または無効にします。
遅延時間	遅延時間（10 マイクロ秒単位）。有効な値は、1 ～ 16777215 です。このオプションは、マルチコンテキストモードのデバイスではサポートされていないため、無効になります。
MD5 認証の有効化（Enable MD5 Authentication）	EIGRP パケットの MD5 認証をイネーブルにします。
キー タイプ	入力するキーがクリアテキストであることを示すには、[クリアテキスト（Clear Text）] を選択します。入力するキーがすでに暗号化されていることを示すには、[暗号化（Encrypted）] を選択します。
キー ID とキー	EIGRP 更新を認証するキーを指定します。 • [Key ID]：数値のキー ID を入力します。有効な値の範囲は 0 ～ 255 です。 • [Key]：最大 16 バイトの英数字文字列。 • [確認（Confirm）]：キーを再入力します。

EIGRPv6 の設定

[EIGRPv6（EIGRPv6）] ページには、ファイアウォールデバイスで Enhanced Interior Gateway Routing Protocol（EIGRPv6）ルーティングを設定するための 6 つのタブ付きパネルがあります。以下のトピックでは、EIGRPv6 の有効化および設定について詳しく説明します。

• [IPv6 EIGRPの詳細設定（IPv6 EIGRP Advanced）] ダイアログボックス （73 ページ）

- [Setup] タブ （76 ページ）
- [フィルタルール（Filter Rules）] タブ （78 ページ）
- [Neighbors] タブ （80 ページ）
- [Redistribution] タブ （81 ページ）
- [サマリーアドレス（Summary Address）] タブ （86 ページ）
- [Interfaces] タブ （88 ページ）

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [ルーティング（Routing）] > [EIGRP（EIGRP）]** を選択します。[IPv6ファミリ（IPv6 Family）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから、**[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [EIGRP（EIGRP）]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。[IPv6ファミリ（IPv6 Family）] タブをクリックします。

フィールド リファレンス

表 30 : [EIGRPv6（EIGRPv6）] ページ

要素	説明
[IPv6 EIGRPの有効化（Enable IPv6 EIGRP）]	このボックスをオンにして EIGRPv6 ルーティングプロセスを有効化します。
AS 番号（AS Number）	EIGRPv6 プロセスの自律システム（AS）番号を入力します。指定できる AS 番号の範囲は 1 ～ 65535 です。
[Advanced] ボタン	[IPv6 EIGRPの詳細設定（IPv6 EIGRP Advanced）] ダイアログボックス （73 ページ）を開きます。ここでは、ルータ ID、スタブルーティング、隣接関係の変更など、追加の EIGRPv6 プロセス設定を設定できます。
[Setup] タブ	[セットアップ（Setup）] タブを使用して、EIGRPv6 ルーティングプロセスで使用されるネットワーク、パッシブインターフェイス、デフォルトルート情報、アドミニストレーティブ ディスタンス、およびデフォルトメトリックを設定します。 詳細については、[Setup] タブ （76 ページ）を参照してください。

要素	説明
[フィルタルール（Filter Rules）] タブ	[フィルタルール（Filter Rules）] タブを使用してフィルタルールを定義すると、EIGRPv6 ルーティングプロセスで受け入れ、またはアドバタイズされるルートを制御することができます。 詳細については、[フィルタルール（Filter Rules）] タブ （78 ページ）を参照してください。
[ネイバー（Neighbors）] タブ	[ネイバー（Neighbors）] タブを使用して、EIGRPv6 ネイバーを手動で定義します。 詳細については、[Neighbors] タブ （80 ページ）を参照してください。
[再配布（Redistribution）] タブ	[再配布（Redistribution）] タブを使用して、他のルーティングプロトコルから EIGRPv6 ルーティングプロセスにルートを再配布するためのルールを定義します。 詳細については、[Redistribution] タブ （81 ページ）を参照してください。
[サマリーアドレス（Summary Address）] タブ	[サマリーアドレス（Summary Address）] タブを使用して、スタティックに定義された EIGRPv6 サマリーアドレスを作成します。 詳細については、[サマリーアドレス（Summary Address）] タブ（86 ページ）を参照してください。
[インターフェイス（Interfaces）] タブ	[インターフェイス（Interfaces）] タブを使用して、EIGRP のインターフェイスを設定します。 詳細については、[Interfaces] タブ （88 ページ）を参照してください。

[IPv6 EIGRPの詳細設定（IPv6 EIGRP Advanced）] ダイアログボックス

[EIGRPV6の詳細設定（EIGRPV6 Advanced）] ダイアログボックスを使用して、ルータ ID、スタブルーティング、隣接関係の変更などの設定を行います。

ナビゲーション パス

[EIGRPv6（EIGRPv6）] ページから [IPv6 EIGRPの詳細設定（IPv6 EIGRP Advanced）] ダイアログボックスにアクセスできます（ EIGRPv6 の設定 （71 ページ）を参照）。

フィールド リファレンス

表 *31 : [IPv6 EIGRPの詳細設定（IPv6 EIGRP Advanced）] ダイアログボックス*

要素	説明
ルータ ID（Router ID）	ルータ IDは、外部ルートの発信元ルータを識別するために使用されます。外部ルートがローカルのルータ ID で受信された場合、このルートは廃棄されます。これを回避するには、ルータ ID のグローバルアドレスを指定します。EIGRPv6 ルータごとに一意の値を設定する必要があります。 単一のデバイスで、[自動（Automatic）] または [IPアドレス（IP Address）] を選択します。（IP アドレスを選択すると、[アドレス（address）] フィールドが表示されます。） [自動（Automatic）] を選択すると、セキュリティアプライアンス上で最上位の IP アドレスがルータ ID として使用されます。固定ルータ ID を使用するには、[IPアドレス（IP Address）] を選択して、[ルータID（Router ID）] フィールドに IPv6 アドレスを入力します。 デバイスクラスタで、[自動（Automatic）] または [クラスタプール（Cluster Pool）] を選択します。（[クラスタプール（Cluster Pool）] を選択すると、[IPv6プールオブジェクトID（IPv6 Pool object ID）] フィールドが表示されます）。 [クラスタプール（Cluster Pool）] を選択した場合は、ルータの ID アドレスを提供する IPv6 プールオブジェクトの名前を入力または選択します。詳細については、を参照してください。

要素	説明
Stub	ASA を EIGRPv6 スタブルータとしてイネーブル化し、設定することができます。スタブルーティングは、ASA でメモリと[IPv6プールの追加または編集（Add or Edit IPv6 Pool）] ダイアログボックスの処理要件を減らす場合があります。ASA をスタブルータとして設定すると、ローカル以外のトラフィックがすべて配布ルータに転送されるようになり、完全な EIGRPv6 ルーティングテーブルを維持する必要がなくなります。一般に、配布ルータからスタブルートに送信する必要があるのは、デフォルト ルートだけです。 スタブルータから配布ルータには、指定されたルートだけが伝搬されます。スタブルータである ASA は、サマリー、接続されているルート、再配布されたスタティック ルート、外部ルート、および内部ルートに対するクエリーすべてに、応答として「inaccessible」というメッセージを返します。ASA がスタブとして設定されているときは、自身のスタブルータとしてのステータスを報告するために、特殊なピア情報パケットをすべての隣接ルータに送信します。スタブ ステータスの情報を伝えるパケットを受信したネイバーはすべて、スタブルータにルートのクエリーを送信しなくなり、スタブ ピアを持つルータはそのピアのクエリーを送信しなくなります。スタブルータが正しいアップデートをすべてのピアに送信するには、配布ルータが必要です。 ASA を EIGRPv6 スタブルーティング プロセスとしてイネーブルにするには、次の EIGRPv6 スタブルーティング プロセスから 1 つ以上を選択します。 • [受信のみ（Receive Only）]：隣接ルータからルート情報を受信しても、その隣接ルータにルート情報を送信しないために、EIGRPv6 スタブルーティングプロセスを設定します。このオプションを選択する場合は、他のスタブルーティング オプションを選択できません。 • [接続済み（Connected）]：接続済みルートをアドバタイズします。 • [再配布済み（Redistributed）]：再配布済みルートをアドバタイズします。 • [スタティック（Static）]：スタティックルートをアドバタイズします。 • [サマリ - （Summary）]：サマリールートをアドバタイズします。

要素	説明
隣接関係の変更	これらのオプションでは、隣接関係の変更が発生したときに送信される syslog メッセージを指定します。 • [ログネイバーの変更（Log Neighbor Changes）]：EIGRPv6 ネイバーの隣接関係に関する変更のロギングを有効にします。このオプションは、デフォルトで選択されます。 • [ログネイバーの警告（Log Neighbor Warnings）]：EIGRPv6 ネイバーの警告メッセージのロギングを有効にします。このオプションは、デフォルトで選択されます。 （任意）ネイバー警告メッセージの反復間隔（秒数）。有効値は 1 ～ 65535 です。この間隔内に警告が繰り返し発生した場合、それらの警告はログに記録されません。

[Setup] タブ

[EIGRPv6（EIGRPv6）] ページの [セットアップ（Setup）] タブを使用して、IPv6 EIGRP ルーティングプロセスで使用されるネットワーク、パッシブインターフェイス、デフォルトルート情報、アドミニストレーティブ ディスタンス、およびデフォルトメトリックを設定します。

ナビゲーション パス

[EIGRPv6（EIGRPv6）]ページから [セットアップ（Setup）] タブにアクセスできます。詳細については、EIGRPv6 の設定 （71 ページ）を参照してください。

関連項目

- EIGRPv6 の設定 （71 ページ）
- [フィルタルール（Filter Rules）] タブ （78 ページ）
- [Neighbors] タブ （80 ページ）
- [Redistribution] タブ （81 ページ）
- [サマリーアドレス（Summary Address）] タブ （86 ページ）
- [Interfaces] タブ （88 ページ）

フィールド リファレンス

表 *32 : [IPv6（IPv6）]*：*[セットアップ（Setup）]* タブ

要素	説明
パッシブインターフェイス	1 つ以上のインターフェイスを受動インターフェイスとして設定できます。EIGRPv6 の場合、受動インターフェイスではルーティングアップデートが送受信されません。 デフォルトでは、そのインターフェイスでルーティングが有効になると、アクティブルーティング（ルーティング更新の送受信）に対してすべてのインターフェイスが有効になります。 パッシブインターフェイスを設定するには、次のいずれかを実行します。 • そのインターフェイスに対してルーティングが有効な場合、アクティブルーティング（ルーティング更新の送受信）に対してすべてのインターフェイスを有効にするには、[なし（None）] を選択します。 • インターフェイスをデフォルトでパッシブとして設定するには、[デフォルト（Default）] を選択します。 • 特定のインターフェイスをパッシブとして設定するには、[指定されたインターフェイス（Specified Interfaces）] を選択し、パッシブにするインターフェイスを入力または選択します。
デフォルトメトリック	EIGRPv6 ルーティングプロセスに再配布されるルートのデフォルトのメトリックを定義できます。 • [帯域幅（Bandwidth）]：ルートの最小帯域幅（キロビット/秒）。有効値の範囲は 1 ～ 4294967295 です。 • [遅延時間（Delay Time）]：ルートの遅延（10 マイクロ秒）。有効値の範囲は、0 ～ 4294967295 です。 • [信頼性（Reliability）]：0 ～ 255 の数値で表現した、パケットが正常に伝送される見込み。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを表します。 • [ローディング（Loading）]：ルートの実効帯域幅。有効値の範囲は 1 ～ 255 で、255 は負荷が 100 % であることを示します。 • [MTU]：パスの最大伝送単位の最小許容値。有効値の範囲は 1 ～ 65535 です。

[フィルタルール（Filter Rules）] タブ

[フィルタルール（Filter Rules）] タブには、EIGRPv6 ルーティングプロセスに設定されているルート フィルタリング ルールを表示する [フィルタルール（Filter Rules）] テーブルが含まれています。フィルタルールによって、EIGRPv6 ルーティングプロセスで受け入れまたはアドバタイズされるルートを制御できます。

ナビゲーション パス

[EIGRPv6（EIGRPv6）] ページから [フィルタルール（Filter Rules）] タブにアクセスできます。詳細については、EIGRPv6 の設定 （71 ページ）を参照してください。

関連項目

- [IPv6 EIGRPフィルタルールの追加/編集（Add/Edit IPv6 EIGRP Filter Rule）] ページダイアログボックス （79 ページ）
- EIGRPv6 の設定 （71 ページ）
- [Setup] タブ （76 ページ）
- [Neighbors] タブ （80 ページ）
- [Redistribution] タブ （81 ページ）
- [サマリーアドレス（Summary Address）] タブ （86 ページ）
- [Interfaces] タブ （88 ページ）

フィールド リファレンス

表 *33 : [IPv6 EIGRP（IPv6 EIGRP）] : [フィルタルール（Filter Rules）] タブ*

要素	説明
EIGRP フィルタの方向	フィルタルールの方向： • [インバウンド（Inbound）]：このルールは、着信 EIGRPv6 ルーティングアップデートからのデフォルトルート情報をフィルタリングします。 • [アウトバウンド（Outbound）]：このルールは、発信 EIGRPv6 ルーティングアップデートからのデフォルトルート情報をフィルタリングします。
インターフェイス（Interface）	フィルタルールが適用されるインターフェイス。

要素	説明
IPv6 プレフィックス リスト	IPv6 プレフィックスリストの名前。このリストは、受信されるネットワークとルーティング アップデートで抑制されるネットワークを定義します。

[IPv6 EIGRPフィルタルールの追加/編集（Add/Edit IPv6 EIGRP Filter Rule）] ページダイアログボックス

[EIGRPv6フィルタルールの追加/編集（Add/Edit EIGRPv6 Filter Rule）] ページダイアログボックスを使用して、既存のフィルタルールテーブルに新しいフィルタルールを追加するか、または既存のフィルタルールを変更します。

ナビゲーション パス

[IPv6 EIGRPフィルタルールの追加/編集（Add/Edit IPv6 EIGRP Filter Rule）] ページダイアログボックスには、[フィルタルール（Filter Rules）] タブ （78 ページ）からアクセスできます。

関連項目

- EIGRPv6 の設定 （71 ページ）
- [フィルタルール（Filter Rules）] タブ （78 ページ）

フィールド リファレンス

表 *34 : [IPv6 EIGRPフィルタルールの追加/編集（Add/Edit IPv6 EIGRP Filter Rule）] ページダイアログボックス*

要素	説明
EIGRP フィルタの方向	フィルタルールの方向を指定します。 • [インバウンド（Inbound）]：このルールは、着信 EIGRPv6 ルーティングアップデートからのデフォルトルート情報をフィルタリングします。 • [アウトバウンド（Outbound）]：このルールは、発信 EIGRPv6 ルーティングアップデートからのデフォルトルート情報をフィルタリングします。
インターフェイス（Interface）	[インターフェイスセレクタ（Interface Selector）] タブからインターフェイスを選択します。
IPv6 プレフィックス リスト	IPv6 プレフィックスリストの名前。このリストは、受信されるネットワークとルーティング アップデートで抑制されるネットワークを定義します。

[Neighbors] タブ

[ネイバー（Neighbors）] タブには、EIGRPv6 のネイバーを定義できるネイバーテーブルが含まれています。手動で EIGRPv6 ネイバーを定義すると、hello パケットはユニキャストメッセージとしてそのネイバーに送信されます。

ナビゲーション パス

[EIGRPv6（EIGRPv6）] ページから [ネイバー（Neighbors）] タブにアクセスできます。詳細については、EIGRPv6 の設定 （71 ページ）を参照してください。

関連項目

- [IPv6 EIGRPネイバーの追加/編集（Add/Edit EIGRP Neighbor）] ダイアログボックス （80 ページ）
- EIGRPv6 の設定 （71 ページ）
- [Setup] タブ （76 ページ）
- [フィルタルール（Filter Rules）] タブ （78 ページ）
- [Redistribution] タブ （81 ページ）
- [サマリーアドレス（Summary Address）] タブ （86 ページ）
- [Interfaces] タブ （88 ページ）

フィールド リファレンス

表 35 : [IPv6 EIGRP（IPv6 EIGRP）] : [ネイバー（Neighbors）] タブ

要素	説明
インターフェイス（Interface）	ネイバーが使用可能なインターフェイス。
ネットワーク （Network）	追加されたネイバーの IPv6 アドレス。

[IPv6 EIGRPネイバーの追加/編集（Add/Edit EIGRP Neighbor）] ダイアログボックス

EIGRPv6 hello パケットはマルチキャストパケットとして送信されます。EIGRPv6 ネイバーが、トンネルなど、非ブロードキャストネットワークを越えた場所にある場合、手動でネイバーを定義する必要があります。手動で EIGRPv6 ネイバーを定義すると、hello パケットはユニキャストメッセージとしてそのネイバーに送信されます。

ネイバーを定義するか、または既存のネイバーの情報を変更するには、[IPv6 EIGRPネイバーの追加/編集（Add/Edit IPv6 EIGRP Neighbor）] ページダイアログボックスを使用します。

ナビゲーション パス

[IPv6 EIGRPネイバーの追加/編集（Add/Edit IPv6 EIGRP Neighbor）] ページダイアログボックスには、 [Neighbors] タブ （80 ページ）からアクセスできます。

関連項目

- EIGRPv6 の設定 （71 ページ）
- [Neighbors] タブ （80 ページ）

フィールド リファレンス

表 *36 : [IPv6 EIGRP*ネイバーの追加/編集（*Add/Edit EIGRP Neighbor*）*]* ページダイアログボックス

要素	説明
インターフェイス（Interface）	ネイバーが使用可能なインターフェイス。 **ヒント** [選択（Select）] をクリックして、インター フェイスオブジェクトのリストからインターフェイスを選択できます。
ネットワーク （Network）	ネイバーの IPv6 アドレス。 **ヒント** [選択（Select）] をクリックすると、ホストオブジェクトのリストからネイバーを選択できます。

[Redistribution] タブ

[再配布（Redistribution）] タブを使用して、他のルーティングプロトコルから EIGRPv6 ルーティングプロセスにルートを再配布するためのルールを定義します。

ナビゲーション パス

[EIGRPv6（EIGRPv6）] ページから [再配布（Redistribution）] タブにアクセスできます。詳細については、 EIGRPv6 の設定 （71 ページ）を参照してください。

関連項目

- [IPv6 EIGRP再配布の追加/編集（Add/Edit IPv6 EIGRP Redistribution）] ダイアログボックス （83 ページ）
- EIGRPv6 の設定 （71 ページ）
- [Setup] タブ （76 ページ）
- [フィルタルール（Filter Rules）] タブ （78 ページ）
- [Neighbors] タブ （80 ページ）

- [サマリーアドレス（Summary Address）] タブ （86 ページ）
- [Interfaces] タブ （88 ページ）

フィールド リファレンス

表 *37 : [IPv6 EIGRP（IPv6 EIGRP）]*：*[*再配布（*Redistribution*）*]* タブ

要素	説明
プロトコル	ルートの再配布元の送信元プロトコル。 • [BGP（BGP）]：BGP ルーティングプロセスによって検出されたルートを EIGRPv6 に再配布します。 • [スタティック（Static）]：スタティックルートを EIGRPv6 ルーティングプロセスに再配布します。ネットワーク設定の範囲内にあるスタティックルートは EIGRPv6 に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。 • [接続済み（Connected）]：接続されたルート（インターフェイス上で IP アドレスをイネーブルにすることによって自動的に確立されるルート）を EIGRPv6 ルーティングプロセスに再配布します。ネットワーク設定の範囲内にある接続済みルートは EIGRPv6 に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。 • [OSPF（OSPF）]：OSPF ルーティングプロセスで検出されたルートを EIGRPv6 に再配布します。このプロトコルを選択すると、このダイアログボックスの [Match] のオプションが表示されます。これらのオプションは、スタティック、接続済み、または BGP ルートを再配布するときには使用できません。 • [ISIS（ISIS）]：ISIS ルーティング プロトコルによって検出されたルートを EIGRPv6 に再配布します。
ID	BGP または OSPF ルーティングプロセスの自律システム（AS）番号。
Bandwidth	ルートの最小帯域幅（キロビット/秒）。有効値の範囲は 1 ～ 4294967295 です。
遅延時間	ルート遅延（10 マイクロ秒単位）。有効値の範囲は、0 ～ 4294967295 です。
信頼性	正常なパケット伝送の可能性。0 ～ 255 の数値で表されます。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを表します。
読み込み中	ルートの実効帯域幅。有効値の範囲は 1 ～ 255 で、255 は負荷が 100 % であることを示します。

要素	説明
[MTU]	パスの最大伝送単位の最小許容値。有効値の範囲は 1 ～ 65535 です。
ルート マップ	再配布エントリに適用されるルートマップオブジェクトの名前。
[ISISレベル（ISIS Level）]	レベル 1 またはレベル 2 またはレベル 1-2 を選択します。デフォルトのレベルは 2 です。

[IPv6 EIGRP再配布の追加/編集（Add/Edit IPv6 EIGRP Redistribution）] ダイアログボックス

[IPv6 EIGRP再配布の追加/編集（Add/Edit IPv6 EIGRP Redistribution）] ダイアログボックスを使用して、再配布ルールを追加するか、[再配布（Redistribution）] テーブルの既存の再配布ルールを編集します。

ナビゲーション パス

[IPv6 EIGRP再配布の追加/編集（Add/Edit IPv6 EIGRP Redistribution）] ダイアログボックスには、[Redistribution] タブ （81 ページ）からアクセスできます。

関連項目

- EIGRPv6 の設定 （71 ページ）
- [Redistribution] タブ （81 ページ）

フィールド リファレンス

表 *38 : [IPv6 EIGRP*再配布の追加/編集（*Add/Edit IPv6 EIGRP Redistribution*）*]* ダイアログボックス

要素	説明
プロトコル	ルートが再配布されているソース プロトコルを選択します。次のいずれかのオプションを選択できます。 • [BGP（BGP）]：BGPルーティングプロセスによって検出されたルートをEIGRPv6 に再配布します。 • [スタティック（Static）]：スタティックルートを EIGRPv6 ルーティングプロセスに再配布します。ネットワーク設定の範囲内にあるスタティックルートは EIGRPv6 に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。 • [接続済み（Connected）]：接続されたルート（インターフェイス上で IP アドレスをイネーブルにすることによって自動的に確立されるルート）を EIGRPv6 ルーティングプロセスに再配布します。ネットワーク設定の範囲内にある接続済みルートは EIGRPv6 に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。 • [OSPF（OSPF）]：OSPF ルーティングプロセスで検出されたルートを EIGRPv6 に再配布します。このプロトコルを選択すると、このダイアログボックスの [Match] のオプションが表示されます。これらのオプションは、スタティック、接続済み、または BGP ルートを再配布するときには使用できません。 • [ISIS（ISIS）]：ISIS ルーティング プロトコルによって検出されたルートを EIGRPv6 に再配布します。
ID	BGP または OSPF ルーティングプロセスの自律システム（AS）番号。

要素	説明
オプションメトリック	EIGRPv6 ルーティングプロセスに再配布されるルートの次のメトリックを定義できます。 • [帯域幅（Bandwidth）]：ルートの最小帯域幅（キロビット/秒）。有効値の範囲は 1 ～ 4294967295 です。 • [遅延時間（Delay Time）]：ルートの遅延（10 マイクロ秒）。有効値の範囲は、0 ～ 4294967295 です。 • [信頼性（Reliability）]：0 ～ 255 の数値で表現した、パケットが正常に伝送される見込み。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを表します。 • [ローディング（Loading）]：ルートの実効帯域幅。有効値の範囲は 1 ～ 255 で、255 は負荷が 100 % であることを示します。 • [MTU]：パスの最大伝送単位の最小許容値。有効値の範囲は 1 ～ 65535 です。
ルート マップ	EIGRPv6 ルーティングプロセスに再配布されるルートを定義するには、ルートマップオブジェクトを選択または入力します。 ヒント [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。
オプションの OSPF 再配布	ルートタイプとして OSPF を選択した場合、1 つのルーティングプロトコルから別のルーティングプロトコルへのルート再配布に使用される条件を選択します。ルートが再配布されるには、選択した条件と一致している必要があります。次の一致条件から 1 つ以上を選択できます。 • [Internal]：ルートは特定の AS の内部です。 • [External 1]：自律システムの外部だが、OSPF にタイプ 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、OSPF にタイプ 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、OSPF にタイプ 2 NSSA 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、OSPF にタイプ 2 NSSA ルートとしてインポートされるルート。

要素	説明
[ISISレベル（ISIS Level）]	レベル 1 またはレベル 2 またはレベル 1-2 を選択します。デフォルトのレベルは 2 です。

[サマリーアドレス（Summary Address）] タブ

[サマリーアドレス（Summary Address）] タブを使用して、特定のインターフェイスの EIGRPv6 のサマリーを設定します。サマリーアドレスはインターフェイスごとに設定できます。ネットワーク番号の境界以外でサマリーアドレスを作成する場合、または自動ルート集約がディセーブルになった ASA でサマリーアドレスを使用する場合は、手動でサマリーアドレスを定義する必要があります。ルーティングテーブルに他にも個別のルートがある場合、EIGRPv6 は、他の個別ルートすべての中で最小のメトリックと等しいメトリックで、サマリーアドレスをインターフェイスからアドバタイズします。

ナビゲーション パス

[EIGRPv6（EIGRPv6）] ページから [サマリーアドレス（Summary Address）] タブにアクセスできます。詳細については、EIGRPv6 の設定 （71 ページ）を参照してください。

関連項目

- [IPv6 EIGRPサマリーアドレスの追加/編集（Add/Edit IPv6 EIGRP Summary Address）] ページダイアログボックス （87 ページ）
- EIGRPv6 の設定 （71 ページ）
- [Setup] タブ （76 ページ）
- [フィルタルール（Filter Rules）] タブ （78 ページ）
- [Neighbors] タブ （80 ページ）
- [Redistribution] タブ （81 ページ）
- [Interfaces] タブ （88 ページ）

フィールド リファレンス

表 39 : [IPv6 EIGRP（IPv6 EIGRP）] : [サマリーアドレス（Summary Address）] タブ

要素	説明
インターフェイス（Interface）	サマリーアドレスのアドバタイズ元となるインターフェイスです。
ネットワーク（Network）	サマリーアドレスの IP アドレスおよびネットワークマスク。

要素	説明
アドミニストレーティブ ディスタンス（Administrative Distance）	サマリールートのアドミニストレーティブ ディスタンス。

[IPv6 EIGRPサマリーアドレスの追加/編集（Add/Edit IPv6 EIGRP Summary Address）] ページダイアログボックス

[IPv6 EIGRPサマリーアドレスの追加/編集（Add/Edit IPv6 EIGRP Summary Address）] ページダイアログボックスを使用して、新しいエントリを追加するか、サマリーアドレステーブルの既存のエントリを変更します。サマリーアドレスはインターフェイスごとに設定できます。ネットワーク番号の境界以外でサマリー アドレスを作成する場合、または自動ルート集約がディセーブルになった ASA でサマリー アドレスを使用する場合は、手動でサマリー アドレスを定義する必要があります。ルーティングテーブルに他にも個別のルートがある場合、EIGRPv6 は、他の個別ルートすべての中で最小のメトリックと等しいメトリックで、サマリーアドレスをインターフェイスからアドバタイズします。

ナビゲーション パス

[IPv6 EIGRPサマリーアドレスの追加/編集（Add/Edit IPv6 EIGRP Summary Address）] ダイアログボックスには、[サマリーアドレス（Summary Address）] タブ （86 ページ）からアクセスできます。

関連項目

- EIGRPv6 の設定 （71 ページ）
- [サマリーアドレス（Summary Address）] タブ （86 ページ）

フィールド リファレンス

表 *40 : [IPv6 EIGRP*サマリーアドレスの追加/編集（*Add/Edit IPv6 EIGRP Summary Address*）*]* ダイアログボックス

要素	説明
インターフェイス（Interface）	サマリーアドレスのアドバタイズ元となるインターフェイスです。 **ヒント** [選択（Select）] をクリックして、インター フェイスオブジェクトのリストからインターフェイスを選択できます。
ネットワーク （Network）	サマリーアドレスの IPv6 アドレスおよびネットワークマスク。 **ヒント** [選択（Select）] をクリックすると、ネットワークオブジェクトのリストからネットワークを選択できます。

要素	説明
アドミニストレーティブ ディスタンス（Administrative Distance）	（任意）集約ルートのアドミニストレーティブ ディスタンス。有効な値は 1 ～ 255 です。デフォルト値は 5 です。

[Interfaces] タブ

[インターフェイス（Interface）] タブを使用して、インターフェイス固有の EIGRPv6 ルーティングプロパティを設定します。

ナビゲーション パス

[EIGRPv6（EIGRPv6）] ページから [インターフェイス（Interfaces）] タブにアクセスできます。詳細については、 EIGRPv6 の設定 （71 ページ）を参照してください。

関連項目

- [IPv6 EIGRPインターフェイスの追加/編集（Add/Edit IPv6 EIGRP Interface）] ページダイアログボックス （89 ページ）
- EIGRPv6 の設定 （71 ページ）
- [Setup] タブ （76 ページ）
- [フィルタルール（Filter Rules）] タブ （78 ページ）
- [Neighbors] タブ （80 ページ）
- [Redistribution] タブ （81 ページ）
- [サマリーアドレス（Summary Address）] タブ （86 ページ）

フィールド リファレンス

表 41 : [IPv6 EIGRP（IPv6 EIGRP）] : [インターフェイス（Interfaces）] タブ

要素	説明
インターフェイス（Interface）	設定が適用されるインターフェイスの名前。
Hello 間隔（Hello Interval）	インターフェイス上で送信される EIGRPv6 hello パケット間の間隔（秒数）。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 5 秒です。
保留時間（Hold Time）	EIGRPv6 hello パケットで ASA によってアドバタイズされる保留時間。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 15 秒です。

要素	説明
Split Horizon	インターフェイスで EIGRPv6 スプリットホライズンが有効になっているか（true）無効になっているか（false）を示します。

[IPv6 EIGRPインターフェイスの追加/編集（Add/Edit IPv6 EIGRP Interface）] ページダイアログボックス

[IPv6 EIGRPインターフェイスの追加/編集（Add/Edit IPv6 EIGRP Interface）] ページダイアログボックスを使用して、インターフェイス固有の EIGRPv6 ルーティングパラメータを設定します。

ナビゲーション パス

[IPv6 EIGRPインターフェイスの追加/編集（Add/Edit IPv6 EIGRP Interface）] ページダイアログボックスには、 [Interfaces] タブ （88 ページ）からアクセスできます。

関連項目

- EIGRPv6 の設定 （71 ページ）
- [Interfaces] タブ （88 ページ）

フィールド リファレンス

表 *42 : [IPv6 EIGRP*インターフェイスの追加/編集（*Add/Edit IPv6 EIGRP Interface*）*]* ページダイアログボックス

要素	説明
インターフェイス（Interface）	設定が適用されるインターフェイスの名前。
Hello 間隔（Hello Interval）	インターフェイス上で送信される EIGRPv6 hello パケット間の間隔（秒数）。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 5 秒です。
保留時間（Hold Time）	EIGRPv6 hello パケットで ASA によってアドバタイズされる保留時間。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 15 秒です。
Split Horizon	インターフェイスで EIGRPv6 スプリットホライズンを有効または無効にします。

ISIS の設定

[ISIS] ページには、ファイアウォールデバイスでの ISIS（Intermediate System-to-Intermediate System）ルーティングを設定するための 9 つのタブ付きパネルがあります。ISIS ルーティング

プロトコルは、Security Manager バージョン 4.11 以降で、ソフトウェアバージョン 9.6(1) 以降を実行している ASA デバイスについてサポートされています。以下のトピックでは、ISIS の有効化および設定について詳しく説明します。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）]>[ルーティング（Routing）] > [ISIS] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [ISIS] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

選択した ASA デバイスで Intermediate System-to-Intermediate System プロトコルを有効にするには、[ISIS の有効化（Enable ISIS）] をオンにします。

ISIS について

Intermediate System-to-Intermediate System（ISIS）ルーティングプロトコルはリンクステートの内部ゲートウェイプロトコル（IGP）です。リンクステートプロトコルは、各参加ルータで完全なネットワーク接続マップを構築するために必要な情報の伝播によって特徴付けられます。このマップは、その後、宛先への最短パスを計算するために使用されます。IOS ISIS の実装は、CLNP、IPv4、および IPv6 をサポートします。

ルーティングドメインは1つ以上のサブドメインに分けることができます。各サブドメインはエリアと呼ばれ、エリアアドレスが割り当てられます。エリア内のルーティングは、レベル 1 ルーティングと呼ばれます。レベル 1 エリア間のルーティングは、レベル 2 ルーティングと呼ばれます。OSI の用語では、ルータは中継システム（IS）と呼ばれます。IS はレベル 1 とレベル 2、またはその両方で稼働します。レベル 1 で稼働している IS は、同じエリア内にある他のレベル 1 の IS とルーティング情報を交換します。レベル 2 で稼働している IS は、他のレベル 2 のルータとルーティング情報を交換します。この場合はルータが同じレベル 1 エリアにあるかどうかは関係しません。レベル 2 にあるルータと、これらとインターコネクトしているリンクは、レベル 2 サブドメインを形成します。ルーティングが正しく機能するためには、これらをパーティション化してはなりません。

[General] タブ

[全般（General）] タブを使用して、[ベストパス選択（Best Path Selection）]、[ネイバータイマー（Neighbor Timers）]、[グレースフルリスタート（Graceful Restart）] などの BGP 設定を構成します。

ナビゲーション パス

[ネイバー（Neighbors）] タブには、[OSPF] ページからアクセスできます（BGP の設定 （2 ページ）を参照）。

関連項目

- BGP の設定 （2 ページ）
- BGP について （4 ページ）
- [IPv4ファミリ（IPv4 Family）] タブ （9 ページ）

フィールド リファレンス

表 *43 : [General]* タブ

要素	説明
[受信されたルートのAS_PATH属性に含まれるAS番号の数（Limit the number of AS numbers in AS_PATH attribute of received routes）]	AS_PATH 属性に含まれる AS 番号の数を特定の数に制限します。有効値は 1 ～ 254 です。
ネイバーの変更を記録（Log Neighbor Changes）	BGP ネイバーの変更（アップまたはダウン）のロギングを有効にします。これは、ネットワーク接続の問題をトラブルシューティングしたり、ネットワークの安定性を評価する際に役に立ちます。
[TCPパスMTUディスカバリを使用する（Use TCP Path MTU Discovery）]	パス MTU ディスカバリ手法を使用して、2 つの IP ホスト間のネットワークパスにおける最大伝送ユニット（MTU）のサイズを決定します。これにより、IP フラグメンテーションが回避されます。
[高速外部フェールオーバーの有効化（Enable fast external failover）]	リンク障害の発生時、外部 BGP セッションを即時にリセットします。
[最初のASをEBGPルートのピアのASとして実行（Enforce that the first AS is peer's AS for EBGP routes）]	AS 番号を AS_path 属性の 1 つ目のセグメントとしてリストに表示していない外部 BGP ピアから受信した着信アップデートを破棄します。これにより、誤って設定されたピアや許可されていないピアが、別の自律システムから送信されたかのようにルートをアドバイタイズしてトラフィックを誤った宛先に送信することがなくなります。
[AS番号にドット表記を使用（Use dot notation for AS numbers）]	完全なバイナリ 4 バイトの AS 番号を、ドットで区切られた 16 ビットの 2 文字ずつに分割します。0 ～ 65553 の AS 番号は 10 進数で表され、65535 を超える AS 番号はドット付き表記を使用して表されます。
[ベストパスの選択（Best Path Selection）]	

要素	説明
Default local preference	0 ～ 4294967295 の数値を指定します。デフォルト値は 100 です。値が大きいほど、優先度が高いことを示します。この優先度は、ローカル自律システム内のすべてのルータおよびアクセス サーバーに送信されます。
[異なるネイバーのMEDの比較を許可（Allow comparing MED from different neighbors）]	異なる自律システムにあるネイバーからのパスの Multi-Exit 識別子（MED）の比較を許可します。
[同一のBGPパスのルータIDを比較（Compare Router-id for identical EBGP paths）]	ベストパスの選択プロセス中に外部 BGP ピアから受信した類似パスを比較し、ベストパスをルータ ID が最も小さいルートに切り替えます。
[隣接ASからアドバタイズされたパスの間で最適なMEDパスを選択（Pick the best MED path among paths advertised from the neighboring AS）]	コンフェデレーション ピアから学習した複数のパスの間で MED 比較をイネーブルにします。MED 間の比較は、外部の自律システムがパスに存在しない場合にのみ行われます。
[欠落MEDを最低優先度として処理（Treat missing MED as the least preferred one）]	欠落している MED 属性は無限大の値を持つものとみなし、このパスを最も推奨度の低いパスにします。したがって、MED が欠落しているパスが最も優先度が低くなります。
[ネイバータイマー（Neighbor Timers）]	
[キープアライブ間隔（Keepalive Interval）]	キープアライブメッセージを送信しなかった場合に、その後 BGP ネイバーがアクティブな状態を継続する時間間隔を入力します。このキープアライブ インターバルが終わると、メッセージが送信されない場合、BGP ピアはデッドとして宣言されます。デフォルト値は 60 秒です。
保留時間（Hold Time）	BGP 接続が開始され設定されている間、BGP ネイバーがアクティブな状態を継続する時間間隔を入力します。デフォルト値は 180 秒です。
Min Hold Time	（任意）BGP 接続が開始され設定されている間、BGP ネイバーがアクティブな状態を継続する最小時間間隔を入力します。0 ～ 65535 の値を指定します。
[グレースフルリスタート（Graceful Restart）]（フェールオーバーまたはスパンドクラスタ モードで使用） （ASA 9.3.1 以降のみ）	
グレースフル リスタートをイネーブルにします。	スイッチオーバー後のルーティングフラップを ASA ピアが回避できるようにします。

要素	説明
再起動時間	BGP オープンメッセージが受信される前に、ASA ピアが古いルートを削除するまでの待機時間を指定します。デフォルト値は 120 秒です。有効な値は 1 ～ 3600 秒です。
[Stalepath時間（Stalepath Time）]	再起動する ASA から End Of Record（EOR）メッセージを受信した後、ASA が古いルートを削除するまでの待機時間を入力します。デフォルト値は 360 秒です。有効な値は 1 ～ 3600 秒です。

[IPv4ファミリ（IPv4 Family）] タブ

[BGP] ページの [IPv4ファミリ（IPv4 Family）] タブを使用して、BGP の IPv4 設定を有効にして構成します。

ナビゲーション パス

[BGP] ページから [IPv4ファミリ（IPv4 Family）] タブにアクセスできます。[BGP] ページの詳細については、BGP の設定 （2 ページ）を参照してください。

関連項目

- BGP について （4 ページ）
- [General] タブ （7 ページ）

フィールド リファレンス

表 *44 : IPv4* ファミリ：*[*集約アドレス（*Aggregate Address*）*]* タブ

要素	説明
IPv4ファミリの有効化（Enable IPv4 Family）	標準の 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の設定を有効にします。
一般	このパネルを使用して、[ベストパス選択（Best Path Selection）]、[ネイバータイマー（Neighbor Timers）]、[グレースフルリスタート（Graceful Restart）] などの一般的な IPv4 設定を設定します。これらの定義の詳細については、IPv4 Family - [全般（General）] タブ （11 ページ）を参照してください。

要素	説明
[Aggregate Address]	このパネルを使用して、特定のルートから 1 つのルートへの集約を定義します。 [Aggregate Timer] フィールドで、集約タイマーの値（秒）を指定します。有効な値は、0 または 6 ～ 60 の値です。デフォルト値は 30 です。 これらの定義の詳細については、[集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス （34 ページ）を参照してください。
フィルタリング	このパネルを使用して、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をフィルタ処理します。これらの定義の詳細については、[Add Filter]/[Edit Filter] ダイアログボックス （15 ページ）を参照してください。
ネイバー	このパネルを使用して、BGP ネイバーとネイバーの設定を定義します。これらの定義の詳細については、[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （16 ページ）を参照してください。
ネットワーク	このパネルを使用して、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します。これらの定義の詳細については、[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （27 ページ）を参照してください。
再配布	このパネルを使用して、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します。これらの定義の詳細については、[Add Redistribution]/[Edit Redistribution] ダイアログボックス （28 ページ）を参照してください。
ルートの挿入	このパネルを使用して、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します。これらの定義の詳細については、[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （29 ページ）を参照してください。

[IPv4ファミリ（IPv4 Family）] タブ：[全般（General）]タブ

フィールド リファレンス

表 *45 : [ISIS IPv4ファミリ（ISIS IPv4 Family）] タブ：[全般（General）]タブ*

要素	説明
隣接関係チェックの実行（Perform Adjacency Check）	[隣接関係チェックの実行（Perform Adjacency Check）] チェックボックスをオンにし、ルータが近隣の IS ルータをチェックするようにします。

要素	説明
距離	
アドミニストレーティブ ディスタンス（Administrative Distance）	[Administrative Distance] フィールドに、IS-IS プロトコルによって検出されたルートに割り当てるディスタンスを入力します。アドミニストレーティブ ディスタンスは、複数のルーティング プロトコル間でルートを比較するのに使用されるパラメータです。通常は、値が大きいほど、信頼性の格付けが下がります。255 のアドミニストレーティブ ディスタンスは、ルーティング情報源がまったく信頼できないため、無視すべきであることを意味します。指定できる範囲は 1 ～ 255 です。デフォルトは 115 です。
転送パスの最大数（Maximum No. of Forward Paths）	ルーティングテーブルにインストールできる IS ルートの最大数を入力します。指定できる範囲は 1 ～ 8 です。デフォルトは 4 です。
デフォルトルートの配布（Distribute Default Route）	[デフォルトルートの配布（Distribute Default Route）] チェックボックスをオンにしてデフォルトルートを配布するように IS ルーティングプロセスを設定し、[ルートマップオブジェクトセレクタ（Route Map Object Selector）] からデフォルトルートを選択します。
ISISメトリック（ISIS Metrics）	
グローバル ISIS メトリック レベル 1	メトリックを指定する数値を入力します。 範囲は、選択した TLV スタイルによって異なります。デフォルトは 10 です。 • [狭いメトリックで古いスタイルのTLVを使用する（Use old style of TLVs with narrow metric）] を選択した場合、範囲は 1 ～ 63 です。 • [より広いメトリックに対応する新しいスタイルのTLVを使用する（Use new style of TLVs to carry wider metric）] を選択した場合、範囲は 1 ～ 16777214 です。 • [移行中に両方のスタイルのTLVを送信して受け入れる（Send and accept both styles of TLVs during transition）] を選択した場合、範囲は 1 ～ 16777214 です。

要素	説明
グローバル ISIS メトリック レベル 2	メトリックを指定する数値を入力します。 範囲は、選択した TLV スタイルによって異なります。デフォルトは 10 です。 • [狭いメトリックで古いスタイルのTLVを使用する（Use old style of TLVs with narrow metric）] を選択した場合、範囲は 1 ～ 63 です。 • [より広いメトリックに対応する新しいスタイルのTLVを使用する（Use new style of TLVs to carry wider metric）] を選択した場合、範囲は 1 ～ 16777214 です。 • [移行中に両方のスタイルのTLVを送信して受け入れる（Send and accept both styles of TLVs during transition）] を選択した場合、範囲は 1 ～ 16777214 です。
TLV スタイル（TLV Style）	次のタイプ、長さ、および値のいずれかを選択します。 • 狭いメトリックで古いスタイルの TLV を使用する（Use old style of TLVs with narrow metric） • より広いメトリックに対応する新しいスタイルの TLV を使用する（Use new style of TLVs to carry wider metric） • 移行中に両方のスタイルの TLV を送信して受け入れる（Send and accept both styles of TLVs during transition）
移行中に両方のスタイルの TLV を受け入れる（Accept both styles of TLVs during transition）	このオプションは、[TLVスタイル（TLV Style）] で最初の 2 つのオプションのいずれかを選択した場合に選択できます。
メトリックスタイルの適用先（Apply metric style to）	次のいずれかを選択します。 • レベル 1 • レベル 2 • 両方 デフォルトはレベル 1 です。

[IPv4ファミリ（IPv4 Family）] タブ：[SPF] タブ

フィールド リファレンス

表 *46 : [ISIS IPv4*ファミリ（*ISIS IPv4 Family*）*]* タブ：*[SPF]* タブ

要素	説明
[最短パス優先（Shortest Path First）]	
[SPF計算に外部メトリックを含める（Honour external metrics during SPF calculations）]	SPF 計算に外部メトリックを含めるには、このチェックボックスをオンにします。
[このルータをSPF計算の中間ホップとして使用しないように他のルータに通知する（Signal other routers to not use this router as an intermediate hop in their SPF calculations）]	このデバイスを除外する場合は、このチェックボックスをオンにして、以下を設定します。
[起動時の動作を指定（Specify on-startup behavior）]	このオプションを選択した場合は、次のいずれかのオプションを選択する必要があります。 • [BGP収束前に過負荷として自身をアドバタイズする（Advertise overself as overloaded until BGP has converged）] • [再起動後に過負荷として自身をアドバタイズする時間を指定する（Specify time to advertise overself as overloaded after reboot）]：5 ～ 86400 秒の範囲で時間を指定します。
[過負荷ビットが設定されている場合に他のプロトコルから学習されたIPプレフィックスをアドバタイズしない（Don't advertise IP prefixes learned from other protocols when overload bit is set）]	IP プレフィックスを除外するには、このチェックボックスをオンにします。
[過負荷ビットが設定されている場合に別のISISレベルから学習されたIPプレフィックスをアドバタイズしない（Don't advertise IP prefixes learned from another ISIS level when overload bit is set）]	IP プレフィックスを除外するには、このチェックボックスをオンにします。
部分ルート計算の最小間隔	
[PRC間隔（PRC Interval）]	ルータが部分ルート計算（PRC）間で待機する時間を入力します。範囲は、1 ～ 120 秒です。デフォルトは 5 秒です。

要素	説明
[PRCの初期待機時間（Initial wait for PRC）]	トポロジ変更後の最初の PRC 計算遅延（ミリ秒単位）を入力します。有効値は 1 ～ 120.000 ミリ秒です。デフォルトは 2000 ミリ秒です。
[1番目と2番目のPRC間の最小待機時間（Minimum wait between first and second PRC）]	ルータが PRC 間で待機する時間（ミリ秒単位）を入力します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5000 ミリ秒です。
SPF 計算の最小間隔	
レベル 1 のパラメータの設定	
[SPF計算の間隔（SPF calculation interval）]	ルータが部分 SPF 計算間で待機する時間を入力します。範囲は、1 ～ 120 秒です。デフォルトは 10 秒です。
[SPF計算の初期待機時間（Initial wait for SPF calculation）]	ルータが SPF 計算で待機する時間を入力します。有効値は 1 ～ 120.000 ミリ秒です。デフォルトは 5500 ミリ秒です。
[1番目と2番目のSPF計算間の最小待機時間（Minimum wait between first and second SPF calculation）]	ルータが SPF 計算間で待機する時間（ミリ秒単位）を入力します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5500 ミリ秒です。
レベル 2 のパラメータの設定	
[SPF計算の間隔（SPF calculation interval）]	ルータが部分 SPF 計算間で待機する時間を入力します。範囲は、1 ～ 120 秒です。デフォルトは 10 秒です。
[SPF計算の初期待機時間（Initial wait for SPF calculation）]	ルータが SPF 計算で待機する時間を入力します。有効値は 1 ～ 120.000 ミリ秒です。デフォルトは 5500 ミリ秒です。
[1番目と2番目のSPF計算間の最小待機時間（Minimum wait between first and second SPF calculation）]	ルータが SPF 計算間で待機する時間（ミリ秒単位）を入力します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5500 ミリ秒です。

IPv4 ファミリータブ：再配布タブ

[追加（Add）]/[編集（Edit）]ボタンを使用して、新しい再配布ルートを追加するか、既存の行を編集します。

フィールド リファレンス

表 *47 : ISIS IPv4* ファミリータブ：再配布タブ

要素	説明
ソース プロトコル	[Source Protocol] ドロップダウン リストから、ISIS ドメインにルートを再配布するプロトコル（[BGP]、[Connected]、[EIGRP]、[OSPF]、[RIP]、または [Static]）を選択します。
プロセス ID（Process ID）	送信元プロトコルのプロセス ID を入力します。
ルートレベル	[Route Level] ドロップダウン リストから、[Level-1]、[Level- 2]、または [Level 1-2] を選択します。
メトリック（Metric）	[メトリック（Metric）] フィールドに、再配布されるルートのメトリックを入力します。指定できる範囲は 1 ～ 4294967295 です。
メトリック タイプ	[Metric Type] で、[internal] または [external] オプション ボタンをクリックします。
ISIS エリア間ルートレベル	
送信元 ISIS レベル	レベル 1 またはレベル 2 を選択します。デフォルトはレベル 1 です。
接続先 ISIS レベル	レベル 1 またはレベル 2 を選択します。デフォルトはレベル 1 です。
[同報リスト（Distribution List）]	利用可能なアクセス制御リストから選択するか、新規に追加します。
ルート マップ	[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から、再配布するネットワークをフィルタ処理するために調べる必要があるルートマップを選択するか、[追加（Add）] をクリックして、新しいルートマップを追加するか、既存のルートマップを編集します。
一致（Match）	[Match] チェックボックス（[Internal]、[External 1]、[External 2]、[NSSA External 1]、[NSSA External 2] チェックボックス）を 1 つ以上オンにして、OSPF ネットワークからルートを再配布します。

[IPv6ファミリ（IPv6 Family）] タブ

[BGP] ページの [IPv6 ファミリ（IPv6 Family）] タブを使用して、BGP の IPv6 設定を有効にして設定します。

ナビゲーション パス

[BGP] ページから [IPv6 ファミリ（IPv6 Family）] タブにアクセスできます。[BGP] ページの詳細については、BGP の設定 （2 ページ）を参照してください。

関連項目

- BGP について （4 ページ）
- [General] タブ （7 ページ）

フィールド リファレンス

表 *48 : IPv6* ファミリ：*[*集約アドレス（*Aggregate Address***）*]* タブ**

要素	説明
[IPv6 ファミリの有効化（Enable IPv6 Family）]	標準の 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の設定を有効にします。
一般	このパネルを使用して、一般的な IPv6 設定を指定します。これらの定義の詳細については、[IPv6 ファミリ（IPv6 Family）] : [全般（General）] タブ （32 ページ）を参照してください。
[Aggregate Address]	このパネルを使用して、特定のルートから 1 つのルートへの集約を定義します。 [Aggregate Timer] フィールドで、集約タイマーの値（秒）を指定します。有効な値は、0 または 6 ～ 60 の値です。デフォルト値は 30 です。 これらの定義の詳細については、[集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス （34 ページ）を参照してください。
ネイバー	このパネルを使用して、BGP ネイバーとネイバーの設定を定義します。これらの定義の詳細については、[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （36 ページ）を参照してください。
ネットワーク	このパネルを使用して、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します。これらの定義の詳細については、[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （46 ページ）を参照してください。
再配布	このパネルを使用して、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します。これらの定義の詳細については、[Add Redistribution]/[Edit Redistribution] ダイアログボックス （47 ページ）を参照してください。

要素	説明
ルートの挿入	このパネルを使用して、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します。これらの定義の詳細については、[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （48 ページ）を参照してください。

[IPv6ファミリ（IPv6 Family）] タブ：[全般（General）]タブ

フィールド リファレンス

表 *49 : [ISIS IPv6ファミリ（ISIS IPv6 Family）] タブ：[全般（General）]タブ*

要素	説明
隣接関係チェックの実行（Perform Adjacency Check）	[隣接関係チェックの実行（Perform Adjacency Check）] チェックボックスをオンにし、ルータが近隣のISルータをチェックするようにします。
距離	
アドミニストレーティブディスタンス（Administrative Distance）	[アドミニストレーティブディスタンス（Administrative Distance）] フィールドに、IS-ISプロトコルによって検出されたルートに割り当てるディスタンスを入力します。アドミニストレーティブディスタンスは、複数のルーティングプロトコル間でルートを比較するのに使用されるパラメータです。通常は、値が大きいほど、信頼性の格付けが下がります。255 のアドミニストレーティブディスタンスは、ルーティング情報源がまったく信頼できないため、無視すべきであることを意味します。指定できる範囲は 1 ～ 255 です。デフォルトは 115 です。
転送パスの最大数（Maximum No. of Forward Paths）	ルーティングテーブルにインストールできるISルートの最大数を入力します。指定できる範囲は 1 ～ 8 です。デフォルトは 4 です。
デフォルトルートの配布（Distribute Default Route）	[デフォルトルートの配布（Distribute Default Route）] チェックボックスをオンにしてデフォルトルートを配布するようにISルーティングプロセスを設定し、[ルートマップオブジェクトセレクタ（Route Map Object Selector）] からデフォルトルートを選択します。

[IPv6ファミリ（IPv6 Family）] タブ：[SPF] タブ

フィールド リファレンス

表 50 : [ISIS IPv6ファミリ（ISIS IPv6 Family）] タブ：[SPF] タブ

要素	説明
[最短パス優先（Shortest Path First）]	
[このルータをSPF計算の中間ホップとして使用しないように他のルータに通知する（Signal other routers to not use this router as an intermediate hop in their SPF calculations）]	このデバイスを除外する場合は、このチェックボックスをオンにして、以下を設定します。
[起動時の動作を指定（Specify on-startup behavior）]	このオプションを選択した場合は、次のいずれかのオプションを選択する必要があります。 • [BGP収束前に過負荷として自身をアドバタイズする（Advertise overself as overloaded until BGP has converged）] • [再起動後に過負荷として自身をアドバタイズする時間を指定する（Specify time to advertise overself as overloaded after reboot）]：5 ～ 86400 秒の範囲で時間を指定します。
[過負荷ビットが設定されている場合に他のプロトコルから学習されたIPプレフィックスをアドバタイズしない（Don't advertise IP prefixes learned from other protocols when overload bit is set）]	IP プレフィックスを除外するには、このチェックボックスをオンにします。
[過負荷ビットが設定されている場合に別のISISレベルから学習されたIPプレフィックスをアドバタイズしない（Don't advertise IP prefixes learned from another ISIS level when overload bit is set）]	IP プレフィックスを除外するには、このチェックボックスをオンにします。
部分ルート計算の最小間隔	
[PRC間隔（PRC Interval）]	ルータが部分ルート計算（PRC）間で待機する時間を入力します。範囲は、1 ～ 120 秒です。デフォルトは 5 秒です。
[PRCの初期待機時間（Initial wait for PRC）]	トポロジ変更後の最初の PRC 計算遅延（ミリ秒単位）を入力します。有効値は 1 ～ 120.000 ミリ秒です。デフォルトは 2000 ミリ秒です。

要素	説明
[1番目と2番目のPRC間の最小待機時間（Minimum wait between first and second PRC）]	ルータが PRC 間で待機する時間（ミリ秒単位）を入力します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5000 ミリ秒です。
SPF 計算の最小間隔	
レベル 1 のパラメータの設定	
[SPF計算の間隔（SPF calculation interval）]	ルータが部分 SPF 計算間で待機する時間を入力します。範囲は、1 ～ 120 秒です。デフォルトは 10 秒です。
[SPF計算の初期待機時間（Initial wait for SPF calculation）]	ルータが SPF 計算で待機する時間を入力します。有効値は 1 ～ 120.000 ミリ秒です。デフォルトは 5500 ミリ秒です。
[1番目と2番目のSPF計算間の最小待機時間（Minimum wait between first and second SPF calculation）]	ルータが SPF 計算間で待機する時間（ミリ秒単位）を入力します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5500 ミリ秒です。
レベル 2 のパラメータの設定	
[SPF計算の間隔（SPF calculation interval）]	ルータが部分 SPF 計算間で待機する時間を入力します。範囲は、1 ～ 120 秒です。デフォルトは 10 秒です。
[SPF計算の初期待機時間（Initial wait for SPF calculation）]	ルータが SPF 計算で待機する時間を入力します。有効値は 1 ～ 120.000 ミリ秒です。デフォルトは 5500 ミリ秒です。
[1番目と2番目のSPF計算間の最小待機時間（Minimum wait between first and second SPF calculation）]	ルータが SPF 計算間で待機する時間（ミリ秒単位）を入力します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5500 ミリ秒です。

IPv6 ファミリータブ：再配布タブ

[追加（Add）]/[編集（edit）] ボタンを使用して、再配布ルートを追加または編集します。

フィールド リファレンス

表 *51 : ISIS IPv6* ファミリータブ：再配布タブ

要素	説明
ソース プロトコル	[Source Protocol] ドロップダウン リストから、ISIS ドメインにルートを再配布するプロトコル（[BGP]、[Connected]、[EIGRP]、[OSPF]、[RIP]、または [Static]）を選択します。
プロセス ID（Process ID）	送信元プロトコルのプロセス ID を入力します。
ルートレベル	[Route Level] ドロップダウン リストから、[Level-1]、[Level- 2]、または [Level 1-2] を選択します。
メトリック（Metric）	[メトリック（Metric）] フィールドに、再配布されるルートのメトリックを入力します。指定できる範囲は 1 ～ 4294967295 です。
メトリック タイプ	[Metric Type] で、[internal] または [external] オプション ボタンをクリックします。
ISIS エリア間ルートレベル	
送信元 ISIS レベル	レベル 1 またはレベル 2 を選択します。デフォルトはレベル 1 です。
接続先 ISIS レベル	レベル 1 またはレベル 2 を選択します。デフォルトはレベル 1 です。
[同報リスト（Distribution List）]	利用可能なアクセス制御リストから選択するか、新規に追加します。
ルート マップ	[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から、再配布するネットワークをフィルタ処理するために調べる必要があるルートマップを選択するか、[追加（Add）] をクリックして、新しいルートマップを追加するか、既存のルートマップを編集します。
一致（Match）	[Match] チェックボックス（[Internal]、[External 1]、[External 2]、[NSSA External 1]、[NSSA External 2] チェックボックス）を 1 つ以上オンにして、OSPF ネットワークからルートを再配布します。

IPv6 Familyタブ：サマリープレフィックス

続行するには、少なくとも 1 つのネットワーク エンティティ タイトルのエントリを設定する必要があります。

詳細については、[ネットワーク エンティティ タイトル（Network Entity Title）] タブ （110 ページ）を参照してください。

[追加/編集（Add/Edit）] ボタンを使用して、サマリープレフィックスを追加または編集します。

フィールド リファレンス

表 *52 : ISIS IPv6* ファミリタブ：サマリープレフィックスタブ

要素	説明
IPv6 Summary Prefix	X.X.X.X.::X/0-128 形式の IPv6 プレフィックス。
Apply Summary Prefix into	レベル 1、レベル 2、または両方を選択します。 レベル 1：設定済みアドレスとマスク値を使用して、レベル 1 に再配布されたルートのみが集約されます。 レベル 2：設定済みアドレスとマスク値を使用して、レベル 1 ルーティングが学習したルートがレベル2バックボーンに集約されます。レベル 2 の IS-IS に再配布されたルートも集約されます。 両方：ルートをレベル 1 およびレベル 2 IS-IS に再配布したとき、レベル 2 IS-IS がレベル 1 ルートをエリアで到達可能なものとしてアドバタイズするとき、集約経路が適用されます。

[Authentication] タブ

フィールド リファレンス

表 *53 : [ISIS*認証（*Authentication*）*]* タブ

要素	説明
レベル 1 の認証パラメータを設定します。	
タイプ（Type）	ドロップダウン リストから [タイプ（Type）] を選択します。
キー（Key）	ISIS 更新を認証するためのキーを入力します。このキーの最大長は 16 文字です。
確認（Confirm）	キーを確認します。
[送信のみ（Send Only）]	[送信のみ（Send Only）] を有効にするかどうかに応じて、[有効化（Enable）] または [無効化（Disable）] をクリックします。

要素	説明
[モード（Mode）]	認証モードを選択するため、[無効（Disabled）]、[MD5]、[プレーンテキスト（Plaintext）] オプションボタンのいずれかをオンにします。
[エリアパスワード（Area password）]	エリアパスワードを入力し、次のテキストボックスに同じパスワードを入力して確認します。
レベル 2 の認証パラメータを設定します。	
タイプ（Type）	ドロップダウン リストから [タイプ（Type）] を選択します。
キー（Key）	ISIS 更新を認証するためのキーを入力します。このキーの最大長は 16 文字です。
確認（Confirm）	キーを確認します。
[送信のみ（Send Only）]	[送信のみ（Send Only）] を有効にするかどうかに応じて、[有効化（Enable）] または [無効化（Disable）] をクリックします。
[モード（Mode）]	認証モードを選択するため、[無効（Disabled）]、[MD5]、[プレーンテキスト（Plaintext）] オプションボタンのいずれかをオンにします。
ドメイン パスワード	ドメインパスワードを入力し、入力したパスワードを確認します。

リンクステートパケット タブ

フィールド リファレンス

表 *54 : [ISIS*リンクステートパケット（*ISIS Link State Packet***）*]* タブ**

要素	説明
[LSPエラーを無視（Ignore LSP errors）]	[LSPエラーを無視（Ignore LSP errors）] チェックボックスをオンにすると、内部チェックサムエラーのある受信 LSP パケットを、ASA がパージするのではなく無視できるようになります。

要素	説明
[SPFを実行する前にLSPをフラッド（Flood LSPs before running SPF）]	SPF を実行する前に LSP を高速フラッディングおよびフィルするには、このボックスをオンにします。このオプションを選択した場合は、フラッディングする LSP の数を 1 ～ 15 の範囲で入力します。 このパラメータでは、指定した数の LSP が ASA から送信されます。LSP 数が指定されない場合、デフォルト設定は5となります。LSP は、SPF の実行前に SPF を呼び出します。高速フラッディングを有効にすることをお勧めします。それにより、LSPのフラッディングプロセスの速度が上げり、ネットワークコンバージェンス時間全体が改善されるからです。デフォルト値は 5 です。
[IPプレフィックスを抑制（Suppress IP prefixes）]	IP プレフィックスを抑制するには、[IPプレフィックスを抑制（Suppress IP prefixes）] チェックボックスをオンにし、以下の 1 つをオンにします。 IS-IS への再配布ルート数に制限がないネットワークでは、LSP がフルになってルートが破棄される可能性があります。これらのオプションを使用することにより、PDU がフルになった場合にどのルートが抑制されるかを制御してください。
[LSPフラグメントが不足した場合に別のISISレベルから学習されたIPプレフィックスをアドバタイズしない（Don’t advertise IP prefixes learned from another ISIS level when ran out of LSP fragments）]	別のレベルから来るルートを抑制します。たとえば、レベル2の LSP がフルになると、レベル 1 からのルートが抑制されます。
[LSPフラグメントが不足した場合に他のプロトコルから学習されたIPプレフィックスをアドバタイズしない（Don’t advertise IP prefixes learned from other protocols when ran out of LSP fragments）]	ASA 上にある再配布済みルートを抑制します。
[LSPの一般的な間隔（LSP General Interval）]	
レベル 1 の LSP 間隔パラメータ	

要素	説明
[LSP計算間隔（LSP Calculation Interval）]	各 LSP の伝送間の間隔を秒数で入力します。範囲は 1 ～ 120 秒です。デフォルトは 5 分です。 接続ネットワーク上の任意の 2 台の ASA 間で想定されるラウンドトリップ遅延より大きな数値にする必要があります。この数は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。再送信が発生するのは、LSP が廃棄される場合だけです。したがって、数を大きい値に設定すると、再コンバージェンスへの影響は小さくなります。ASA のネイバーが多くなるほど、LSP フラッディングの可能性のあるパスが多くなり、この値をより高く設定できます。
[LSP計算の初期待機時間（Initial wait for LSP calculation）]	最初の LSP が生成されるまでの初期待機時間をミリ秒単位で入力します。指定できる範囲は 1 ～ 120,000 です。デフォルトは 50 です。
[1番目と2番目の間の最小待機時間（Minimum wait between first and second）]	最初と 2 番目の LSP 生成の間の時間をミリ秒単位で入力します。指定できる範囲は 1 ～ 120,000 です。デフォルト値は 5000 です。
レベル 2 の LSP 間隔パラメータ	
[レベル2にもレベル1パラメータを使用する（Use level 1 parameter also for level 2）]	レベル 1 に設定した値をレベル 2 にも適用する場合は、[Use level 1 parameters also for level 2] チェック ボックスをオンにします。
[LSP計算間隔（LSP Calculation Interval）]	各 LSP の伝送間の間隔を秒数で入力します。範囲は 1 ～ 120 秒です。デフォルトは 5 分です。 接続ネットワーク上の任意の 2 台の ASA 間で想定されるラウンドトリップ遅延より大きな数値にする必要があります。この数は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。再送信が発生するのは、LSP が廃棄される場合だけです。したがって、数を大きい値に設定すると、再コンバージェンスへの影響は小さくなります。ASA のネイバーが多くなるほど、LSP フラッディングの可能性のあるパスが多くなり、この値をより高く設定できます。
[LSP計算の初期待機時間（Initial wait for LSP calculation）]	最初の LSP が生成されるまでの初期待機時間をミリ秒単位で入力します。指定できる範囲は 1 ～ 120,000 です。デフォルトは 50 です。
[1番目と2番目の間の最小待機時間（Minimum wait between first and second）]	最初と 2 番目の LSP 生成の間の時間をミリ秒単位で入力します。指定できる範囲は 1 ～ 120,000 です。デフォルト値は 5000 です。

要素	説明
[最大LSPサイズ（Maximum LSP size）]	[最大LSPサイズ（Maximum LSP size）] フィールドに秒数を入力します。指定できる範囲は 128 ～ 4352 です。デフォルトは 1492 です。
LSP リフレッシュ インターバル	[LSP refresh interval] フィールドには、LSP 更新間隔の秒数を入力します。指定できる範囲は 1 ～ 65,5535 です。デフォルトは 900 です。 リフレッシュ間隔によって、ソフトウェアが定期的に LSP で発信元のルート トポロジ情報を送信するレートが決定されます。これは、データベース情報が古くなるのを避けるために実行されます。 リフレッシュ間隔を短くすると、増加したリンク利用率のコストで未検出のリンク ステート データベース破損が持続する可能性のある期間が短くなります（破損に対する他の予防措置があるため、これは発生する可能性は極めて低いイベントです）。間隔を長くすると、更新されたパケットのフラッディングによるリンク使用率が低下します（ただしこの使用率は非常に低いです）。
最大 LSP ライフタイム	[Maximum LSP lifetime] フィールドには、ルータのデータベース内に更新なしで LSP が保持される最大秒数を入力します。指定できる範囲は 1 ～ 65535 です。デフォルトは 1200（20 分）です。 LSP の更新間隔を変更した場合、このパラメータを調整する必要があるかもしれません。LSP は、ライフタイムが経過するまで定期的にリフレッシュされる必要があります。LSP 更新間隔に設定する値は LSP 最大ライフタイムに設定する値よりも小さな値である必要があり、そうでない場合、リフレッシュされる前に LSP がタイムアウトします。LSP 更新間隔と比べて LSP ライフタイムを大幅に少なく設定すると、LSP 更新間隔が自動的に短くされて、LSP がタイムアウトしないようになります。

[サマリーアドレス（Summary Address）] タブ

[追加/編集（Add/Edit）] ボタンを使用して、サマリーアドレスを追加または編集します。

フィールド リファレンス

表 *55 : [ISIS*サマリーアドレス（*ISIS Summary Address*）] タブ

要素	説明
IP アドレス	サマリールートの IP アドレスを入力します。
ネット マスク（Net Mask）	IP アドレスに適用されるネットワークマスクを選択または入力します。
レベルの選択（Select level）	サマリーアドレスを受信するレベルに応じて、[Level 1]、[Level 2]、または [Level 1 and 2] オプション ボタンをオンにします。
タグ	[Tag] フィールドに、タグの番号を入力します。範囲は 1 ～ 4294967295 です。
メトリック（Metric）	[メトリック（Metric）] フィールドに、サマリールートに適用するメトリックを入力します。範囲は 1 ～ 4294967295 です。デフォルト値は 10 です。

[ネットワーク エンティティ タイトル（Network Entity Title）] タブ

[追加（Add）]/[編集（Edit）] ボタンを使用して、ネットワーク エンティティ タイトルを追加および編集します。

フィールド リファレンス

表 *56 : [ISIS* ネットワーク エンティティ タイトル（*ISIS Network Entity Title*）] タブ

要素	説明
[ネットワーク エンティティ タイトル（NET）（Network Entity Title (NET)）]	アドレス形式48.0000.1111.2222.00 で値を入力します。NET アドレスの合計の長さは 16 ～ 40 文字である必要があります。

要素	説明
[NET プール（NET Pool）]	[選択（Select）] をクリックして、[NET プールオブジェクトセレクタ（NET Pool Object Selector）] ダイアログボックスを開きます。このダイアログボックスを使用すると、NET プールオブジェクトを追加および編集できます。NET プールオブジェクトを追加または編集する方法の詳細については、[NETプールオブジェクトの追加/編集（Add or Edit NET Pool Object）] ダイアログボックスを参照してください。 NET プールは、個別モードのクラスタデバイスにのみ適用されます。 ネットワーク エンティティ タイトル（NET）は、個別モードのクラスタデバイスには適用されません。
[NET の許容最大数（Maximum allowed NET）]	NET 値を 3 ～ 254 の範囲で入力します。デフォルト値は 3 です。

[Interface] タブ

[Interface] タブを使用して、インターフェイス固有の OSPF 認証ルーティング プロパティを設定します。

ナビゲーション パス

[Interface] タブには、[OSPF] ページからアクセスできます。[OSPF] ページの詳細については、OSPF の設定 （129 ページ）を参照してください。

関連項目

- [Add Interface]/[Edit Interface] ダイアログボックス （163 ページ）

フィールド リファレンス

表 57 : [Interface] タブ

要素	説明
インターフェイス（Interface）	設定が適用されるインターフェイスの名前。

要素	説明
認証	インターフェイス上でイネーブルにするOSPF認証のタイプ。認証タイプには、次のいずれかの値を指定できます。 • [None]：OSPF 認証はディセーブルになります。 • [Password]：クリアテキストパスワード認証がイネーブルになります。 • [MD5]：MD5 認証がイネーブルになります。 • [Area]：エリアに対して指定された認証タイプがインターフェイスでイネーブルになります。エリア認証が、インターフェイスのデフォルト値です。ただし、エリア認証は、デフォルトではディセーブルになっています。そのため、あらかじめエリア認証タイプを指定してある場合を除いて、エリア認証を指定したインターフェイスでは認証がディセーブルになります。 • [キーチェーン（Key Chain）]：キーチェーン認証を許可します。
ポイントツーポイント	インターフェイスが非ブロードキャスト（ポイントツーポイント）に設定されている場合は「true」が表示されます。インターフェイスがブロードキャストに設定されている場合は、「false」が表示されます。
コスト（Cost）	インターフェイスを介したパケット送信のコスト。
プライオリティ	インターフェイスに割り当てられる OSPF プライオリティ。
MTU Ignore	MTU不一致検出がイネーブルの場合は、「false」が表示されます。MTU不一致検出がディセーブルの場合は「true」が表示されます。
Database Filter	同期およびフラッディング中に発信 LSA がフィルタリングされる場合は、「true」が表示されます。フィルタリングがイネーブルではない場合は「false」を表示します。
Hello 間隔（Hello Interval）	インターフェイス上で送信されるhelloパケット間の間隔（秒数）。hello間隔を小さくすると、トポロジ変更はより高速に検出されますが、インターフェイス上で送信されるトラフィックはより多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバーで同じである必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 10 秒です。

要素	説明
送信遅延（Transmit Delay）	インターフェイス上で LSA パケットを送信するために必要と推定される時間（秒数）。更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 1 秒です。
再送信間隔（Retransmit Interval）	インターフェイスに属する隣接関係へのLSA再送信間の時間（秒数）。ルータが自身のネイバーにLSAを送信する場合、ルータは確認応答メッセージを受信するまでそのLSAを保持します。確認応答を受信しなかった場合、ルータでは LSA を再送します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 5 秒です。
dead 間隔（Dead Interval）	hello パケットが受信されないために、ネイバーがルータ ダウンを宣言するまでの時間間隔（秒数）。有効値の範囲は1～65535 です。この設定のデフォルト値は、[Hello Interval] フィールドに設定されている時間間隔の 4 倍です。
Hello Multiplier （ASA 9.2(1) 以降のみ）	1 秒あたりに送信される hello パケットの数。有効な値は、3～20 です。

[インターフェイス（Interface）] タブ：[全般（General）] タブ

フィールド リファレンス

表 *58 : [ISIS* インターフェイス（*ISIS Interface*）*]* タブ：*[*全般（*General*）*]* タブ

要素	説明
インターフェイス（Interface）	使用可能なインターフェイスからインターフェイスを選択します。
[このインターフェイスでのISISのシャットダウン（Shutdown ISIS on this interface）]	[Shutdown ISIS on this interface]：設定パラメータを削除することなく、このインターフェイスの IS-IS プロトコルを無効化できます。IS-IS プロトコルはこのインターフェイスの隣接関係（アジャセンシー）を形成しません。ASA が生成した LSP にインターフェイスの IP アドレスが設定されます。

要素	説明
[このインターフェイスで ISIS を有効化（Enable ISIS on this interface）]	選択したインターフェイスで IS-IS プロトコルを有効にします。
[このインターフェイスで IPv6 ISIS を有効化（Enable IPv6 ISIS on this interface）]	選択したインターフェイスで IPv6 IS-IS ルーティングを有効にします。
[レベル 1 のプライオリティ（Priority for level 1）]	レベル 1 のプライオリティを設定します。プライオリティ値は、LAN 上の指定ルータまたは Designated Intermediate System（DIS）を決める際に使用されます。プライオリティは hello パケットでアドバタイズされます。最高のプライオリティを持つルータが DIS になります。指定できる範囲は 0 ～ 127 です。デフォルトは 64 です。
[レベル 2 のプライオリティ（Priority for level 2）]	レベル 2 のプライオリティを設定します。プライオリティ値は、LAN 上の指定ルータまたは Designated Intermediate System（DIS）を決める際に使用されます。プライオリティは hello パケットでアドバタイズされます。最高のプライオリティを持つルータが DIS になります。指定できる範囲は 0 ～ 127 です。デフォルトは 64 です。
タグ	この IP プレフィックスが ISIS LSP に設定されている場合に、インターフェイスに設定された IP アドレスにタグを設定します。
[レベル 1 の CSNP 間隔（CSNP Interval for level 1）]	レベル 1 のマルチアクセスネットワークにおける、CSNP の送信間隔の完全なシーケンス番号 PDU（CSNP）を秒数で設定します。このインターバルは指定ルータだけに適用されます。範囲は 0 ～ 65535 です。デフォルトは 10 秒です。
[レベル 2 の CSNP 間隔（CSNP Interval for level 2）]	レベル 2 のマルチアクセスネットワークにおける、CSNP の送信間隔の完全なシーケンス番号 PDU（CSNP）を秒数で設定します。このインターバルは指定ルータだけに適用されます。範囲は 0 ～ 65535 です。デフォルトは 10 秒です。
[隣接関係のフィルタ処理（Adjacency filter）]	IS-IS 隣接関係の確立をフィルタ処理します。
[すべてのエリアアドレスに一致（Match all area addresses）]	隣接関係（アジャセンシー）を受け入れるには、すべての NSAP アドレスがフィルタと一致する必要があります。 指定しない場合（デフォルト）、受け入れる隣接関係（アジャセンシー）に関するフィルタに一致する必要があるのは 1 つのアドレスだけです。

[インターフェイス（Interface）] タブ : [認証（Authentication）] タブ

フィールド リファレンス

表 *59 : [ISIS*インターフェイス（*ISIS Interfaces***）*]* タブ *- [*認証（***ISIS Interfaces***）*]* タブ**

要素	説明
レベル 1 パラメータ	
キー タイプ	[クリアテキスト（Clear Text）] または [暗号化（Encrypted）] を選択します。
キー（Key）	IS-IS 更新を認証するためのキーを入力します。範囲は 0 ～ 8 文字です。 [Key] オプションで設定されたパスワードが存在しない場合、キー認証は行われません。 （注） [キータイプ（Key Type）] を [クリアテキスト（Clear Text）] として選択した場合は、[キー（Key）] フィールドに最大 17 文字を入力できます。[キー タイプ（Key Type）] を [暗号化（Encrypted）] として選択した場合は、[キー（Key）] フィールドに最大 50 文字を入力できます。
送信のみ（Send only）	[Send only] については、[Enable] または [Disable] のオプション ボタンをクリックします。 [Send only] を選択すると、システムは SNP へのパスワードの挿入だけは行うようになりますが、SNP での受け取ったパスワードの確認は行われません。このキーワードは、ソフトウェアのアップグレード中、移行をスムーズに行うために使用します。デフォルトではディセーブルになっています。
[モード（Mode）]	[モード（Mode）] チェックボックスをオンにし、ドロップダウンリストから [MD5] または [テキスト（Text）] を選択します。
[パスワード（Password）]	パスワードを入力します。 （注） いずれかのモードを選択するか、パスワード値を入力できます。
レベル 2 パラメータ	
キー タイプ	[クリアテキスト（Clear Text）] または [暗号化（Encrypted）] を選択します。

要素	説明
キー（Key）	IS-IS 更新を認証するためのキーを入力します。範囲は 0 ～ 8 文字です。 [Key] オプションで設定されたパスワードが存在しない場合、キー認証は行われません。 （注） [キータイプ（Key Type）] を [クリアテキスト（Clear Text）] として選択した場合は、[キー（Key）] フィールドに最大 17 文字を入力できます。[キー タイプ（Key Type）] を [暗号化（Encrypted）] として選択した場合は、[キー（Key）] フィールドに最大 50 文字を入力できます。
送信のみ（Send only）	[Send only] については、[Enable] または [Disable] のオプション ボタンをクリックします。 [Send only] を選択すると、システムは SNP へのパスワードの挿入だけは行うようになりますが、SNP での受け取ったパスワードの確認は行われません。このキーワードは、ソフトウェアのアップグレード中、移行をスムーズに行うために使用します。デフォルトではディセーブルになっています。
[モード（Mode）]	[モード（Mode）] チェックボックスをオンにし、ドロップダウンリストから [MD5] または [テキスト（Text）] を選択します。
[パスワード（Password）]	パスワードを入力します。 （注） いずれかのモードを選択するか、パスワード値を入力できます。

[インターフェイス（Interface）] タブ：[Helloパディング（Hello Padding）] タブ

フィールド リファレンス

表 *60 : [ISIS*インターフェイス（*ISIS Interfaces*）*]* タブ：*[Hello*パディング（*Hello Padding*）*]* タブ

要素	説明
Hello Padding	Hello パディングを有効にします。 最大伝送ユニット（MTU）サイズになるまで IS-IS hello がパディングされます。IS-IS hello をフル MTU に埋め込むことにより、大きなフレームに関連した送信問題によるエラーや隣接インターフェイスの MTU 不一致によるエラーの検出が可能になります。
レベル 1 の最小保留時間 1 秒（Minimal holdtime 1 second for level 1）	LSP がレベル 1 で有効であり続ける保留時間（秒数）を有効にします。

要素	説明
レベル 1 の Hello 間隔（Hello interval for level 1）	レベル 1 の hello パケット間の時間の長さを秒数で指定します。指定できる範囲は 1 ～ 65535 です。デフォルトは 10 です。
レベル 2 の最小保留時間 1 秒（Minimal holdtime 1 second for level 2）	LSP がレベル 2 で有効であり続ける保留時間（秒数）を有効にします。
レベル 2 の Hello インターバル（Hello interval for level 2）	レベル 2 の hello パケット間の時間の長さを秒数で指定します。指定できる範囲は 1 ～ 65535 です。デフォルトは 10 です。
レベル 1 のHello 乗数（Hello multiplier for level 1）	ネイバーにおいて欠落できる IS-IS hello パケット数の最大値を指定します。欠落したパケット数がこの値を超えると、ASA は隣接がレベル 1 でダウンしていると宣言します。 IS-IS hello パケットでアドバタイズされる保持時間は、hello インターバルに hello 乗数を掛けた値に設定されます。ネイバーは、アドバタイズされた保持時間中に IS-IS hello パケットをまったく受信しなかった場合、このルータへの隣接がダウンしていると宣言します。保持時間（つまり、hello 乗数と hello インターバル）はインターフェイス単位で設定できます。また、1 つのエリア内のルータごとに別々の保持時間を設定できます。指定できる範囲は 3 ～ 1000 です。デフォルトは 3 です。
レベル 2 のHello 乗数（Hello multiplier for level 2）	ネイバーにおいて欠落できる IS-IS hello パケット数の最大値を指定します。欠落したパケット数がこの値を超えると、ASA は隣接がレベル 2 でダウンしていると宣言します。 IS-IS hello パケットでアドバタイズされる保持時間は、hello インターバルに hello 乗数を掛けた値に設定されます。ネイバーは、アドバタイズされた保持時間中に IS-IS hello パケットをまったく受信しなかった場合、このルータへの隣接がダウンしていると宣言します。保持時間（つまり、hello 乗数と hello インターバル）はインターフェイス単位で設定できます。また、1 つのエリア内のルータごとに別々の保持時間を設定できます。指定できる範囲は 3 ～ 1000 です。デフォルトは 3 です。
回線タイプの設定（Configure Circuit Type）	ローカルルーティング（レベル 1）、エリアルーティング（レベル 2）、またはローカルとエリアの両方のルーティング（レベル 1-2）のどれについてインターフェイスが設定されているかを指定します。

[インターフェイス（Interface）] タブ：[LSP設定（LSP Settings）] タブ

フィールド リファレンス

表 *61 : [ISIS*インターフェイス（*ISIS Interfaces*）*]* タブ *- [LSP*設定（*LSP Settings*）*]* タブ

要素	説明
ISISプレフィックスのアドバタイズ（Advertise ISIS Prefix）	IS-IS インターフェイスごとの LSP アドバタイズメントで、接続されたネットワークの IP プレフィックスのアドバタイズを許可します。 このオプションを無効にすることは、LSP アドバタイズメントから、接続されたネットワークの IP プレフィックスを除外し、IS-IS コンバージェンス時間を削減するための IS-IS メカニズムです。
再送信間隔（Retransmit Interval）	ポイントツーポイントリンク上にある各 IS-IS LSP の再送信間隔を秒単位で指定します。 接続ネットワーク上の任意の 2 台のルータ間で想定される往復遅延より大きな数値にする必要があります。指定できる範囲は 0 ～ 65535 です。デフォルトは 5 分です。
Retransmit Throttle Interval	ポイントツーポイント インターフェイス上にある各 IS-IS LSP の再送信間隔をミリ秒単位で指定します。 このオプションは、LSP 再送信トラフィックの制御方法として、多くの LSP およびインターフェイスを持つ大規模なネットワークで役立つ場合があります。このオプションは、インターフェイスで LSP を再送信できるレートを制御します。指定できる範囲は 0 ～ 65535 です。デフォルトは 33 です。
LSP Interval	連続した IS-IS LSP 伝送間の遅延時間をミリ秒単位で指定します。 多数の IS-IS ネイバーやインターフェイスが存在するトポロジでは、LSP 送信および受信を原因とする CPU 負荷が、ルータの障害となる可能性があります。このオプションにより、LSP の送信率（および、暗黙のうちにその他のシステムの受信率）を下げることができます。指定できる範囲は 1 ～ 4294967295 です。デフォルトは 33 です。

[インターフェイス（Interface）] タブ：[メトリック（Metrics）] タブ

フィールド リファレンス

表 *62 : [ISIS*インターフェイス（*ISIS Interface*）*]* タブ：*[*メトリック（*Metrics*）*]* タブ

要素	説明
レベル 1 の指標	

要素	説明
最大メトリック値を使用（Use maximum metric value）	リンクに割り当てるメトリックを指定します。このメトリックは、このリンクを通じてネットワーク内の他の各ルータからその他の宛先へのコストの計算に使用されます。この設定はデフォルトでイネーブルになっています。
デフォルト メトリック	メトリックの番号を入力します。指定できる範囲は 1 ～ 16777214 です。
レベル 2 の指標	
最大メトリック値を使用（Use maximum metric value）	リンクに割り当てるメトリックを指定します。このメトリックは、このリンクを通じてネットワーク内の他の各ルータからその他の宛先へのコストの計算に使用されます。この設定はデフォルトでイネーブルになっています。
デフォルト メトリック	メトリックの番号を入力します。指定できる範囲は 1 ～ 16777214 です。

[パッシブインターフェイス（Passive Interfaces）] タブ

[パッシブインターフェイス（Passive Interfaces）] タブでは、インターフェイスでのルーティングの更新を許可または抑制できます。名前が設定されているインターフェイスのみ、ルーティング更新の送信を抑制できます。

フィールド リファレンス

表 *63 : [ISIS* ネットワーク エンティティ タイトル（*ISIS Network Entity Title*）*]* タブ

要素	説明
パッシブ インターフェイス	次のオプションから選択します。 • [なし（None）] : インターフェイスは選択されません。 • [デフォルト（Default）] : [インターフェイスセレクタ（Interfaces Selector）] ダイアログを開き、除外するインターフェイスを選択します。デフォルトでは、すべてのインターフェイスが選択されます。 • [指定されたインターフェイス（Specified Interfaces）] : [インターフェイスセレクタ（Interfaces Selector）] ダイアログを開き、含めるインターフェイスを選択します。

BFD ルーティングの設定

[BFD] ページには、ファイアウォールデバイスで BFD（Bidirectional Forwarding Detection）ルーティングを設定するための2つのタブがあります。以下のトピックでは、BFD の設定について詳しく説明します。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [ルーティング（Routing）] > [BFD]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [BFD]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- BFD について （120 ページ）
- BFD テンプレートの作成 （125 ページ）
- [BFDマップの追加/編集（Add/Edit BFD Map）] ダイアログボックス （127 ページ）
- [BFDインターフェイスの追加/編集（Add/Edit BFD Interface）] ダイアログボックス （128 ページ）

BFD について

双方向フォワーディング検出（BFD）は、すべてのメディアタイプ、カプセル化、トポロジ、およびルーティング プロトコルのために短時間での転送パス障害検出を提供するために設計された検出プロトコルです。BFD は、2 つのシステム間の転送データ プロトコルすべてに加えて、ユニキャストのポイントツーポイントモードで動作します。パケットは、メディアやネットワークに対して適切なカプセル化プロトコルのペイロードで送信されます。

BFD は高速転送パス障害検出に加えて、ネットワーク管理者に一貫した障害検出方法を提供します。ネットワーク管理者は BFD を使用することで、さまざまなルーティング プロトコルの HELLO メカニズムにより、変動速度ではなく一定速度で転送パス障害を検出できるため、ネットワーク プロファイリングおよびプランニングが容易になります。また、再収束時間の整合性が保たれ、予測可能になります。

BFD 非同期モードおよびエコー機能

BFD は、エコー機能が有効であるかどうかに関わらず非同期モードで動作できます。

非同期モード

非同期モードでは、システムが相互に BFD 制御パケットを定期的に送信します。一方のシステムがこれらのパケットの多くを連続して受信しない場合、セッションはダウンしているものと宣言されます。純粋な非同期モード（エコー機能なし）では、エコー機能に必要な特定の検出時間を達成するのに必要なパケットの数が半分で済むため、便利です。

BFD エコー機能

BFD エコー機能は、フォワーディング エンジンから、直接接続シングル ホップ BFD ネイバーへエコー パケットを送信します。エコー パケットはフォワーディング エンジンによって送信され、検出を実行するために同じパスに沿って返信されます。もう一方の BFD セッションは、エコー パケットの実際のフォワーディングに参加しません。エコー機能およびフォワーディング エンジンが検出プロセスを処理するため、BFD ネイバー間で送信される BFD 制御パケットの数が減少します。また、フォワーディング エンジンがリモート ネイバー システムでフォワーディング パスをテストする際にリモート システムが関与しないため、パケット間の遅延のばらつきが改善します。この結果、障害検出にかかる時間が短くなります。

エコー機能が有効な場合、BFD はスロー タイマーを使用して、非同期セッションの時間を長くし、BFD ネイバー間で送信される BFD 制御パケットの数を減らすことができます。これにより、処理オーバーヘッドが削減し、同時に障害検出時間が短くなります。

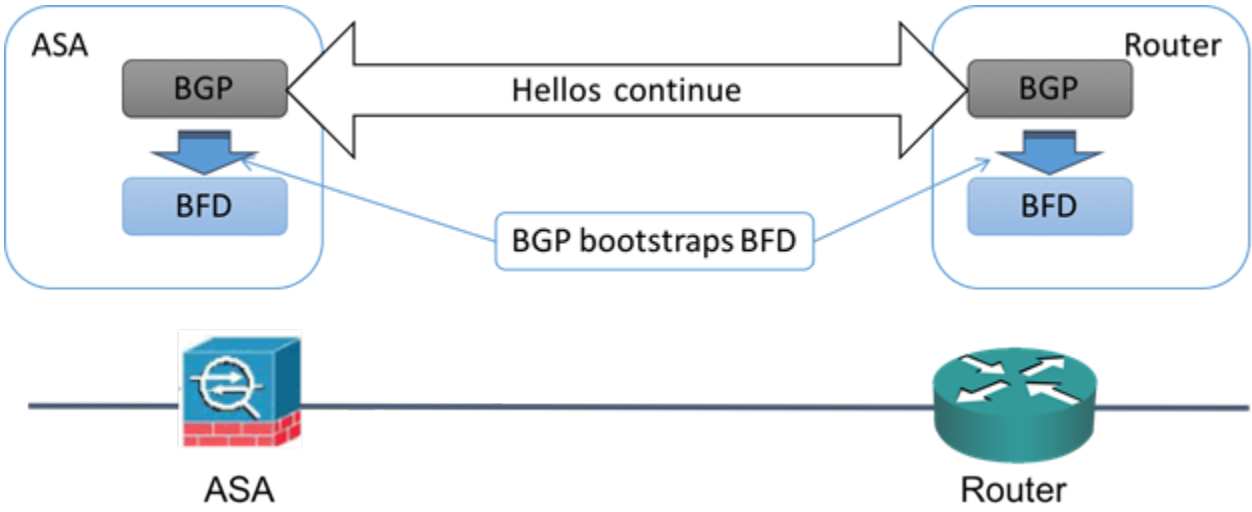
（注） IPv4 マルチホップまたは IPv6 シングルホップ BFD ネイバーでは、エコー機能はサポートされていません。

BFD はインターフェイス レベルとルーティング プロトコル レベルで有効にできます。両方のシステム（BFD ピア）で BFD を設定する必要があります。インターフェイスと、該当するルーティング プロトコルのルータ レベルで BFD を有効にすると、BFD セッションが作成され、BFD タイマーがネゴシエートされ、BFD ピアが BFD コントロール パケットをネゴシエートされたレベルで相互に送信し始めます。

BFD セッション確立

次の例は、ボーダー ゲートウェイ プロトコル（BGP）を実行している ASA とネイバールータを示しています。両方のデバイスが起動した時点では、デバイス間に BFD セッションは確立されていません。

図 *1: BFD* セッションの開始



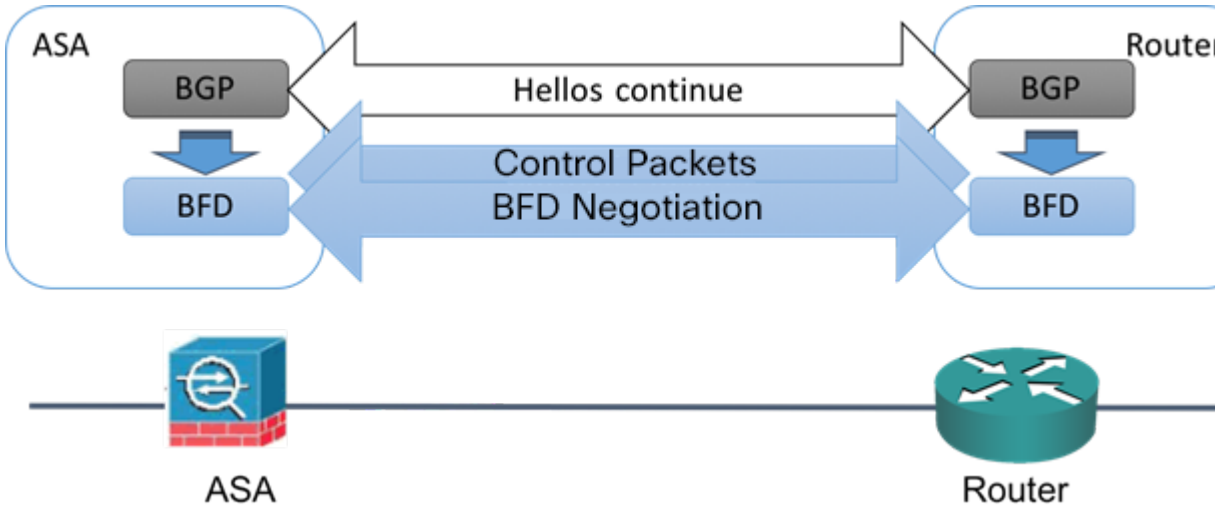
BGP は、BGP ネイバーの特定後に、そのネイバーの IP アドレスを使用して BFD プロセスをブートストラップします。BFD はそのピアを動的に検出しません。BFD は、設定されているルーティング プロトコルから、使用する IP アドレスと形成するピア関係を把握します。

ルータの BFD と ASA の BFD により BFD 制御パケットが形成され、BFD セッションが確立されるまで 1 秒間隔でこのパケットが相互に送信されます。両方のシステムの最初の制御パケットは非常によく似ています。たとえば、Vers、Diag、H、D、P、および F ビットはすべてゼロに設定され、State は Down に設定されます。[My Discriminator] フィールドには、送信デバイスで一意の値が設定されます。[Your Discriminator] フィールドにはゼロが設定されます。これは、BFD セッションがまだ確立されていないためです。TX タイマーと RX タイマーには、デバイスの設定で検出された値が設定されます。

リモート BFD デバイスは、セッション開始フェーズで BFD 制御パケットを受信すると、[My Discriminator] フィールドの値をデバイス自体の [Your Discriminator] フィールドに設定し、[Down] 状態から [Init] 状態、そして最終的には [Up] 状態に移行します。両方のシステムが、相互の制御パケットで各自の Discriminator を検出すると、セッションが正式に確立されます。

次の図は、確立された BFD 接続を示します。

図 *2 : BFD* セッションの確立



BFD タイマー ネゴシエーション

BFD デバイスは、BFD 制御パケットの送信速度を制御および同期するため、BFD タイマーをネゴシエートする必要があります。

BFD タイマーをネゴシエートする前に、デバイスは以下の点を確認する必要があります。

- そのピア デバイスが、ローカル デイバスの提示されるタイマーを含むパケットを確認している。
- ピアで設定されている BFD 制御パケットの受信速度を上回る速度でデバイスが BFD 制御パケットを送信することがない。
- ローカル システムで設定されている BFD 制御パケットの受信速度を上回る速度でピアが BFD 制御パケットを送信することがない。

[Your Discriminator] フィールドと H ビットの設定は、初期タイマーの期間中にリモート デバイスがそのパケットを確認するローカルデバイスを交換できるようにするのに十分です。各システムは BFD 制御パケットを受信すると、Required Min RX Interval をシステム自体の Desired Min TX Interval と比較し、2 つの値のうち大きい方の値（低速な値）を、BDF パケットの転送速度として使用します。2 つのシステムのうち低速なシステムによって、転送速度が決定します。

これらのタイマーがネゴシエートされていない場合、セッション中の任意の時点で、セッションをリセットすることなく再ネゴシエートできます。タイマーを変更するデバイスは、F ビットがセットされている BFD 制御パケットをリモート システムから受信するまで、後続のすべての BFD 制御パケットの P ビットをセットします。このビット交換により、転送中に失われる可能性があるパケットが保護されます。

（注） リモート システムによって F ビットがセットされている場合、新たに提示されるタイマーをリモート システムが受け入れることを意味しているわけではありません。これは、タイマーが変更されたパケットをリモート システムが確認したことを意味します。

BFD 障害検出

BFD セッションとタイマーがネゴシエートすると、BFD のピアは、ネゴシエートされた間隔で BFD 制御パケットを相互に送信します。これらの制御パケットはハートビートの役割を果たします。これは、IGP Hello プロトコルとよく似ていますが、レートはさらに速くなっています。

設定されている検出間隔（必要な最小 RX 間隔）内の BFD 制御パケットを各 BFD ピアが受信する限り、BFD セッションは有効であり、BFD と関連付けられたルーティング プロトコルは隣接関係を維持します。BFD ピアがこの間隔内に制御パケットを受信しない場合、その BFD セッションに参加しているクライアントに障害発生を通知します。ルーティングプロトコルにより、その情報に対する適切な応答が決定されます。標準的な応答は、ルーティングプロトコル ピア セッションを終了し、再コンバージェンスの後、障害の発生したピアをバイパスすることです。

BFD セッション中に BFD ピアが正常に BFD 制御パケットを受信するたびに、このセッションの検出タイマーがゼロにリセットされます。したがって、障害検出は、受信側が最後にパケットを送信した時点ではなく、パケット受信に依存しています。

BFD 導入シナリオ

具体的なシナリオで BFD がどのように動作するかについて、以下に説明します。

フェールオーバー

フェールオーバー シナリオでは、アクティブ ユニットとネイバー ユニット間で BFD セッションが確立、維持されます。スタンバイ ユニットはネイバーとの BFD セッションを維持しません。フェールオーバーが発生すると、新しいアクティブユニットがネイバーとのセッション確立を開始する必要があります。これは、アクティブ ユニットとスタンバイ ユニットの間ではセッション情報が同期されないためです。

グレースフル リスタート/NSF シナリオでは、クライアント（BGP IPv4/IPv6）がそのネイバーに対してイベントを通知します。ネイバーはこの情報を受信すると、フェールオーバーが完了するまで RIB テーブルを維持します。フェールオーバー中に、デバイスで BFD と BGP セッションがダウンします。フェールオーバーが完了し、BGPセッションがアップになると、ネイバー間で新しい BFD セッションが確立されます。

スパンド EtherChannel および L2 クラスタ

スパンド EtherChannel クラスタ シナリオでは、プライマリ ユニットとそのネイバー間で BFD セッションが確立、維持されます。従属ユニットはネイバーとの BFD セッションを維持しません。スイッチでのロードバランシングが原因で BFD パケットが従属ユニットにルーティン

グされる場合、従属ユニットはこのパケットをクラスタリンク経由でプライマリユニットに転送する必要があります。クラスタ スイッチオーバーが発生すると、新しいプライマリ ユニットがネイバーとのセッション確立を開始します。これは、プライマリ ユニットと従属ユニットの間でセッション情報が同期されていないためです。

個別インターフェイス モードと L3 クラスタ

個別インターフェイス モード クラスタのシナリオでは、個々のユニットが各自のネイバーとの BFD セッションを維持します。

BFD テンプレートの作成

このセクションでは、BFD テンプレート ポリシー オブジェクトを作成するために必要な手順を説明します。BFD テンプレートは、一連の BFD 間隔値を指定します。BFD テンプレートで指定された BFD 間隔値は、1 つのインターフェイスに限定されるものではありません。また、シングルホップセッションとマルチホップセッションの認証も設定できます。エコーをイネーブルにできるのは、シングルホップのみです。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [BFDテンプレート（BFD Template）] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

フィールド リファレンス

表 *64 : BFD* テンプレートの追加/編集

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成を参照してください。
説明	（任意）オブジェクトの説明。
設定モード	インターフェイスに関連付けられた BFD の送信元と宛先の間に単一の IP ホップがあるか、複数の IP ホップがあるかを指定します。
エコーの有効化（Enable Echo）	（オプション）選択するとエコーが有効になります。有効にすると、エコーパケットはフォワーディングエンジンによって送信され、検出を実行するために同じパスに沿って返信されます。 （注） これは、単一ホップのコンフィギュレーション モードにのみ適用されます。

要素	説明
[間隔（Interval）]タブ（オプション）	
間隔タイプ（Interval Type）	間隔タイプをマイクロ秒またはミリ秒のどちらで定義するかを指定します。デフォルトの間隔タイプは「なし」です。
送受信の値（間隔値はマイクロ秒単位）（Transmit and Receive Values Interval Values in Microseconds）	このセクションは、間隔タイプがマイクロ秒の場合に有効になります。有効な値は 50000 ～ 999000 マイクロ秒です。 [最小伝送値（Minimum Transmit Values）]：最小伝送間隔機能をマイクロ秒単位で入力します。 [最小受信値（Minimum Receive Values）]：最小受信間隔機能をマイクロ秒単位で入力します。
送受信の値（間隔値はミリ秒単位）（Transmit and Receive Values Interval Values in Milliseconds）	このセクションは、間隔タイプがミリ秒の場合に有効になります。有効値の範囲は、50 ～ 999 ミリ秒です。 [最小伝送値（Minimum Transmit Values）]：最小伝送間隔機能をミリ秒単位で入力します。 [最小受信値（Minimum Receive Values）]：最小受信間隔機能をミリ秒単位で入力します。
乗算値（Multiplier Value）	連続して紛失してよい BFD 制御パケットの数を入力します。この数に達すると、BFDはそのピアが利用不可になっていることを宣言します。デフォルト値は 3 です。有効な値は、3 ～ 50 です。
[認証（Authentication）] タブ（オプション）	
認証タイプ（Authentication Type）	BFDテンプレートの認証を設定する場合に選択します。認証に暗号化されたパスワードを使用するか、暗号化されていないパスワードを使用するかを指定します。
Key Value	BFD パスワードを入力して確認します。 • 暗号化された BFD テンプレートの場合、キー値の長さは 17 ～ 66 文字です。 • sha-1 または meticulous-sha-1 認証タイプの暗号化されていない BFD テンプレートの場合、キー値の長さは 29 文字未満でなければなりません。 • md5 または meticulous-md5 認証タイプの暗号化されていない BFD テンプレートの場合、キー値の長さは 25 文字未満である必要があります。
Key ID	認証キー ID を入力します。これは、キー文字列に一致する共有キー ID です。

要素	説明
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリオブジェクトの使用を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[BFDマップの追加/編集（Add/Edit BFD Map）] ダイアログボックス

[BFDマップの追加/編集（Add/Edit BFD Map）] ダイアログボックスでは、マルチホップテンプレートに関連付けることができる宛先が含まれているBFDマップを作成できます。マルチホップ BFD テンプレートがすでに設定されている必要があります。詳細については、BFD テンプレートの作成 （125 ページ）を参照してください。

ナビゲーション パス

[BFDマップの追加/編集（Add/Edit BFD Map）] ダイアログボックスには、[BFD] ページの [マップ（Map）] タブからアクセスできます。新しい BFD マップを追加するには、[行の追加（Add Row）] ボタンをクリックします。既存の BFD マップを編集するには、そのマップを選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- BFD テンプレートの作成 （125 ページ）

フィールド リファレンス

表 65 : [BFDマップ（BFD Map）] タブ

要素	説明
BFD テンプレート（BFD Template）	マルチホップ BFD テンプレートを選択するか、マルチホップ BFD テンプレートを追加します。詳細については、BFDテンプレートの作成 （125ページ）を参照してください。

要素	説明
IP バージョン（IP version）	送信元と宛先の適切なアドレス形式（IPv4 または IPv6）を選択します。
IPv4 宛先/プレフィックス、IPv4 送信元/プレフィックス（IPv4 Destination/Prefix, IPv4 Source/Prefix）	宛先と送信元の IPv4 アドレスを、xxxx/プレフィックス形式で適切なフィールドに入力します。
IPv6 宛先/プレフィックス、IPv6 送信元/プレフィックス（IPv6 Destination/ Prefix, IPv6 Source/prefix）	宛先と送信元の IPv6 アドレスを、x:x:x:x:x:x:x:x/プレフィックス形式で適切なフィールドに入力します。
低速タイマー（Slow Timers）	これにより、BFD ネイバー間で送信される BFD 制御パケットの数が削減されます。これにより、非同期セッションの速度が低下し、処理のオーバーヘッドが削減され、障害検出が迅速になります。 低速タイマーのデフォルト値は 1000 で、有効な値は 1000 から 30000 です。

[BFDインターフェイスの追加/編集（Add/Edit BFD Interface）] ダイアログボックス

[BFDインターフェイスの追加（Add BFD Interface）] /[BFDインターフェイスの編集（Edit BFD Interface）] ダイアログボックスを使用すると、BFD テンプレートをインターフェイスにバインドすることで、基準 BFD セッションパラメータの設定およびエコーモードのイネーブル化をインターフェイスごとに行うことができるようになります。

ナビゲーション パス

[BFDインターフェイスの追加（Add BFD Interface）] /[BFDインターフェイスの編集（Edit BFD Interface）] ダイアログボックスには、[インターフェイス（Interfaces）] ページからアクセスできます。新しい BFD インターフェイスを追加するには、[行の追加（Add Row）] ボタンをクリックします。既存の BFD インターフェイスを編集するには、そのインターフェイスを選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- BFD テンプレートの作成 （125 ページ）

フィールド リファレンス

表 66 : [BFD インターフェイス（BFD Interface）] タブ

要素	説明
インターフェイス（Interface）	インターフェイス名を入力するか、インターフェイスを選択するか、インターフェイスロールを追加します。
BFDの設定（BFD Configuration）	BFDテンプレートを選択して既存のシングルホップBFDテンプレートを選択するか、シングルホップBFDテンプレートを追加します。または、BFD 間隔を選択します。 詳細については、BFD テンプレートの作成 （125 ページ）を参照してください。
BFD間隔（BFD Interval）	
最小伝送間隔値（Minimum Transmit Value）	許容される最小伝送間隔をミリ秒単位で入力します。有効な値は 50 ～ 999 ミリ秒です。
最小受信間隔値（Minimum Receive Value）	許容される最小受信間隔をミリ秒単位で入力します。有効な値は 50 ～ 999 ミリ秒です。
Multiplier（乗数）	連続して紛失してよいBFD制御パケットの数を入力します。この数に達すると、BFD はそのピアが利用不可になっていることを宣言します。デフォルト値は 3 です。有効な値は、3 ～ 50 です。
Echo	（オプション）選択するとエコーが有効になります。有効にすると、エコーパケットはフォワーディングエンジンによって送信され、検出を実行するために同じパスに沿って返信されます。

OSPF の設定

[OSPF] ページには、ファイアウォールデバイス上の Open Shortest Path First（OSPF）ルーティングを設定するための 10 のタブ付きパネルがあります。ここでは、OSPF のイネーブル化および設定について詳しく説明します。

（注） 設定しているデバイスのバージョンによっては、一部のタブが使用できない場合があります。

（注） ASA バージョン 9.2(1) 以降、特定の OSPF 設定が変更されました。ASA 9.2(1)+ に固有の設定を使用する共有ポリシーを設定した場合、そのポリシーが 9.2(1) より前のバージョンのデバイスに割り当てられていると、検証エラーが発生します。同様に、ASA 9.2(1)+ に適用されなくなった設定を使用する共有ポリシーを設定した場合、そのポリシーが 9.2(1)+ デバイスに割り当てられていると、検証エラーが発生します。

- OSPF について （130 ページ）
- [General] タブ （7 ページ）
- [Area] タブ （140 ページ）
- [Range] タブ （143 ページ）
- [Neighbors] タブ （61 ページ）
- [Redistribution] タブ （63 ページ）
- [Virtual Link] タブ （150 ページ）
- [Filtering] タブ （154 ページ）
- [フィルタルール（Filter Rule）] タブ （157 ページ）
- [サマリーアドレス（Summary Address）] タブ （67 ページ）
- [Interface] タブ （111 ページ）
- キーチェーンの設定 （166 ページ）

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）]>[ルーティング（Routing）] > [OSPF] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [OSPF] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

OSPF について

Open Shortest Path First（OSPF）は、パス選択に距離ベクトルではなくリンク ステートを使用する Interior Gateway Routing Protocol です。OSPF は、ルーティング テーブル更新ではなく Link-State Advertisement（LSA; リンクステート アドバタイズメント）を伝播します。ルーティング テーブル全体ではなく LSA だけが交換されるため、OSPF ネットワークは RIP ネットワークよりも迅速に収束します。

OSPF は、MD5 およびクリア テキスト ネイバー認証をサポートします。攻撃者は潜在的に OSPF と他のプロトコル（RIP など）間のルート再配布を使用してルーティング情報を操作できるため、可能なかぎり、すべてのルーティング プロトコルで認証を使用する必要があります。

OSPF がパブリック エリアおよびプライベート エリアで動作しているときに NAT が使用される場合で、アドレス フィルタリングが必要な場合は、2 つの OSPF プロセスを実行する必要があります。パブリック エリア用のプロセスとプライベート エリア用のプロセスです。

複数のエリアにインターフェイスを持つルータは、エリア境界ルータ（ABR）と呼ばれます。ゲートウェイとして動作し、OSPF を使用しているルータと他のルーティング プロトコルを使用しているルータ間でトラフィックを再配布するルータは、自律システム境界ルータ（ASBR）と呼ばれます。

ABR は LSA を使用して、使用可能なルータに関する情報を他の OSPF ルータに送信します。ABR タイプ 3 LSA フィルタリングを使用して、セキュリティ アプライアンスが ABR として動作している別々のプライベート エリアとパブリック エリアを持つことができます。タイプ 3 LSA（エリア間ルート）を 1 つのエリアから他のエリアにフィルタリングできます。このことにより、プライベート ネットワークをアドバタイズしなくても、NAT と OSPF を一緒に使用できます。

（注） タイプ 3 LSA だけをフィルタリングできます。プライベート ネットワークでセキュリティ アプライアンスを ASBR として設定すると、セキュリティ アプライアンスはプライベート ネットワークを記述するタイプ 5 LSA を送信します。これは、パブリック エリアを含む自律システム（AS）全体にブロードキャストされます。

NAT が使用されるが、OSPF がパブリック エリアだけで実行されている場合、パブリック ネットワークへのルートは、プライベート ネットワーク内でデフォルトまたはタイプ 5 AS External LSA として再配布できます。ただし、セキュリティ アプライアンスによって保護されているプライベート ネットワークのスタティック ルートを設定する必要があります。また、同じセキュリティ アプライアンス インターフェイスで、パブリック ネットワークとプライベート ネットワークを混在させないでください。

関連項目

- OSPF の設定 （129 ページ）

[General] タブ

[OSPF] ページの [General] パネルを使用して、最大 2 つの OSPF プロセス インスタンスをイネーブルにします。各 OSPF プロセスには、独自のエリアとネットワークが関連付けられます。

（注） RIP をイネーブルにしている場合は、OSPF をイネーブルにすることはできません。

ナビゲーション パス

[全般（General）] パネルには、[OSPF] ページからアクセスできます。詳しくは、OSPF の設定 （129 ページ）を参照してください。

関連項目

- [Area] タブ （140 ページ）
- [Range] タブ （143 ページ）
- [Neighbors] タブ （61 ページ）
- [Redistribution] タブ （63 ページ）
- [Virtual Link] タブ （150 ページ）
- [Filtering] タブ （154 ページ）
- [サマリーアドレス（Summary Address）] タブ （67 ページ）
- [Interface] タブ （111 ページ）

フィールド リファレンス

表 67 : OSPF の [General] タブ

要素	説明
[General] タブには 2 つの同一のセクションがあり、それぞれ 1 つの OSPF プロセスをイネーブルにするために使用されます。各セクションで次のオプションを使用できます。	
Enable this OSPF Process	OSPF プロセスをイネーブルにするには、このチェックボックスをオンにします。セキュリティ アプライアンスで RIP をイネーブルにしている場合は、OSPF プロセスをイネーブルにすることはできません。OSPF プロセスを削除するには、このオプションの選択を解除します。
OSPF プロセス ID（OSPF Process ID）	OSPF プロセスの一意の数値 ID を入力します。このプロセス ID は内部的に使用され、他の OSPF デバイスの OSPF プロセス ID と一致している必要はありません。有効値は 1 ～ 65535 です。

要素	説明
[Advanced] ボタン	[OSPF Advanced] ダイアログボックス （133 ページ）が開き、[ルータID（Router ID）]、[隣接関係の変更（Adjacency Changes）]、[ルートのアドミニストレーティブディスタンス（Administrative Route Distances）]、[タイマー（Timers）]、[デフォルトの情報送信元（Default Information Originate）] 設定など、その他のプロセス関連パラメータを設定できます。

[OSPF Advanced] ダイアログボックス

[OSPF Advanced] ダイアログボックスを使用して、OSPF プロセスの [Router ID]、[Adjacency Changes]、[Administrative Route Distances]、[Timers]、[Default Information Originate] などの設定を行うことができます。

（注） ASA バージョン 9.2(1) 以降、特定の OSPF 設定が変更されました。ASA 9.2(1)+ に固有の設定を使用する共有ポリシーを設定した場合、そのポリシーが 9.2(1) より前のバージョンのデバイスに割り当てられていると、検証エラーが発生します。同様に、ASA 9.2(1)+ に適用されなくなった設定を使用する共有ポリシーを設定した場合、そのポリシーが 9.2(1)+ デバイスに割り当てられていると、検証エラーが発生します。

ナビゲーション パス

[OSPF Advanced] ダイアログボックスには、 [General] タブ （131 ページ）からアクセスできます。

関連項目

- OSPF の設定 （129 ページ）

フィールド リファレンス

表 68 : [OSPF Advanced] ダイアログボックス

要素	説明
OSPF Process	設定している OSPF プロセスの ID が表示されます。このダイアログボックスでこの値を変更することはできません。
[General] タブ	

要素	説明
ルータ ID（Router ID）	固定ルータ ID を使用するには、[IPアドレス（IP Address）] を選択してから、[ルータID（Router ID）] フィールドにルータ ID を IP アドレス形式で入力します。ルータ IDが自動的に生成されるようにするには（セキュリティアプライアンスの最高レベルのIPアドレスがルータ ID として使用されます）、[自動（Automatic）] を選択します。
Ignore LSA MOSPF	このオプションを選択すると、セキュリティアプライアンスがタイプ 6（MOSPF）LSA パケットを受信したときに、syslog メッセージの送信が抑止されます。
RFC 1583 Compatible	このオプションを選択すると、RFC 1583 に基づいてサマリールートのコストが計算されます。このオプションを選択解除すると、RFC 2328 に基づいてサマリールートのコストが計算されます。ルーティング ループの可能性を最小限に抑えるには、OSPF ルーティング ドメイン内のすべての OSPF デバイスに同じように RFC 互換性が設定されている必要があります。このオプションは、デフォルトで選択されます。
隣接関係の変更	これらのオプションでは、隣接関係の変更が発生したときに送信される syslog メッセージを指定します。 • [Log Adjacency Changes]：選択すると、OSPF ネイバーの起動またはダウン時に常に、セキュリティ アプライアンスによって syslog メッセージが送信されます。このオプションは、デフォルトで選択されます。 • [Log Adjacency Changes Detail]：選択すると、OSPF ネイバーの起動またはダウン時だけでなく、状態の変更が発生したときに常に、セキュリティ アプライアンスによって syslog メッセージが送信されます。このオプションは、デフォルトでは選択されません。
Administrative Route Distances	ルート タイプに基づく管理ルート ディスタンスの設定。 • [Inter Area]：1 つのエリアから別のエリアへのすべてのルートのアドミニストレーティブ ディスタンス。有効値の範囲は 1 ～ 255 で、デフォルト値は 110 です。 • [Intra Area]：エリア内のすべてのルートのアドミニストレーティブ ディスタンス。有効値の範囲は 1 ～ 255 で、デフォルト値は 110 です。 • [External]：再配布によって学習された他のルーティング ドメインからのすべてのルートのアドミニストレーティブ ディスタンス。有効値の範囲は 1 ～ 255 で、デフォルト値は 110 です。

要素	説明
タイマー	

要素	説明

	ASA 9.2(1)+ デバイスの LSA 着信、LSA ペーシング、およびスロットリングの設定に使用される設定：
	• [LSA着信（LSA Arrival）]：ネイバーから同じ LSA が着信する場合に、同じLSAの着信と着信の間に経過する最小遅延（ミリ秒単位）。有効な範囲は 0 ～ 600,000 ミリ秒です。デフォルトは 1000 ミリ秒です。
	• [LSAフラッドペーシング（LSA Flood Pacing）]：フラッディングキュー内のLSAが更新と更新の間にペーシング処理される時間（ミリ秒単位）。設定できる範囲は 5 ～ 100 ミリ秒です。デフォルト値は、33 ミリ秒です。
	• [LSA Group Pacing]：LSA がグループにまとめられ、リフレッシュ、チェックサム、およびエージングされる間隔。有効値の範囲は 10 ～ 1800 で、デフォルト値は 240 秒です。
	• [LSA再送信ペーシング（LSA Retransmission Pacing）]：再送信キュー内のLSAがペーシングされる時間（ミリ秒単位）。設定できる範囲は 5 ～ 200 ミリ秒です。デフォルト値は、66 ミリ秒です。
	• [LSAスロットル（LSA Throttle）]：LSA の最初の発信を引き起こす遅延（ミリ秒単位）。有効な値の範囲は、0 ～ 600000 ミリ秒です。このフィールドに値を入力すると、[最小（Min）]および [最大（Max）] フィールドが有効になります。
	  • [最小（Min）]：同じ LSA を発信するための最小遅延。有効値の範囲は、1 ～ 600000 ミリ秒です。
	  • [最大（Max）]：同じ LSA を発信するための最大遅延。有効値の範囲は、1 ～ 600000 ミリ秒です。
	（注） LSAスロットリングの場合、最初に発生する値は最小値以下である必要があり、最小値は最大値以下である必要があります。
	• [SPFスロットル（SPF Throttle）]：SPF 計算への変更を受信する遅延。有効値の範囲は、1 ～ 600000 ミリ秒です。このフィールドに値を入力すると、[最小（Min）] および [最大（Max）] フィールドが有効になります。
	  • [最小（Min）]：1 番目と 2 番目の SPF 計算間の遅延。有効値の範囲は、1 ～ 600000 ミリ秒です。
	  • [最大（Max）]：SPF 計算の最大待機時間。有効値の範囲は、1 ～ 600000 ミリ秒です。

要素	説明
	（注） SPF スロットリングの場合、最初に発生する値は最小値以下である必要があり、最小値は最大値以下である必要があります。 9.2(1) よりも前のデバイスバージョンで、LSA ペーシングおよび SPF 計算タイマーを設定するために使用される設定。 • [SPF Delay]：トポロジ変更の受信と Shortest Path First（SPF）計算の開始の間の時間。有効値の範囲は 0 ～ 65535 で、デフォルト値は 5 秒です。 • [SPF Hold]：連続する SPF 計算間のホールド時間。有効値の範囲は 1 ～ 65534 で、デフォルト値は 10 秒です。 • [LSA Group Pacing]：LSA がグループにまとめられ、リフレッシュ、チェックサム、およびエージングされる間隔。有効値の範囲は 10 ～ 1800 で、デフォルト値は 240 秒です。

要素	説明
デフォルトの情報発信元	OSPF ルーティング ドメインへのデフォルトの外部ルートを生成するために ASBR によって使用される設定。 • [Enable Default Information Originate]：OSPF ルーティング ドメインへのデフォルト ルートの生成をイネーブルにするには、このチェックボックスをオンにします。次のオプションが使用可能になります。 • [Always advertise the default route]：デフォルト ルートを常にアドバタイズするには、このチェックボックスをオンにします。 • [Metric Value]：デフォルト ルートの OSPF メトリックを入力します。有効値の範囲は 0 ～ 16777214 で、デフォルト値は 1 です。 • [Metric Type]：OSPF ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられる外部リンク タイプを選択します。選択肢は [1] または [2] で、タイプ 1 またはタイプ 2 外部ルートを示します。デフォルト値は 2 です。 • [ルートマップ（Route Map）]：（任意）適用するルートマップオブジェクトを入力または選択します。ルート マップが一致すると、ルーティング プロセスによってデフォルト ルートが生成されます。 ヒント [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。
[Nontop Forwarding] タブ （注） Nonstop Forwarding（NSF）は、スパンクラスタモードまたはフェールオーバーモードの ASA 9.3(1)+ デバイスでのみサポートされます。	
[Cisco Nonstop Forwarding機能を有効にする（Enable Cisco Nonstop Forwarding Capability）]	Cisco Nonstop Forwarding（NSF）操作の設定を有効にします。

要素	説明
[Cisco Nonstop Forwarding（NSF）ヘルパーモードの有効化（Enable Cisco Nonstop Forwarding Helper mode）]	Cisco Nonstop Forwarding（NSF）ヘルパーモードを有効にします。 ASA が NSF を有効にしている場合、ASA は NSF 対応であると見なされ、グレースフル リスタート モードで動作します。OSPF プロセスは、ルートプロセッサ（RP）スイッチオーバーのため、ノンストップ フォワーディングの復帰を実行します。デフォルトでは、NSF 対応 ASA に隣接する ASA は NSF 認識となり、NSF ヘルパーモードで動作します。NSF 対応 ASA がグレースフル リスタートを実行しているときは、ヘルパーの ASA はそのノンストップ フォワーディングの復帰プロセスを支援します。 再起動するネイバーのノンストップ フォワーディングの復帰を ASA が支援しないようにする場合は、Cisco Nonstop Forwarding ヘルパーの有効化オプションを解除します。
[Cisco Nonstop Forwardingの有効化（Enable Cisco Nonstop Forwarding）]	Cisco Nonstop Forwarding（NSF）を有効にします。
[非NSF対応のネイバーネットワーキングデバイスが検出されたときにNSF再起動をキャンセルする（Enforce Global）（Cancel NSF restart when non-NSF-aware neighboring networking devices are detected (Enforce Global)）]	NSF グレースフル リスタートの実行時にネットワーク インターフェイスで NSF 認識でないネイバーが検出された場合、そのインターフェイスでのみ再起動が中止され、他のインターフェイスではグレースフル リスタートが続行されます。再起動中に非 NSF 対応のネイバーが検出されたときに OSPF プロセス全体の再起動をキャンセルするには、[非NSF対応のネイバーネットワーキングデバイスが検出されたときにNSF再起動をキャンセルする（Enforce Global）（Cancel NSF restart when non-NSF-aware neighboring networking devices are detected (Enforce Global)）] オプションを選択します。 （注） ネイバーとの隣接関係のリセットが任意のインターフェイスで検出された場合、または、OSPF インターフェイスがダウンした場合も、プロセス全体で NSF の再起動がキャンセルされます。
[IETFノンストップフォワーディング機能を有効にする（Enable IETF Non Stop Forwarding Capability）]	Internet Engineering Task Force（IETF）NSF 操作の設定を有効にします。

要素	説明
[IETFノンストップフォワーディングヘルパーモードの有効化（Enable IETF Non Stop Forwarding Helper mode）]	IETF ノンストップ フォワーディング（NSF）ヘルパーモードを有効にします。 ASA が NSF を有効にしている場合、ASA は NSF 対応であると見なされ、グレースフル リスタート モードで動作します。OSPF プロセスは、ルートプロセッサ（RP）スイッチオーバーのため、ノンストップ フォワーディングの復帰を実行します。デフォルトでは、NSF 対応 ASA に隣接する ASA は NSF 認識となり、NSF ヘルパーモードで動作します。NSF 対応 ASA がグレースフル リスタートを実行しているときは、ヘルパーの ASA はそのノンストップ フォワーディングの復帰プロセスを支援します。 再起動するネイバーのノンストップ フォワーディングの復帰を ASA が支援しないようにする場合は、IETF ノンストップ フォワーディング ヘルパーの有効化オプションを解除します。
[リンクステートアドバタイズメント（LSA）の厳密なチェックの有効化（Enable Strict Link State advertisement checking）]	IETF NSF ヘルパーモードの厳密なリンクステート アドバタイズメント（LSA）を有効にします。
[IETFノンストップフォワーディングの有効化（Enable IETF Non Stop Forwarding）]	IETF ノンストップ フォワーディング（NSF）を有効にします。
グレースフルリスタート間隔の長さ	（オプション）グレースフル リスタートの間隔を秒数で指定します。有効な範囲は 1 ～ 1800 です。デフォルトは 120 です。 （注） 30 秒未満の再起動間隔では、グレースフル リスタートが中断します。

[Area] タブ

[OSPF] ページの [Area] タブを使用して、OSPF エリアおよびネットワークを設定します。

ナビゲーション パス

[Area] タブには、[OSPF] ページからアクセスできます。[OSPF] ページの詳細については、OSPF の設定 （129 ページ）を参照してください。

関連項目

- [Add Area/Area Networks]/[Edit Area/Area Networks] ダイアログボックス （141 ページ）

- OSPF の設定 （129 ページ）
- [General] タブ （131 ページ）
- [Range] タブ （143 ページ）
- [Neighbors] タブ （61 ページ）
- [Redistribution] タブ （63 ページ）
- [Virtual Link] タブ （150 ページ）
- [Filtering] タブ （154 ページ）
- [サマリーアドレス（Summary Address）] タブ （67 ページ）
- [Interface] タブ （111 ページ）

フィールド リファレンス

表 *69 : [Area]* タブ

要素	説明
OSPF Process	エリアが適用される OSPF プロセス。
エリア ID（Area ID）	エリア ID。
エリア タイプ	エリア タイプ（[Normal]、[Stub]、または [NSSA]）。
ネットワーク	エリア ネットワーク。
オプション	エリア タイプに対して設定するオプション（ある場合）。
認証	エリアに対して設定する認証のタイプ（[None]、[Password]、または [MD5]）。
コスト（Cost）	エリアのデフォルト コスト。

[Add Area/Area Networks]/[Edit Area/Area Networks] ダイアログボックス

[Add Area/Area Networks]/[Edit Area/Area Networks] ダイアログボックスを使用して、エリア パラメータ、エリアによって含まれるネットワーク、およびエリアに関連付けられる OSPF プロセスを定義します。

ナビゲーション パス

[Add Area/Area Networks]/[Edit Area/Area Networks] ダイアログボックスには、[Area] タブ （140 ページ）からアクセスできます。

関連項目

- OSPF の設定 （129 ページ）

フィールド リファレンス

表 70 : [Add Area/Area Networks]/[Edit Area/Area Networks] ダイアログボックス

要素	説明
OSPF Process	新しいエリアを追加する場合、エリアが追加される OSPF プロセスの OSPF プロセス ID を選択します。セキュリティ アプライアンスでイネーブルにされている OSPF プロセスが 1 つだけの場合、そのプロセスがデフォルトで選択されます。既存のエリアを編集する場合、OSPF プロセス ID を変更することはできません。
エリア ID（Area ID）	新しいエリアを追加する場合、そのエリア ID を入力します。このエリア ID には、10 進数か IP アドレスを指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。既存のエリアを編集する場合、エリア ID は変更できません。
エリア タイプ	
標準	エリアを標準 OSPF エリアにするには、このオプションを選択します。エリアを最初に作成するときは、このオプションがデフォルトで選択されています。
Stub	このオプションを選択すると、エリアはスタブ エリアになります。スタブ エリアには、その向こう側にルータまたはエリアはありません。スタブ エリアは、AS External LSA（タイプ 5 LSA）がスタブ エリアにフラッドされないようにします。スタブエリアを作成すると、[Summary] チェックボックスをオフにすることによって、集約 LSA（タイプ 3 および 4）がそのエリアにフラッドされるのを防ぐことができます。
[サマリー（LSA のスタブエリアへの送信を許可）（Summary (allows sending LSAs into the stub area)）]	定義しているエリアがスタブ エリアである場合、このチェックボックスをオフにすると、LSA はスタブ エリアに送信されません。スタブ エリアの場合、このチェックボックスはデフォルトでオンになっています。
NSSA	エリアを Not-So-Stubby Area にするには、このオプションを選択します。NSSA は、タイプ 7 LSA を受け入れます。NSSA を作成すると、[Summary] チェックボックスをオフにすることによって、集約 LSA がそのエリアにフラッドされるのを防ぐことができます。また、[Redistribute] チェックボックスをオフにし、[Default Information Originate] をイネーブルにすることによって、ルート再配布をディセーブルにすることができます。

要素	説明
Redistribute (imports routes to normal and NSSA areas)	ルートが NSSA にインポートされないようにするには、このチェックボックスをオフにします。このチェックボックスは、デフォルトでオンになっています。
Summary (allows sending LSAs into the NSSA area)	定義しているエリアが NSSA である場合、このチェックボックスをオフにすると、LSA はスタブ エリアに送信されません。NSSA の場合、このチェックボックスはデフォルトでオンになっています。
Default Information Originate (generate a Type 7 default)	タイプ 7 デフォルトを NSSA 内に生成するには、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオフになっています。
メトリック値	デフォルト ルートの OSPF メトリック値を指定します。有効値の範囲は 0 ～ 16777214 です。デフォルト値は 1 です。
メトリック タイプ	デフォルト ルートの OSPF メトリック タイプ。選択肢は、1（タイプ 1）または 2（タイプ 2）です。デフォルト値は 2 です。
ネットワーク（Network）	エリアに追加するネットワークまたはホストの IP アドレスおよびネットワークマスク。デフォルト エリアを作成するには、0.0.0.0 およびネットマスク 0.0.0.0 を使用します。0.0.0.0 は 1 つのエリア内だけで使用できます。 **ヒント** [選択（Select）] をクリックすると、インターフェイス オブジェクトのリストからインターフェイスを選択できます。
認証	OSPF エリア認証の設定が含まれます。 • [None]：OSPF エリア認証をディセーブルにするには、このオプションを選択します。これがデフォルトの設定です。 • [Password]：エリア認証にクリア テキスト パスワードを使用するには、このオプションを選択します。セキュリティ面が懸念される場合、このオプションは推奨しません。 • [MD5]：MD5 認証を使用するには、このオプションを選択します。
デフォルト コスト（Default Cost）	エリアのデフォルト コストを指定します。有効な値の範囲は、9.2(1) より前の ASA デバイスの場合は 0 ～ 65535、ASA 9.2(1) 以降の場合は 0 ～ 16777214 です。デフォルト値は 1 です。

[Range] タブ

[Range] タブを使用して、エリア間のルートをサマライズします。

ナビゲーション パス

[Range] タブには、[OSPF] ページからアクセスできます。[OSPF] ページの詳細については、OSPF の設定 （129 ページ）を参照してください。

関連項目

- [エリア範囲ネットワークの追加/編集（Add/Edit Area Range Network）] ダイアログボックス （144 ページ）

フィールド リファレンス

表 *71 : [Range]* タブ

要素	説明
プロセス ID（Process ID）	ルート要約と関連付ける OSPF プロセスの ID。
エリア ID（Area ID）	ルート要約と関連付けるエリアの ID。
ネットワーク （Network）	サマリー IP アドレスおよびネットワーク マスク。
[アドバタイズ（Advertise）]	ルート要約がアドレス/マスクペアと一致したときにアドバタイズされる場合は、「true」が表示されます。または、ルート要約がアドレス/マスク ペアと一致したときに抑止される場合は、「false」が表示されます。

[エリア範囲ネットワークの追加/編集（Add/Edit Area Range Network）] ダイアログボックス

[Add Area Range Network]/[Edit Area Range Network] ダイアログボックスを使用して、[Route Summarization] テーブルに新しいエントリを追加するか、既存のエントリを変更します。

ナビゲーション パス

[Add Area Range Network]/[Edit Area Range Network] ダイアログボックスには、[Range] タブ（143 ページ）からアクセスできます。

関連項目

- OSPF の設定 （129 ページ）

フィールド リファレンス

表 *72 : [*エリア範囲ネットワークの追加/編集（*Add/Edit Area Range Network*）*]* ダイアログボックス

要素	説明
OSPF Process	ルート要約が適用される OSPF プロセスを選択します。既存のルート要約エントリを編集する場合、この値は変更できません。
領域	ルート要約が適用されるエリアのエリア ID を選択します。既存のルート要約エントリを編集する場合、この値は変更できません。
ネットワーク（Network）	サマライズされているルートのネットワークの IP アドレスおよびマスク。 **ヒント** [選択（Select）] をクリックすると、ネットワークオブジェクトのリストからネットワークを選択できます。
[アドバタイズ（Advertise）]	アドレスの範囲ステータスを「アドバタイズ」に設定するには、このチェックボックスをオンにします。これにより、タイプ 3 集約 LSA が生成されます。指定したネットワークのタイプ 3 集約 LSA を抑止するには、このチェックボックスをオフにします。

[Neighbors] タブ

[ネイバー（Neighbors）] タブを使用して、静的ネイバーを手動で定義します。ポイントツーポイントの非ブロードキャスト インターフェイスごとに、スタティック ネイバーを定義する必要があります。また、[Neighbors] テーブルのスタティック ネイバーごとに、スタティック ルートを定義する必要があります。

ナビゲーション パス

[Neighbors] タブには、[OSPF] ページからアクセスできます。[OSPF] ページの詳細については、OSPF の設定 （129 ページ）を参照してください。

関連項目

- [Add Static Neighbor]/[Edit Static Neighbor] ダイアログボックス （146 ページ）

フィールド リファレンス

表 *73 : [Neighbors]* タブ

要素	説明
OSPF Process	スタティック ネイバーと関連付ける OSPF プロセス。
ネイバー	スタティック ネイバーの IP アドレス。

要素	説明
インターフェイス	スタティック ネイバーと関連付けるインターフェイス。

[Add Static Neighbor]/[Edit Static Neighbor] ダイアログボックス

スタティック ネイバーを定義するか、または既存のスタティック ネイバーの情報を変更するには、[Add Static Neighbor]/[Edit Static Neighbor] ダイアログボックスを使用します。ポイントツーポイントの非ブロードキャスト インターフェイスごとに、スタティック ネイバーを定義する必要があります。

ナビゲーション パス

[Add Static Neighbor]/[Edit Static Neighbor] ダイアログボックスには、[Neighbors] タブ （145 ページ）からアクセスできます。

関連項目

- OSPF の設定 （129 ページ）

フィールド リファレンス

表 *74 : [Add Static Neighbor]/[Edit Static Neighbor]* ダイアログボックス

要素	説明
OSPF Process	スタティック ネイバーと関連付ける OSPF プロセス。
ネイバー	スタティック ネイバーの IP アドレス。 **ヒント** [選択（Select）] をクリックすると、ホストオブジェクトのリストからネイバーを選択できます。
インターフェイス	スタティック ネイバーと関連付けるインターフェイス。 **ヒント** [選択（Select）] をクリックして、インターフェイスオブジェクトのリストからインターフェイスを選択できます。

[Redistribution] タブ

1 つのルーティング ドメインから別のドメインへのルートの再配布ルールを定義するには、[Redistribution] タブを使用します。

ナビゲーション パス

[再配布（Redistribution）] タブには、[OSPF] ページからアクセスできます。[OSPF] ページの詳細については、OSPF の設定 （129 ページ）を参照してください。

関連項目

- [Redistribution] ダイアログボックス （148 ページ）

フィールド リファレンス

表 *75 : [Redistribution]* タブ

要素	説明
OSPF Process	ルート再配布エントリに関連付けられた OSPF プロセス。
ルート タイプ（Route Type）	ルートの再配布元であるソース プロトコル。有効なエントリは次のとおりです。 • [BGP]：BGP ルーティング プロセスからルートを再配布します。 • [Connected]：接続されたルート（インターフェイス上で IP アドレスをイネーブルにすることによって自動的に確立されるルート）を OSPF ルーティング プロセスに再配布します。接続済みルートは、AS の外部として再配布されます。 • [EIGRP]：EIGRP ルーティング プロセスからルートを再配布します。リストから EIGRP ルーティング プロセスの自律システム番号を選択してください。 • [OSPF]：別の OSPF ルーティング プロセスからのルートを再配布します。 • [RIP]：RIP ルーティング プロセスからルートを再配布します。 • [Static]：スタティック ルートを OSPF ルーティング プロセスに再配布します。
一致（Match）	1 つのルーティング プロトコルから別のルーティング プロトコルへのルート再配布に使用される条件。これらのオプションは、スタティック、接続済み、RIP、BGP、または EIGRP ルートを再配布するときに選択できます。
サブネット	サブネット化されたルートが再配布される場合は、「true」と表示されます。サブネット化されていないルートだけが再配布される場合は、何も表示されません。
メトリック値	ルートに使用されるメトリック。デフォルトのメトリックが使用される場合、このカラムは再配布エントリに対してブランクです。
メトリック タイプ	メトリックがタイプ 1 外部ルートの場合は「1」が表示され、メトリックがタイプ 2 外部ルートの場合は「2」が表示されます。

要素	説明
[タグ値（Tag Value）]	各外部ルートに付加される 32 ビットの 10 進値。この値は OSPF 自体には使用されません。ASBR 間での情報通信に使用されることはあります。有効値の範囲は、0 ～ 4294967295 です。
ルート マップ	再配布エントリに適用されるルートマップオブジェクトの名前。

[Redistribution] ダイアログボックス

[Redistribution] ダイアログボックスを使用して、再配布ルールを追加するか、[Redistribution] テーブルの既存の再配布ルールを編集します。

ナビゲーション パス

[Redistribution] ダイアログボックスには、[Redistribution] タブ （146 ページ）からアクセスできます。

関連項目

- OSPF の設定 （129 ページ）

フィールド リファレンス

表 *76 : [OSPF Redistribution Settings]* ダイアログボックス

要素	説明
OSPF Process	ルート再配布エントリと関連付ける OSPF プロセスを選択します。

要素	説明
ルート タイプ（Route Type）	ルートが再配布されているソースプロトコルを選択します。次のいずれかのオプションを選択できます。 • [BGP]：BGP ルーティング プロセスからルートを再配布します。 • [Connected]：接続されたルート（インターフェイス上でIPアドレスをイネーブルにすることによって自動的に確立されるルート）を OSPF ルーティング プロセスに再配布します。接続済みルートは、AS の外部として再配布されます。 • [EIGRP]：EIGRP ルーティング プロセスからルートを再配布します。リストから EIGRP ルーティング プロセスの自律システム番号を選択してください。 • [OSPF]：別の OSPF ルーティング プロセスからのルートを再配布します。このプロトコルを選択すると、このダイアログボックスの [Match] のオプションが表示されます。これらのオプションは、スタティック、接続済み、RIP、BGP、または EIGRP ルートを再配布するときに選択できます。 • [RIP]：RIP ルーティング プロセスからルートを再配布します。 • [Static]：スタティック ルートを OSPF ルーティング プロセスに再配布します。
ルーティングプロセス ID（Routing Process ID）	BGP または EIGRP ルーティングプロセスの自律システム（AS）番号です。
一致（Match）	ルートタイプとして OSPF を選択した場合、1 つのルーティングプロトコルから別のルーティングプロトコルへのルート再配布に使用される条件を選択します。ルートが再配布されるには、選択した条件と一致している必要があります。次の一致条件から 1 つ以上を選択できます。 • [Internal]：ルートは特定の AS の内部です。 • [External 1]：自律システムの外部だが、OSPF にタイプ 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、OSPF にタイプ 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、OSPF にタイプ 2 NSSA 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、OSPF にタイプ 2 NSSA ルートとしてインポートされるルート。

要素	説明
メトリック値	再配布されるルートのメトリック値。有効値の範囲は1～16777214です。同じデバイス上で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。
メトリック タイプ	メトリックがタイプ1外部ルートの場合は「1」を選択し、メトリックがタイプ2外部ルートの場合は「2」を選択します。
[タグ値（Tag Value）]	タグ値は、各外部ルートに付加される32ビットの10進値です。これはOSPF自体には使用されません。ASBR間での情報通信に使用されることはあります。有効値の範囲は、0～4294967295です。
Use Subnets	選択すると、サブネット化されたルートの再配布がイネーブルになります。サブネット化されていないルートだけを再配布するには、このチェックボックスをオフにします。
ルート マップ	再配布エントリに適用するルートマップオブジェクトを入力または選択します。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214ページ）を参照してください。

[Virtual Link] タブ

[Virtual Link] タブを使用して、仮想リンクを作成します。OSPFネットワークにエリアを追加し、そのエリアをバックボーンエリアに直接接続できない場合、仮想リンクを作成する必要があります。仮想リンクは、通過エリアと呼ばれる共通エリアを持つ2つのOSPFデバイスを接続します。OSPFデバイスのいずれかは、バックボーン エリアに接続されている必要があります。

ナビゲーション パス

[Virtual Link] タブには、[OSPF] ページからアクセスできます。[OSPF] ページの詳細については、OSPF の設定 （129 ページ）を参照してください。

関連項目

- [Add OSPF Virtual Link Configuration]/[Edit OSPF Virtual Link Configuration] ダイアログボックス （151 ページ）

フィールド リファレンス

表 *77 : [Virtual Link]* タブ

要素	説明
OSPF Process	仮想リンクと関連付ける OSPF プロセス。
エリア ID（Area ID）	通過エリアの ID。
Peer Router	仮想リンク ネイバーの IP アドレス。
認証	仮想リンクによって使用される認証のタイプを表示します。 • [None]：認証は使用されません。 • [Password]：クリア テキスト パスワード認証が使用されます。 • [MD5]：MD5 認証が使用されます。 • [キーチェーン（Key Chain）]：キーチェーン認証を有効にします。

[Add OSPF Virtual Link Configuration]/[Edit OSPF Virtual Link Configuration] ダイアログボックス

[Add OSPF Virtual Link Configuration]/[Edit OSPF Virtual Link Configuration] ダイアログボックスを使用して、仮想リンクを定義するか、既存の仮想リンクのプロパティを変更します。

ナビゲーション パス

[Add OSPF Virtual Link Configuration]/[Edit OSPF Virtual Link Configuration] ダイアログボックスには、[Virtual Link] タブ （150 ページ）からアクセスできます。

関連項目

- [Add OSPF Virtual Link MD5 Configuration]/[Edit OSPF Virtual Link MD5 Configuration] ダイアログボックス （154 ページ）
- OSPF の設定 （129 ページ）

フィールド リファレンス

表 78 : [Add OSPF Virtual Link Configuration]/[Edit OSPF Virtual Link Configuration] ダイアログボックス

要素	説明
OSPF Process	仮想リンクと関連付ける OSPF プロセスを選択します。
エリア ID（Area ID）	ネイバー OSPF デバイスによって共有されるエリアを選択します。選択するエリアは、NSSA またはスタブ エリアであってはなりません。
Peer Router	仮想リンク ネイバーの IP アドレスを入力します。
Hello 間隔（Hello Interval）	インターフェイス上で送信される hello パケット間の間隔（秒数）。hello 間隔を小さくすると、トポロジ変更はより高速に検出されますが、インターフェイス上で送信されるトラフィックはより多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバーで同じである必要があります。有効な値の範囲は、9.2(1) より前の ASA デバイスの場合は 1 ～ 65535 秒、ASA 9.2(1) 以降の場合は 1 ～ 8192 秒です。デフォルト値は 10 秒です。
再送信間隔（Retransmit Interval）	インターフェイスに属する隣接関係への LSA 再送信間の時間（秒数）。ルータが自身のネイバーに LSA を送信する場合、ルータは確認応答メッセージを受信するまでその LSA を保持します。ルータは、確認応答メッセージを受信しないと、LSA を再び送信します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。有効な値の範囲は、9.2(1) より前の ASA デバイスの場合は 1 ～ 65535 秒、ASA 9.2(1) 以降の場合は 1 ～ 8192 秒です。デフォルト値は 5 秒です。
送信遅延（Transmit Delay）	インターフェイス上で LSA パケットを送信するために必要と推定される時間（秒数）。更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。有効な値の範囲は、9.2(1) より前の ASA デバイスの場合は 1 ～ 65535 秒、ASA 9.2(1) 以降の場合は 1 ～ 8192 秒です。デフォルト値は 1 秒です。
dead 間隔（Dead Interval）	hello パケットが受信されないために、ネイバーがルータ ダウンを宣言するまでの時間間隔（秒数）。有効な値の範囲は、9.2(1) より前の ASA デバイスの場合は 1 ～ 65535 秒、ASA 9.2(1) 以降の場合は 1 ～ 8192 秒です。このフィールドのデフォルト値は、[Hello Interval] フィールドに設定されている時間間隔の 4 倍です。

要素	説明
認証	OSPF 認証オプションを含みます。 • [None]：OSPF 認証をディセーブルにするには、このオプションを選択します。 • [エリア（Area）]：エリアに対して指定された認証タイプを使用するには、このオプションを選択します。エリア認証の設定については、[Add Area/Area Networks]/[Edit Area/Area Networks] ダイアログボックス （141 ページ）を参照してください。エリア認証はデフォルトでディセーブルになっています。したがって、それ以前にエリア認証タイプを指定していない限り、エリア認証を設定するインターフェイスでは、設定するまで認証がディセーブルになっています。 • [Password]：クリアテキストパスワード認証を使用するには、このオプションを選択します。セキュリティ面が懸念される場合は推奨しません。 • [MD5]：MD5認証を使用するには、このオプションを選択します（推奨）。 • [キーチェーン（Key Chain）]：キーチェーン認証を使用するには、このオプションを選択します。
Key Chain	このフィールドは、キー チェーン認証がイネーブルになっている場合に表示されます。][選択（Select）]をクリックして、設定されたキーチェーンを選択します。設定手順については、 キーチェーンの設定 （166 ページ）を参照してください。 （注） 隣接関係を正常に確立するには、ピアに対して同じ認証タイプとキー ID を使用します。
認証パスワード（Authentication Password）	パスワード認証をイネーブルにした場合のパスワード入力設定を指定します。 • [Password]：最大 8 文字のテキスト文字列を入力します。 • [Confirm]：パスワードを再入力します。
MD5のIDとキー（MD5 ID and Keys）	MD5 認証をイネーブルにした場合、MD5 キーおよびパラメータの入力設定を指定します。OSPF 認証を使用するインターフェイス上のすべてのデバイスで、同じ MD5 キーおよび ID を使用する必要があります。 • [MD5キーIDとMD5キー（MD5 Key ID and MD5 Key）] テーブル • [MD5 Key ID]：数値のキー ID。有効値の範囲は、1 ～ 255 です。 • [MD5キー（MD5 Key）]：最大 16 バイトの英数字文字列。

[Add OSPF Virtual Link MD5 Configuration]/[Edit OSPF Virtual Link MD5 Configuration] ダイアログボックス

仮想リンクの認証用の MD5 キーを定義するには、[OSPF 仮想リンク MD5 設定の追加（Add OSPF Virtual Link MD5 Configuration）]/[OSPF 仮想リンク MD5 設定の編集（Edit OSPF Virtual Link MD5 Configuration）] ダイアログボックスを使用します。

ナビゲーション パス

[Add OSPF Virtual Link MD5 Configuration]/[Edit OSPF Virtual Link MD5 Configuration] ダイアログボックスには、[Add OSPF Virtual Link Configuration]/[Edit OSPF Virtual Link Configuration] ダイアログボックス （151 ページ）からアクセスできます。

関連項目

- [Add OSPF Virtual Link Configuration]/[Edit OSPF Virtual Link Configuration] ダイアログボックス （151 ページ）
- [Virtual Link] タブ （150 ページ）
- OSPF の設定 （129 ページ）

フィールド リファレンス

表 79 : [Add OSPF Virtual Link MD5 Configuration]/[Edit OSPF Virtual Link MD5 Configuration] ダイアログボックス

要素	説明
MD5 キー ID（MD5 Key ID）	数値のキー ID。有効値の範囲は、1 ～ 255 です。
MD5 キー（MD5 Key）	最大 16 バイトの英数字文字列。
確認（Confirm）	MD5 キーを再入力します。

[Filtering] タブ

各 OSPF プロセスの ABR タイプ 3 LSA フィルタを設定するには、[Filtering] タブを使用します。ABR タイプ 3 LSA フィルタによって、指定したプレフィックスだけが 1 つのエリアから別のエリアに送信され、その他のプレフィックスはすべて制限されます。このタイプのエリア フィルタリングは、特定の OSPF エリアから、特定の OSPF エリアへ、または同じ OSPF エリアへ同時に適用できます。

利点

OSPF ABR タイプ 3 LSA フィルタリングによって、OSPF エリア間のルート再配布の制御が向上します。

制約事項

フィルタリングされるのは、ABR から送信されるタイプ 3 LSA だけです。

ナビゲーション パス

[Filtering] タブには、[OSPF] ページからアクセスできます。[OSPF] ページの詳細については、OSPF の設定 （129 ページ）を参照してください。

関連項目

- [Add Filtering]/[Edit Filtering] ダイアログボックス （155 ページ）

フィールド リファレンス

表 *80 : [Filtering]* タブ

要素	説明
OSPF Process	フィルタエントリと関連付ける OSPF プロセス。
エリア ID（Area ID）	フィルタ エントリと関連付けるエリアの ID。
プレフィックスリスト名（Prefix List Name）	プレフィックス リストの名前。
Filtered Network	フィルタリングするネットワークの IP アドレスおよびマスク。
トラフィックの方向	OSPF エリアに着信する LSA にフィルタエントリが適用される場合「Inbound」を、OSPF エリアから発信される LSA に適用される場合は「Outbound」を表示します。
シーケンス番号（Sequence #）	フィルタエントリのシーケンス番号。複数のフィルタが LSA に適用されている場合、最もシーケンス番号の小さいフィルタが使用されます。
操作	フィルタに一致する LSA が許可される場合は「Permit」を、フィルタに一致する LSA が拒否される場合は「Deny」を表示します。
下限範囲（Lower Range）	照合される最小プレフィックス長。
Upper Range	照合される最大プレフィックス長。

[Add Filtering]/[Edit Filtering] ダイアログボックス

[Add Filtering]/[Edit Filtering] ダイアログボックスを使用して、[Filter] テーブルに新しいフィルタを追加するか、既存のフィルタを変更します。

ナビゲーション パス

[フィルタ処理の追加（Add Filtering）]/[フィルタ処理の編集（Edit Filtering）] ダイアログボックスには、[Filtering] タブ （154 ページ）からアクセスできます。

関連項目

- OSPF の設定 （129 ページ）

フィールド リファレンス

表 *81 : [Add Filtering]/[Edit Filtering]* ダイアログボックス

要素	説明
OSPF Process	フィルタ エントリと関連付ける OSPF プロセスを選択します。
エリア ID（Area ID）	フィルタ エントリと関連付けるエリアの ID を選択します。
プレフィックスリスト名	適切なプレフィックス リスト オブジェクトを入力または選択します。 **ヒント** [選択（Select）] をクリックして、プレフィックス リスト オブジェクトを選択できるプレフィックス リスト オブジェクト セレクタを開きます。オブジェクト プレフィックス リスト オブジェクト セレクタから新しいオブジェクトを作成することもできます。詳細については、[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （235 ページ）を参照してください。
Filtered Network	フィルタリングするネットワークの IP アドレスおよびマスクを入力します。
トラフィックの方向	フィルタリングするトラフィックの方向を選択します。OSPF エリアへの LSA をフィルタリングするには [着信（Inbound）] を選択し、OSPF エリアからの LSA をフィルタリングするには [発信（Outbound）] を選択します。
シーケンス番号（Sequence Number）	フィルタのシーケンス番号を入力します。有効値の範囲は 1 ～ 4294967294 です。複数のフィルタが LSA に適用されている場合、最もシーケンス番号の小さいフィルタが使用されます。
操作	LSA トラフィックを許可するには [許可（Permit）] を選択し、LSA トラフィックをブロックするには [拒否（Deny）] を選択します。
下限範囲（Lower Range）	照合される最小プレフィックス長を指定します。この設定の値は、[Filtered Network] フィールドに入力するネットワーク マスクの長さよりも大きく、[Upper Range] フィールドに入力する値（ある場合）以下である必要があります。

要素	説明
Upper Range	照合される最大プレフィックス長を入力します。この設定の値は、[Lower Range] フィールドに入力する値（ある場合）以上である必要があります。または、[Lower Range] フィールドがブランクの場合は、[Filtered Network] フィールドに入力するネットワーク マスクの長さよりも大きい値である必要があります。

[フィルタルール（Filter Rule）] タブ

[フィルタルール（Filter Rule）] タブを使用して、Open Shortest Path First（OSPF）アップデートで送受信されるネットワークをフィルタリングするルールを設定します。

（注） フィルタ ルールは、ASA 9.2(1)+ でのみサポートされます。

ナビゲーション パス

[フィルタルール（Filter Rule）] タブには、[OSPF] ページからアクセスできます。[OSPF] ページの詳細については、OSPF の設定 （129 ページ）を参照してください。

関連項目

- [フィルタルールの追加/編集（Add/Edit Filter Rule）] ダイアログボックス （158 ページ）

フィールド リファレンス

表 *82 : [フィルタルール（Filter Rule）] タブ*

要素	説明
プロセス ID（Process ID）	フィルタルールと関連付ける OSPF プロセス。
ACL	標準 IP アクセス リスト名。このリストは、受信されるネットワークとルーティング アップデートで抑制されるネットワークを定義します。
方向（Direction）	フィルタルールの方向： • [in]：このルールは、着信ルーティングアップデートからのデフォルトルート情報をフィルタリングします。 • [out]：このルールは、発信ルーティングアップデートからのデフォルトルート情報をフィルタリングします。

要素	説明
インターフェイス	（オプション）フィルタルールが適用されるインターフェース。
ルーティングプロセス（Routing Process）	ルーティングプロセス：[なし（None）]、[BGP]、[接続（Connected）]、[EIGRP]、[OSPF]、[RIP]、または [静的（Static）]。
ルーティングプロセス ID（Routing Process ID）	ルーティングプロセスの識別子。

[フィルタルールの追加/編集（Add/Edit Filter Rule）] ダイアログボックス

[フィルタルールの追加（Add Filter Rule）]/[フィルタルールの編集（Edit Filter Rule）] ダイアログボックスを使用して、既存のフィルタルールテーブルに新しいフィルタルールを追加するか、または既存のフィルタルールを変更します。

（注） フィルタ ルールは、ASA 9.2(1)+ でのみサポートされます。

ナビゲーション パス

[フィルタルールの追加（Add Filter Rule）]/[フィルタルールの編集（Edit Filter Rule）] ダイアログボックスには、[フィルタルール（Filter Rule）] タブ （157 ページ）からアクセスできます。

関連項目

- OSPF の設定 （129 ページ）

フィールド リファレンス

表 *83 : [フィルタルールの追加/編集（Add/Edit Filter Rule）] ダイアログボックス*

要素	説明
OSPF Process	フィルタルールと関連付ける OSPF プロセスを選択します。
ACL	受信されるネットワークとルーティングアップデートで抑制されるネットワークを定義するアクセス制御リストを選択します。

要素	説明
方向	フィルタルールの方向を指定します。 • [in]：このルールは、着信ルーティングアップデートからのデフォルトルート情報をフィルタリングします。 • [out]：このルールは、発信ルーティングアップデートからのデフォルトルート情報をフィルタリングします。
インターフェイス	（任意）ルーティングアップデートを適用するインターフェイスを指定します。インターフェイスを指定すると、アクセスリストは指定されたインターフェイスで受信されたルーティングアップデートにのみ適用されます。
ルーティングプロセス	[なし（None）]、[BGP]、[接続済み（Connected）]、[EIGRP]、[OSPF]、[RIP]、または [スタティック（Static）] のルーティングプロセスのうち、フィルタ処理するものを選択します。
ルーティングプロセス ID	ルーティングプロセスの識別子を入力します。BGP、EIGRP、EIGRP、および OSPF ルーティングプロトコルに適用されます。

[サマリーアドレス（Summary Address）] タブ

各 OSPF ルーティング プロセスのサマリー アドレスを設定するには、[Summary Address] タブを使用します。

他のルーティングプロトコルから学習したルートをサマライズできます。サマリーのアドバタイズに使用されるメトリックは、具体的なルートすべての中で最小のメトリックです。集約ルートは、ルーティング テーブルのサイズを削減するのに役立ちます。

OSPF の集約ルートを使用すると、OSPF ASBR は、そのアドレスでカバーされるすべての再配布ルートの集約として、1 つの外部ルートをアドバタイズします。OSPF に再配布されている、他のルーティング プロトコルからのルートだけをサマライズできます。

ナビゲーション パス

[Summary Address] タブには、[OSPF] ページからアクセスできます。[OSPF] ページの詳細については、OSPF の設定 （129 ページ）を参照してください。

関連項目

- [サマリーアドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス （160 ページ）

フィールド リファレンス

表 84 : [サマリーアドレス（*Summary Address*）] タブ

要素	説明
プロセス ID（Process ID）	サマリーアドレスに関連付けられた OSPF プロセス。
ネットワーク （Network）	サマリーアドレスの IP アドレスおよびネットワークマスク。
タグ	各外部ルートに付加される 32 ビットの 10 進値。この値は OSPF 自体には使用されません。ASBR 間での情報通信に使用されることはあります。
[アドバタイズ（Advertise）]	サマリールートがアドバタイズされる場合は「true」が表示されます。サマリールートがアドバタイズされない場合は「false」が表示されます。

[サマリーアドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス

[サマリーアドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックスを使用して、新しいエントリを追加するか、サマリーアドレステーブルの既存のエントリを変更します。

ナビゲーション パス

[サマリーアドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックスには、[サマリーアドレス（Summary Address）] タブ （159 ページ）からアクセスできます。

関連項目

- OSPF の設定 （129 ページ）

フィールド リファレンス

表 85 : [サマリーアドレスの追加/編集（*Add/Edit Summary Address*）] ダイアログボックス

要素	説明
OSPF Process	サマリーアドレスに関連付けられた OSPF プロセスを選択します。既存のエントリを編集する場合、この情報は変更できません。
ネットワーク （Network）	サマリーアドレスの IP アドレスおよびネットワークマスク。
タグ	タグ値は、各外部ルートに付加される 32 ビットの 10 進値です。これは OSPF 自体には使用されません。ASBR 間での情報通信に使用されることはあります。有効値の範囲は、0 ～ 4294967295 です。

要素	説明
[アドバタイズ（Advertise）]	選択すると、サマリー ルートがアドバタイズされます。サマリー アドレスになるルートを抑止するには、このチェックボックスをオフにします。デフォルトでは、このチェックボックスはオンです。

[Interface] タブ

[Interface] タブを使用して、インターフェイス固有の OSPF 認証ルーティング プロパティを設定します。

ナビゲーション パス

[Interface] タブには、[OSPF] ページからアクセスできます。[OSPF] ページの詳細については、OSPF の設定 （129 ページ）を参照してください。

関連項目

- [Add Interface]/[Edit Interface] ダイアログボックス （163 ページ）

フィールド リファレンス

表 86 : [Interface] タブ

要素	説明
インターフェイス（Interface）	設定が適用されるインターフェイスの名前。
認証	インターフェイス上でイネーブルにする OSPF 認証のタイプ。認証タイプには、次のいずれかの値を指定できます。 • [None]：OSPF 認証はディセーブルになります。 • [Password]：クリア テキスト パスワード認証がイネーブルになります。 • [MD5]：MD5 認証がイネーブルになります。 • [Area]：エリアに対して指定された認証タイプがインターフェイスでイネーブルになります。エリア認証が、インターフェイスのデフォルト値です。ただし、エリア認証は、デフォルトではディセーブルになっています。そのため、あらかじめエリア認証タイプを指定してある場合を除いて、エリア認証を指定したインターフェイスでは認証がディセーブルになります。 • [キーチェーン（Key Chain）]：キーチェーン認証を許可します。

要素	説明
ポイントツーポイント	インターフェイスが非ブロードキャスト（ポイントツーポイント）に設定されている場合は「true」が表示されます。インターフェイスがブロードキャストに設定されている場合は、「false」が表示されます。
コスト（Cost）	インターフェイスを介したパケット送信のコスト。
プライオリティ	インターフェイスに割り当てられる OSPF プライオリティ。
MTU Ignore	MTU不一致検出がイネーブルの場合は、「false」が表示されます。MTU不一致検出がディセーブルの場合は「true」が表示されます。
Database Filter	同期およびフラッディング中に発信 LSA がフィルタリングされる場合は、「true」が表示されます。フィルタリングがイネーブルではない場合は「false」を表示します。
Hello 間隔（Hello Interval）	インターフェイス上で送信されるhelloパケット間の間隔（秒数）。hello間隔を小さくすると、トポロジ変更はより高速に検出されますが、インターフェイス上で送信されるトラフィックはより多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバーで同じである必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 10 秒です。
送信遅延（Transmit Delay）	インターフェイス上で LSA パケットを送信するために必要と推定される時間（秒数）。更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 1 秒です。
再送信間隔（Retransmit Interval）	インターフェイスに属する隣接関係へのLSA再送信間の時間（秒数）。ルータが自身のネイバーにLSAを送信する場合、ルータは確認応答メッセージを受信するまでそのLSAを保持します。確認応答を受信しなかった場合、ルータでは LSA を再送します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 5 秒です。
dead 間隔（Dead Interval）	helloパケットが受信されないために、ネイバーがルータ ダウンを宣言するまでの時間間隔（秒数）。有効値の範囲は1～65535です。この設定のデフォルト値は、[Hello Interval] フィールドに設定されている時間間隔の 4 倍です。

要素	説明
Hello Multiplier （ASA 9.2(1) 以降のみ）	1 秒あたりに送信される hello パケットの数。有効な値は、3 ～ 20 です。

[Add Interface]/[Edit Interface] ダイアログボックス

[Add Interface]/[Edit Interface] ダイアログボックスを使用して、インターフェイスの OSPF 認証ルーティング プロパティを追加するか、既存のエントリを変更します。

（注） ASA バージョン 9.2(1) 以降、Hello 間隔、送信遅延、再送信間隔、およびデッド間隔の許容エントリの上限が 65535 秒から 8192 秒に削減されました。8192 を超える値を使用する共有ポリシーを設定した場合、そのポリシーが 9.2(1) 以降のデバイスに割り当てられていると、検証エラーが送信されます。

ナビゲーション パス

[Add Interface]/[Edit Interface] ダイアログボックスには、[Interface] タブ （111 ページ）からアクセスできます。

関連項目

- OSPF の設定 （129 ページ）

フィールド リファレンス

表 87 : [Add Interface]/[Edit Interface] ダイアログボックス

要素	説明
インターフェイス（Interface）	設定が適用されるインターフェイスの名前。

要素	説明
認証	インターフェイス上でイネーブルにする OSPF 認証のタイプ。認証タイプには、次のいずれかの値を指定できます。 • [認証なし（No Authentication）]：OSPF 認証が無効になります。 • [Area Authentication]：エリアに対して指定された認証タイプがインターフェイスでイネーブルになります。エリア認証が、インターフェイスのデフォルト値です。ただし、エリア認証は、デフォルトではディセーブルになっています。そのため、あらかじめエリア認証タイプを指定してある場合を除いて、エリア認証を指定したインターフェイスでは認証がディセーブルになります。 • [パスワード認証（Password Authentication）]：クリアテキストパスワード認証を有効にします。 • [MD5 Authentication]：MD5 認証がイネーブルになります。 • [キーチェーン（Key Chain）]：キーチェーン認証を有効にします。
Key Chain	[選択（Select）] をクリックして、設定されたキーチェーンを選択します。設定手順については、キーチェーンの設定 （166 ページ）を参照してください。 （注） 隣接関係を正常に確立するには、ピアに対して同じ認証タイプとキー ID を使用します。
認証パスワード（Authentication Password）	パスワード認証をイネーブルにした場合のパスワード入力設定を指定します。 • [Enter Password]：最大 8 文字のテキスト文字列を入力します。 • [Confirm]：パスワードを再入力します。
MD5 キー ID とキー（MD5 Key ID and Keys）	MD5 認証をイネーブルにした場合、MD5 キーおよびパラメータの入力設定を指定します。OSPF 認証を使用するインターフェイス上のすべてのデバイスで、同じ MD5 キーおよび ID を使用する必要があります。 • [Key ID]：数値のキー ID を入力します。有効値の範囲は、1 ～ 255 です。 • [Key]：最大 16 バイトの英数字文字列。 • [Confirm]：MD5 キーを再入力します。 上記の値を入力し、[>>] をクリックしてキー情報を [キー（Keys）] テーブルに追加します。キーエントリを選択し、[<<] をクリックして [キー（Keys）] テーブルから削除します。
コスト（Cost）	インターフェイスを介したパケット送信のコスト。

要素	説明
プライオリティ	インターフェイスに割り当てられる OSPF プライオリティ。
MTU Ignore	選択すると、MTU 不一致検出がディセーブルになります。MTU 不一致検出をイネーブルにするには、このチェックボックスをオフにします。
データベースフィルタ All Out（Database Filter All Out）	選択すると、同期およびフラッディング中に発信 LSA がフィルタリングされます。フィルタリングをディセーブルにするには、このチェックボックスをオフにします。
Hello 間隔（秒）（Hello Interval (sec)）	インターフェイス上で送信される hello パケット間の間隔（秒数）。hello間隔を小さくすると、トポロジ変更はより高速に検出されますが、インターフェイス上で送信されるトラフィックはより多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバーで同じである必要があります。 ASA 9.2(1)+ デバイスでは、有効な値の範囲は 1 ～ 8192 秒です。その他すべてのデバイスでは、有効な値の範囲は 1 ～ 65535 秒です。デフォルト値は 10 秒です。
Transmit Delay (sec)	インターフェイス上で LSA パケットを送信するために必要と推定される時間（秒数）。更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。 ASA 9.2(1)+ デバイスでは、有効な値の範囲は 1 ～ 8192 秒です。その他すべてのデバイスでは、有効な値の範囲は 1 ～ 65535 秒です。デフォルト値は 1 秒です。
再送信間隔（Retransmit Interval）（秒）	インターフェイスに属する隣接関係への LSA 再送信間の時間（秒数）。ルータが自身のネイバーに LSA を送信する場合、ルータは確認応答メッセージを受信するまでその LSA を保持します。ルータは、確認応答メッセージを受信しないと、LSA を再び送信します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。 ASA 9.2(1)+ デバイスでは、有効な値の範囲は 1 ～ 8192 秒です。その他すべてのデバイスでは、有効な値の範囲は 1 ～ 65535 秒です。デフォルト値は 5 秒です。

要素	説明
デッド間隔（Dead Interval）（秒）	helloパケットが受信されないために、ネイバーがルータ ダウンを宣言するまでの時間間隔（秒数）。 ASA 9.2(1)+ デバイスでは、有効な値の範囲は 1 ～ 8192 秒です。その他すべてのデバイスでは、有効な値の範囲は 1 ～ 65535 秒です。この設定のデフォルト値は、[Hello Interval] フィールドに設定されている時間間隔の 4 倍です。
hello 乗数（Hello Multiplier）（Hello/秒） （ASA 9.2(1) 以降のみ）	1 秒あたりに送信される hello パケットの数。有効な値は、3 ～ 20 です。 （注） Hello 乗数を指定すると、Hello 間隔とデッド間隔の値は無視されます。Hello 間隔またはデッド間隔の値を入力した場合、Hello 間隔およびデッド間隔の設定の代わりに Hello 乗数を使用するかどうかを確認するように求められます。
ポイントツーポイント	インターフェイスが非ブロードキャスト（ポイントツーポイント）に設定されている場合は「true」が表示されます。インターフェイスがブロードキャストに設定されている場合は、「false」が表示されます。

キーチェーンの設定

ネットワークデバイスは、データセキュリティと保護を向上させるため、IGP ピアを認証するために 180 日以下の期間の循環キーを使用して設定されます。循環キーは、悪意のあるユーザーがルーティング プロトコル認証に使用されているキーを推測できないようにし、ネットワークによる誤ったルートのアドバタイズやトラフィックのリダイレクトを防ぎます。頻繁にキーを変更することで、推測されるリスクを最終的に軽減します。キー チェーンを提供するルーティング プロトコルの認証を設定する場合は、キー チェーン内でキーを設定してライフタイムを重複させます。このように設定すると、アクティブなキーの不在によりキーで保護された通信が失われるのを防ぐことができます。キーのライフタイムが切れ、アクティブなキーがなくなると、OSPF は最後に有効だったキーを使用してピアとの隣接関係を維持します。

Cisco Security Manager のキーチェーン設定には、次の 2 つの制限があります。

- 設定されたキー ID は、[OOB (Out of Band) Changes] ダイアログボックスでは暗号化されていない形式で表示されます
- プロビジョニングをコピーするオプションは、キーチェーンでは利用できません。

関連項目

- キーのライフタイム （167 ページ）
- キーチェーンの追加/編集 （167 ページ）

キーのライフタイム

安定した通信を維持するためには、各デバイスがキー チェーンの認証キーを保存し、複数のキーを同時に機能に使用します。キーの送信と受け入れのライフタイムに基づき、キーのロールオーバーを処理するセキュアなメカニズムがキーチェーン管理によって提供されます。デバイスは、キーのライフタイムを使用してキーチェーン内でアクティブになっているキーを判断します。

キー チェーン内の各キーには 2 つのライフタイムがあります。

- 受け入れライフタイム：別のデバイスとのキー交換時にデバイスがそのキーを受け入れる期間。
- 送信ライフタイム：別のデバイスとのキー交換時にデバイスがそのキーを送信する期間。

キーの送信ライフタイム中、デバイスはルーティング アップデート パケットをキーとともに送信します。送信されたキーがデバイス上のキーの受け入れライフタイム期間内でない場合、そのデバイスはキーを送信したデバイスからの通信を受け入れません。

ライフタイムが設定されていない場合は、タイムラインなしで MD5 認証を設定するのと同じことになります。

キーの選択

- キー チェンに複数の有効なキーがある場合、OSPF はライフタイムが最大のキーを選択します。
- ライフタイムが無限のキーが優先されます。
- ライフタイムが同じキーが複数ある場合は、もっとも大きなキー ID を持つキーが優先されます。

関連項目

- キーチェーンの設定 （166 ページ）
- キーチェーンの追加/編集 （167 ページ）

キーチェーンの追加/編集

[キーチェーンの追加/編集（Add/Edit KeyChain）] ダイアログボックスを使用して、新しいエントリを追加するか、キーチェーンテーブルの既存のエントリを変更します。

ナビゲーション パス

- [キーチェーン（Key Chain）] ページタブには、[OSPF] ページの [インターフェイス（Interface）] からアクセスできます。[Interface] タブの詳細については、[Interface] タブ（111 ページ）を参照してください。
- [管理（Manage）]>[ポリシーオブジェクト（Policy Objects）]>[キーチェーン（Key Chain）] から、[キーチェーンの追加（Add Key Chain）] ページに直接アクセスできます。

ステップ 1 認証用のキーチェーンを含むキー チェーン ポリシー オブジェクトを作成します。

a) [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] ウィンドウを開きます（Policy Object Managerを参照）。
b) コンテンツテーブルから [キーチェーン（Key Chain）] を選択します。
c) 右クリックし、[新規オブジェクト（New Object）] を選択します。
d) [キーチェーンの追加（Add Key Chain）] ダイアログボックスで、オブジェクトの名前を入力します（Chain 1 など）。
e) [追加（Add）] ボタンをクリックして、キーチェーンエントリを [キーチェーン（Key Chain）] リストに追加します。

ステップ 2 [キーチェーンエントリの追加（Add Key Chain Entry）] ダイアログボックスに関連する値を入力します。

フィールドリファレンス

表 *88 : [キーチェーンエントリの追加（Add Key Chain Entry）] ページ*

要素	説明
アルゴリズム	認証に使用されるデフォルトの暗号化アルゴリズムは MD5 です。
Key ID	0 ～ 255 の範囲の値を入力します。 （注） キー ID は、[OOB (Out of Band) Changes] ダイアログボックス に暗号化された形式では表示されません。
認証タイプ（Authentication Type）	関連するオプションを選択します。 • [クリアテキスト（Clear Text）]：認証キーをテキスト形式で取得します。 • [暗号化（Encryption）]：認証キーを暗号化された形式にします。
Key String	キー文字列を入力します。
[キー文字列の確認（Confirm Key String）]	同じキー文字列を再入力します。
[受け入れライフタイムの設定（Accept Lifetime Settings）]：別のデバイスとのキー交換時にデバイスがそのキーを受け入れる期間を入力します。	
タイムゾーン（Timezone）	[UTC] または [ローカル（Local）] のいずれかを選択します。
[開始日時（Start Date/Time）]	開始日時を hh:mm:ss 形式で入力します。

要素	説明
[終了時間のタイプ（End Time Type）]	関連するオプションを選択します。 • [日時（Date Time）]：ライフタイムが終了する絶対時間。 • [期間（Duration）]：開始時からライフタイムが終了するまでの経過秒数。 • [無限（Infinite）]：無限のライフタイム（終了時間なし）
End Date	絶対的な日時を指定します。このオプションは、[終了時間のタイプ（End Time Type）] として [期間（Duration）] または [無限（Infinite）] を選択した場合は使用できません。
期間	開始時からライフタイムが終了するまでの経過秒数を入力します。許容範囲は 1 ～ 2147483646 です。このオプションは、[終了時間のタイプ（End Time Type）] として [日時（Date Time）] または [無限（Infinite）] を選択した場合は使用できません。
[送信ライフタイムの設定（Send Lifetime Settings）]：別のデバイスとのキー交換時にデバイスがそのキーを送信する期間。	
タイムゾーン（Timezone）	[UTC] または [ローカル（Local）] のいずれかを選択します。
[開始日時（Start Date/Time）]	開始日時を hh:mm:ss 形式で入力します。
[終了時間のタイプ（End Time Type）]	関連するオプションを選択します。 • [日時（Date Time）]：ライフタイムが終了する絶対時間。 • [期間（Duration）]：開始時からライフタイムが終了するまでの経過秒数。 • [無限（Infinite）]：無限のライフタイム（終了時間なし）
End Date	絶対的な日時を指定します。このオプションは、[終了時間のタイプ（End Time Type）] として [期間（Duration）] または [無限（Infinite）] を選択した場合は使用できません。
期間	開始時からライフタイムが終了するまでの経過秒数を入力します。許容範囲は 1 ～ 2147483646 です。このオプションは、[終了時間のタイプ（End Time Type）] として [日時（Date Time）] または [無限（Infinite）] を選択した場合は使用できません。

ステップ 3 [OK] をクリックします。データベースに変更を送信することを忘れないでください。

次のタスク

関連項目

- キーチェーンの設定 （166 ページ）
- キーのライフタイム （167 ページ）

OSPFv3 の設定

[OSPFv3] ページには、ファイアウォールデバイスで OSPF（Open Shortest Path First）バージョン 3 ルーティングを設定するための 2 つのタブ付きパネルがあります。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから[プラットフォーム（Platform）]>[ルーティング（Routing）] > [OSPFv3] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [OSPFv3] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

これは、OSPFv3 プロセスを設定して [OSPFv3] ページでインターフェイスに割り当てるための基本的な手順です。

1. [プロセス（Process）] タブ （173 ページ） で、次の手順を実行します。
   - [OSPFv3プロセス（OSPFv3 Process）] ドロップダウンリストから [プロセス1（Process 1）] または [プロセス2（Process 2）] を選択して、2 つのプロセスのどちらを設定するかを指定します。
   - [OSPFv3プロセスの有効化（Enable OSPFv3 Process）] をオンにします。
   - [プロセスID（Process ID）] を割り当てます。1 ～ 65535 の任意の正の整数を使用できます。
   - プロセスを定義するには、必要に応じて次の機能を使用します。
   - [詳細（Advanced）] ボタン。[OSPFv3の詳細プロパティ（OSPFv3 Advanced Properties）] ダイアログボックス （174 ページ）が開きます。
   - [エリア（Area）] タブ（OSPFv3） （180 ページ）。Add/Edit Area Dialog Box（OSPFv3） （181 ページ）、範囲の追加/編集ダイアログボックス（OSPFv3） （183 ページ）、Add/Edit Virtual Link Dialog Box（OSPFv3） （184 ページ）を使用して、エリア、範囲、および仮想リンクの定義を管理します。
   - [再配布（Redistribution）] パネル。Add/Edit Redistribution Dialog Box（OSPFv3） （186 ページ）を使用して、ルート再配布の定義を管理します。

- [サマリープレフィックス（Summary Prefix）] パネル。[サマリープレフィックスの追加/編集（Add/Edit Summary Prefix）] ダイアログボックス（OSPFv3） （188 ページ）を使用してサマリープレフィックス定義のを管理します。

2. [OSPFv3インターフェイス（OSPFv3 Interface）] タブ （189 ページ） で、次の手順を実行します。
   1. [インターフェイス（Interface）] パネルと [ネイバー（Neighbor）] パネルで、[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（OSPFv3） （189 ページ）および[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス（OSPFv3） （194 ページ）を使用してプロセスを特定のインターフェイスに割り当てます。

関連項目

- OSPFv3 について （171 ページ）

OSPFv3 について

Open Shortest Path First（OSPF）は、パス選択に距離ベクトルではなくリンク ステートを使用する Interior Gateway Routing Protocol です。バージョン 3 は、基本的に IPv6 向けに拡張された OSPFv2 です。OSPFv2 に似ていますが（OSPF について （130 ページ）を参照）、下位互換性はありません。OSPF を使用して IPv4 パケットと IPv6 パケットの両方をルーティングするには、OSPFv2 と OSPFv3 の両方を同時に実行する必要があります。これらは互いに共存しますが、相互に連携しません。

（注） OSPFv3 は、シングルコンテキストのルーテッドモードでのみ動作する ASA 9.0 以降のデバイスでサポートされます。つまり、マルチコンテキストとトランスペアレントモードはサポートされていません。

リンクを、ネットワーキングデバイス上のインターフェイスとして考えます。リンクステートプロトコルは、送信元デバイスと宛先デバイスを接続するリンクの状態に基づいて、ルーティングの決定を行います。リンク ステートは、インターフェイスと、その隣接ネットワーキングデバイスとの関係を説明するものです。インターフェイス情報には、インターフェイスの IPv6 プレフィックス/長、接続先のネットワークのタイプ、そのネットワークに接続されているデバイスなどが含まれます。この情報は、さまざまなタイプのリンクステートアドバタイズメント（LSA）で伝播されます。ルーティングテーブル全体ではなく LSA だけが交換されるため、OSPF ネットワークは RIP ネットワークよりも迅速に収束します。

ASA は、OSPFv3 プロトコルのプロセスを 2 つ同時に異なるインターフェイスセット上で実行できます。同じ IP アドレスを使用する複数のインターフェイス（NAT ではこのようなインターフェイスが共存可能ですが、OSPFv3 ではアドレスは重複できません）がある場合に、2 つのプロセスを実行できます。あるいは、ルートのサブセットを 2 つのプロセス間で再配布して、一方のプロセスを内部インターフェイスで実行しながら別のプロセスを外部で実行できます。

同様に、プライベート アドレスをパブリック アドレスから分離する必要がある場合もあります。

別の OSPFv3 ルーティングプロセス、RIP ルーティングプロセス、または OSPFv3 対応インターフェイスで設定されたスタティックルートおよび接続ルートから、ルートを OSPFv3 ルーティングプロセスに再配布できます。

NAT が使用されるが、OSPFv3 がパブリックエリアだけで実行されている場合、パブリック ネットワークへのルートは、プライベートネットワーク内でデフォルトまたはタイプ 5 AS External LSA として再配布できます。ただし、セキュリティ アプライアンスによって保護されているプライベート ネットワークのスタティック ルートを設定する必要があります。また、同じセキュリティ アプライアンス インターフェイスで、パブリック ネットワークとプライベート ネットワークを混在させないでください。

OSPFv2 と OSPFv3 の相違点

OSPFv3 では、OSPFv2 の機能に次の機能が追加されます。

- ネイバー探索およびその他の機能に対する IPv6 リンクローカル アドレスの使用。
- プレフィックスおよびプレフィックス長として表される LSA。
- 2 つの LSA タイプの追加。
- 未知の LSA タイプの処理。
- リンクごとのプロトコル処理。
- アドレッシング セマンティックの削除。
- フラッディング スコープの追加。
- リンクごとの複数インスタンスのサポート。
- RFC-4552 で指定されている OSPFv3 ルーティング プロトコル トラフィックの IPSec ESP 標準を使用する認証サポート。

設定の制約事項

ASA OSPFv3 設定の制限は次のとおりです。

- 特定のインターフェイスで OSPFv3 をイネーブルにするには、そのインターフェイスで IPv6 を有効にし、名前を付ける必要があります。
- インターフェイスに割り当てることができるのは、1 つのエリアと 1 つのインスタンスを持つ 1 つの OSPFv3 プロセスだけです。
- インターフェイス ネイバー エントリは、OSPFv3 がイネーブルになっている場合にのみ有効であり、ネットワークタイプは指定されたインターフェイスでポイントツーポイントである必要があります。
- インターフェイス ネイバー アドレスは、リンクローカルアドレスである必要があります。

- エリア範囲テーブルの範囲値は、エリア全体で一意である必要があります。
- エリアがNSSA またはスタブに設定されている場合、同じエリアを仮想リンクに設定することはできません。
- OSPFv3 再配布は、同じ OSPFv3 プロセスには適用されません。
- ASA クラスタで使用する場合は、OSPFv3 暗号化を無効にする必要があります。
- レイヤ 3 クラスタプールは、OSPFv3 とインターフェイスの間で共有されません。

関連項目

- OSPFv3 の設定 （170 ページ）
- [プロセス（Process）] タブ （173 ページ）
- [OSPFv3インターフェイス（OSPFv3 Interface）] タブ （189 ページ）

[プロセス（Process）] タブ

[OSPFv3] ページの [プロセス（Process）] タブを使用して、最大 2 つの OSPFv3 ルーティングプロセスを有効にして設定します。各 OSPF プロセスには、独自のエリアとネットワークが関連付けられます。それぞれについて、最低でも OSPFv3 用のエリアを作成して、OSPFv3 のインターフェイスを有効にする必要があります。その後、ターゲットの OSPFv3 ルーティングプロセスにルートを再配布する必要があります。シングルコンテキストモードのみがサポートされていることに注意してください。

ナビゲーション パス

[プロセス（Process）] タブは [OSPFv3] ページにあります。

- （デバイスビュー）デバイスポリシーセレクタから[プラットフォーム（Platform）]>[ルーティング（Routing）] > [OSPFv3] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [OSPFv3] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- OSPFv3 の設定 （170 ページ）
- OSPFv3 について （171 ページ）
- [エリア（Area）] タブ（OSPFv3） （180 ページ）
- [OSPFv3インターフェイス（OSPFv3 Interface）] タブ （189 ページ）

フィールド リファレンス

表 89 : [プロセス（Process）] タブ

要素	説明
OSPFv3 Process	設定している OSPFv3 プロセスを識別します。[プロセス1（Process 1）] または [プロセス2（Process 2）] を選択します。1 つまたは両方を有効にすることができます。
OSPFv3 プロセスを有効化	選択した OSPFv3 プロセスを有効にするには、このボックスをオンにします。OSPFv3 プロセスを無効にするには、このオプションの選択を解除します。プロセス設定情報は、後で再度有効にする場合に備えて保持されます。
プロセス ID（Process ID）	このプロセスの一意の数値 ID を入力します。ID には、1 から 65535 までの任意の正の整数を指定できます。 このプロセス ID は内部で使用され、他の OSPFv3 デバイスの OSPFv3 プロセス ID と一致する必要はありません。
詳細設定（Advanced）	[OSPFv3の詳細プロパティ（OSPFv3 Advanced Properties）] ダイアログボックス （174 ページ）が開き、[ルータID（Router ID）]、[隣接関係の変更（Adjacency Changes）]、[ルートのアドミニストレーティブディスタンス（Administrative Route Distances）]、[タイマー（Timers）]、[デフォルトの情報送信元（Default Information Originate）]、[パッシブインターフェイス（Passive Interface）] 設定など、その他のプロセス関連パラメータを設定できます。
領域	このパネルのタブとテーブルを使用して、エリア、範囲、および仮想リンクの定義を管理します。これらの定義の詳細については、[エリア（Area）] タブ（OSPFv3） （180 ページ）を参照してください。
再配布	このパネルを使用して、再配布定義を管理します。これらの定義の詳細については、 Add/Edit Redistribution Dialog Box（OSPFv3） （186 ページ）を参照してください。
サマリープレフィックス	このパネルを使用して、サマリープレフィックスの定義を管理します。これらの定義の詳細については、[サマリープレフィックスの追加/編集（Add/Edit Summary Prefix）] ダイアログボックス（OSPFv3） （188 ページ）を参照してください。

[OSPFv3の詳細プロパティ（OSPFv3 Advanced Properties）] ダイアログボックス

[OSPF Advanced] ダイアログボックスを使用して、OSPF プロセスの [Router ID]、[Adjacency Changes]、[Administrative Route Distances]、[Timers]、[Default Information Originate] などの設定を行うことができます。

ナビゲーション パス

[OSPF Advanced] ダイアログボックスには、[プロセス（Process）] タブ （173 ページ）からアクセスできます。

関連項目

- OSPFv3 の設定 （170 ページ）
- OSPFv3 について （171 ページ）

フィールド リファレンス

表 90 : [OSPF Advanced] ダイアログボックス

要素	説明
OSPF Process	この読み取り専用フィールドには、設定している OSPF プロセスの ID が表示されます。
ルータ ID（Router ID）	単一のデバイスで、[自動（Automatic）] または [IPアドレス（IP Address）] を選択します。（IP アドレスを選択すると、[アドレス（address）] フィールドが表示されます。） [自動（Automatic）] を選択すると、セキュリティアプライアンス上で最上位の IP アドレスがルータ ID として使用されます。固定ルータ ID を使用するには、[IPアドレス（IP Address）] を選択して、[ルータID（Router ID）] フィールドに IPv4 アドレスを入力します。 デバイスクラスタで、[自動（Automatic）] または [クラスタプール（Cluster Pool）] を選択します。（[クラスタプール（Cluster Pool）] を選択すると、[IPv4プールオブジェクトID（IPv4 Pool object ID）] フィールドが表示されます）。 [クラスタプール（Cluster Pool）] を選択した場合は、ルータの ID アドレスを提供する IPv4 プールオブジェクトの名前を入力または選択します。詳細については、[IPv4プールの追加または編集（Add or Edit IPv4 Pool）] ダイアログボックスを参照してください。
Ignore LSA MOSPF	このオプションを選択すると、セキュリティ アプライアンスがタイプ 6（MOSPF）LSA パケットを受信したときに、syslog メッセージの送信が抑止されます。

要素	説明
隣接関係の変更	これらのオプションでは、隣接関係の変更が発生したときに送信される syslog メッセージを指定します。 • [Log Adjacency Changes]：選択すると、OSPF ネイバーの起動またはダウン時に常に、セキュリティ アプライアンスによって syslog メッセージが送信されます。このボックスをチェックすると、[詳細を含める（Include Details）] オプションが有効になります。 • [詳細を含める（Include Details）]：選択すると、ネイバーの起動またはダウン時だけでなく、状態の変更が発生したときにはいつでも、セキュリティアプライアンスによって syslog メッセージが送信されます。このオプションは、[隣接関係の変更を記録（Log Adjacency Changes）] がチェックされている場合にのみ使用できます。
Administrative Route Distances	ルート タイプに基づく管理ルート ディスタンスの設定。 • [Inter Area]：1 つのエリアから別のエリアへのすべてのルートのアドミニストレーティブ ディスタンス。有効値の範囲は 1 ～ 254 で、デフォルト値は 110 です。 • [Intra Area]：エリア内のすべてのルートのアドミニストレーティブ ディスタンス。有効値の範囲は 1 ～ 254 で、デフォルト値は 110 です。 • [External]：再配布によって学習された他のルーティング ドメインからのすべてのルートのアドミニストレーティブディスタンス。有効値の範囲は 1 ～ 254 で、デフォルト値は 110 です。

要素	説明
タイマー（ミリ秒）	

要素	説明
	LSA およびSPF スロットリングは、ネットワークが不安定になっている間に OSPFv3 の LSA 更新速度を低下させ、LSA レート制限を提供することにより、より高速な OSPFv3 変換を可能にするダイナミックメカニズムを提供します。LSA ペーシングおよびSPF 計算タイマーを設定するために使用される設定。 • [LSA着信（LSA Arrival）]：ネイバーから着信する同一 LSA の最短受信間隔を指定します。有効な値の範囲は、0～600000 ミリ秒です。デフォルトは 1000 です。 • [LSAフラッドペーシング（LSA Flood Pacing）]：フラッディングキュー内の LSA が更新と更新の間でペーシングされる時間の長さ。有効値の範囲は、5 ～ 100 ミリ秒です。デフォルト値は 33 です。 • [LSAグループのペーシング（LSA Group Pacing）]：LSA がグループにまとめられ、更新、チェックサム、およびエージングされる間隔。有効値の範囲は 10 ～ 1800 で、デフォルト値は 240 ミリ秒です。 • [LSA再送信のペーシング（LSA Retransmission Pacing）]：再送信キュー内の LSA がペーシングされる時間の長さ。有効値の範囲は、5 ～ 200 ミリ秒です。デフォルト値は 66 です。 • [LSAスロットル（LSA Throttle）]：LSA の最初の発信を引き起こす遅延（ミリ秒単位）。有効な値の範囲は、0～600000 ミリ秒です。このフィールドに値を入力すると、[最小（min）] および [最大（max）] フィールドが有効になります。 • [最小（min）]：同じ LSA を発信するための最小遅延。有効値の範囲は、1 ～ 600000 ミリ秒です。 • [最大（max）]：同じ LSA を発信するための最大遅延。有効値の範囲は、1 ～ 600000 ミリ秒です。 • [SPFスロットル（SPF Throttle）]：SPF 計算への変更を受信する遅延。有効値の範囲は、1～600000 ミリ秒です。このフィールドに値を入力すると、[最小（min）] および [最大（max）] フィールドが有効になります。 • [最小（min）]：1 番目と 2 番目の SPF 計算間の遅延。有効値の範囲は、1 ～ 600000 ミリ秒です。 • [最大（max）]：SPF 計算の最大待機時間。有効値の範囲は、1～600000 ミリ秒です。 （注） LSA スロットリングでは、最小時間または最大時間が最初のオカレンスの値よりも小さい場合、OSPFv3 が自動的に最初のオカレンス値に修正します。同様に、指定された最遅延が最小

要素	説明
	遅延よりも小さい場合、OSPFv3 が自動的に最小遅延値に修正します。
デフォルトの情報発信元	OSPFv3 ルーティングドメインへのデフォルトの外部ルートを生成するために ASBR によって使用される設定。 • [デフォルトの情報発信元の有効化（Enable Default Information Originate）]：OSPFv3 ルーティングドメインへのデフォルトルートの生成を有効にするには、このチェックボックスをオンにします。次のオプションが使用可能になります。 • [Always advertise the default route]：デフォルト ルートを常にアドバタイズするには、このチェックボックスをオンにします。 • [メトリック値（Metric Value）]：デフォルトルートの生成に使用する OSPFv3 メトリック。有効値の範囲は 0 ～ 16777214 です。 • [メトリックタイプ（Metric Type）]：OSPFv3 ルーティングドメインにアドバタイズされるデフォルトルートに関連付けられた外部リンクタイプ。タイプ 1 外部ルートまたはタイプ 2 外部ルートを示す [1] か [2] を選択します。デフォルト値は 1 です。 • [ルートマップ（Route Map）]：（任意）適用するルートマップオブジェクトの名前を入力または選択します。ルートマップが一致すると、ルーティング プロセスによってデフォルト ルートが生成されます。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。
パッシブ インターフェイス	パッシブルーティングは、OSPFv3 ルーティング情報のアドバタイズメントの制御に有効であり、インターフェイスでの OSPFv3 ルーティング更新の送受信を無効にします。 1 つ以上のインターフェイスまたはインターフェイス オブジェクトを入力または選択して、それらのインターフェイスでパッシブ OSPFv3 ルーティングを有効にします。IPv4 および IPv6 アドレスがサポートされます。
[Non Stop Forwarding] タブ （注） Non Stop Forwarding（NSF）は、ASA 9.3(1)+ でのみサポートされています。	

要素	説明
グレースフル リスタート ヘルパーの有効化	グレースフル リスタート ヘルパー モードを有効にします。 ASA で NSF が有効になっている場合、ASA は NSF 対応であると見なされ、グレースフル リスタート モードで動作します。デフォルトでは、NSF 対応 ASA に隣接する ASA は NSF 認識となり、NSF ヘルパー モードで動作します。NSF 対応 ASA がグレースフル リスタートを実行しているときは、ヘルパーの ASA はそのノンストップ フォワーディングの復帰プロセスを支援します。 再起動するネイバーのノンストップ フォワーディングの復帰を ASA が支援しないようにする場合は、グレースフル リスタート ヘルパーの有効化オプションをクリアします。
リンク ステート アドバタイズメントの有効化	リンク ステート アドバタイズメント（LSA）の厳密なチェックを有効にします。 （注） イネーブルにすると、再起動ルータにフラッディングされる可能性がある LSA への変更があることが検出された場合、またはグレースフル リスタート プロセスが開始されたときに再起動ルータの再送リスト内に変更された LSA があると検出された場合、ヘルパー ルータはルータの再起動プロセスを終了させることを示します。
グレースフルリスタートの有効化（スパンドクラスタまたはフェールオーバーが設定されている場合に使用）	ASA でグレースフルリスタートを有効にします。
グレースフルリスタート間隔の長さ	（オプション）グレースフル リスタートの間隔を秒数で指定します。有効な範囲は 1 ～ 1800 です。デフォルトは 120 です。 （注） 30 秒未満の再起動間隔では、グレースフル リスタートが中断します。

[エリア（Area）] タブ（OSPFv3）

[OSPFv3] ページの [プロセス（Process）] タブ （173 ページ）の [エリア（Area）] パネルを使用して、OSPFv3 エリア、範囲、および仮想リンクを設定します。[エリア（Area）] は、[エリア（Area）]、[範囲（Range）]、および [仮想リンク（Virtual Link）] の 3 つの定義テーブルで構成されています。

- [エリア（Area）] テーブルエントリの追加と編集については、 Add/Edit Area Dialog Box（OSPFv3） （181 ページ）を参照してください。

- [範囲（Range）]テーブルエントリの追加と編集については、範囲の追加/編集ダイアログボックス（OSPFv3） （183 ページ）を参照してください。
- [仮想リンク（Virtual Link）]テーブルエントリの追加と編集については、 Add/Edit Virtual Link Dialog Box（OSPFv3） （184 ページ）を参照してください。

Security Manager テーブルの操作に関する基本情報については、テーブルの使用を参照してください。

ナビゲーション パス

[エリア（Area）] タブには、[OSPFv3] ページの [プロセス（Process）] タブ （173 ページ）からアクセスできます。[OSPFv3] ページの詳細については、 OSPFv3 の設定 （170 ページ）を参照してください。

関連項目

- OSPFv3 について （171 ページ）
- [OSPFv3インターフェイス（OSPFv3 Interface）] タブ （189 ページ）

Add/Edit Area Dialog Box（OSPFv3）

[エリアの追加/編集（Add/Edit Area）]ダイアログボックスを使用して、エリアのパラメータを定義します。

ナビゲーション パス

[エリアの追加（Add Area）]/[エリアの編集（Edit Area）] ダイアログボックスには、[エリア（Area）] タブ（OSPFv3） （180 ページ）からアクセスできます。

関連項目

- OSPFv3 の設定 （170 ページ）
- OSPFv3 について （171 ページ）
- [プロセス（Process）] タブ （173 ページ）

フィールド リファレンス

表 *91 : [*エリアの追加/編集（*Add/Edit Area***）*]* ダイアログボックス**

要素	説明
エリア ID（Area ID）	10 進数または IP アドレスのいずれかを使用して、エリアの ID を入力します。有効な 10 進値の範囲は、0 ～ 4294967295 です。

要素	説明
コスト（Cost）	インターフェイス上でパケットを送信するコスト。有効値は、0 ～ 65535 です。 ルーティングはコスト、つまり特定のインターフェイスを介してパケットを送信するために必要なオーバーヘッドに基づいて決定されます。ASA は、インターフェイスのコストをリンク帯域幅に基づいて計算し、宛先までのホップ数は使用しません。コストを設定して優先パスを指定することができます。
タイプ（Type）	次のいずれかを選択して、エリアタイプを定義します。 • [通常（Normal）]：このエリアは標準の OSPF エリアとなります。エリアを最初に作成するときは、このオプションがデフォルトで選択されています。 • [NSSA]：このエリアは「Not-So-Stubby Area」となります。NSSA は、タイプ 7 LSA を受け入れます。このオプションを選択すると、デフォルトの情報発信オプションが有効になります。 NSSA を作成するときに、[このエリアへのサマリーLSAの送信を許可する（Allow Sending summary LSA into this area）] チェックボックスをオフにすると、サマリー LSA がそのエリアにフラッドされるのを防ぐことができます。また、[再配布（Redistribute）] の選択を解除し、[デフォルトの情報送信元（Default Information Originate）] をイネーブルにすることによって、ルート再配布をディセーブルにすることができます。 • [スタブ（Stub）]：このエリアはスタブエリアとなります。スタブ エリアには、その向こう側にルータまたはエリアはありません。スタブ エリアは、AS External LSA（タイプ 5 LSA）がスタブ エリアにフラッドされないようにします。このオプションを選択すると、[このエリアへのサマリーLSAの送信を許可する（Allow Sending summary LSA into this area）] が有効になります。 スタブエリアを作成するときに、[このエリアへのサマリーLSAの送信を許可する（Allow Sending summary LSA into this area）] チェックボックスをオフにすると、サマリー LSA がそのエリアにフラッドされるのを防ぐことができます。
デフォルトの情報発信元（Default Information Originate） これらのオプションは、エリアタイプとして NSSA を選択すると有効になります。最初のオプションは、エリアタイプとして [Stub] を選択すると有効になります。	

要素	説明
このエリアへのサマリー LSA の送信を許可する（Allow sending summary LSA into this area）	エリアへのサマリー LSA のフラッディングを許可する場合に選択します。
Redistribute (imports routes to normal and NSSA areas)	ルートの再配布を許可する場合に選択します。
Default information originate	タイプ 7 デフォルトを NSSA 内に生成するには、このチェックボックスをオンにします。このオプションを選択すると、次のメトリックオプションが有効になります。 • [メトリック（Metric）]：デフォルトルートの OSPF メトリック値。有効値の範囲は 1 ～ 16777214 です。デフォルトは 1 です。 • [メトリックタイプ（Metric Type）]：デフォルトルートの OSPF メトリックタイプ。1（タイプ 1）または 2（タイプ 2）を選択します。デフォルトは 1 です。

範囲の追加/編集ダイアログボックス（OSPFv3）

[エリア範囲ネットワークの追加（Add Area Range Network）]/[エリア範囲ネットワークの編集（Edit Area Range Network）] ダイアログボックスを使用して、エリアテーブルで選択されたエリアに新しい範囲を追加するか、既存のエントリを変更します。

ナビゲーション パス

[範囲の追加（Add Range）]/[範囲の編集（Edit Range）] ダイアログボックスには、[エリア（Area）] タブ（OSPFv3） （180 ページ）の [範囲（Range）] パネルからアクセスできます。

関連項目

- OSPFv3 の設定 （170 ページ）
- OSPFv3 について （171 ページ）
- [プロセス（Process）] タブ （173 ページ）

フィールド リファレンス

表 *92 : [*範囲の追加（*Add Range*）*]/[*範囲の編集（*Edit Range*）*]* ダイアログボックス

要素	説明
エリア ID（Area ID）	この読み取り専用エントリは、この範囲が適用されるエリアの ID です。
IPv6 Prefix/Length	集約されるルートの IPv6 アドレス。 **ヒント** [選択（Select）] をクリックすると、ネットワークオブジェクトのリストからネットワークを選択できます。
コスト（Cost）	集約ルートのコスト。宛先への最短パスを決定するための OSPF SPF 計算で使用します。有効値の範囲は 0 ～ 16777215 です。 ルーティングはコスト、つまり特定のインターフェイスを介してパケットを送信するために必要なオーバーヘッドに基づいて決定されます。ASA は、インターフェイスのコストをリンク帯域幅に基づいて計算し、宛先までのホップ数は使用しません。コストを設定して優先パスを指定することができます。
[アドバタイズ（Advertise）]	アドレス範囲ステータスを「アドバタイズ」に設定するには、このオプションを選択します。これにより、タイプ 3 集約 LSA が生成されます（これがデフォルトです）。指定したネットワークのタイプ 3 集約 LSA を抑止するには、このオプションを選択解除します。

Add/Edit Virtual Link Dialog Box（OSPFv3）

[仮想リンクの追加（Add Virtual Link）]/[仮想リンクの編集（Edit Virtual Link）] ダイアログボックスを使用して、エリアテーブルで選択されたエリアの仮想リンクを定義するか、既存の仮想リンクのプロパティを変更します。

ナビゲーション パス

[仮想リンクの追加（Add Virtual Link）]/[仮想リンクの編集（Edit Virtual Link）] ダイアログボックスには、[エリア（Area）] タブ（OSPFv3） （180 ページ）の下の [仮想リンク（Virtual Link）] パネルからアクセスできます。

関連項目

- OSPFv3 の設定 （170 ページ）
- OSPFv3 について （171 ページ）
- [プロセス（Process）] タブ （173 ページ）

フィールド リファレンス

表 *93 : [*仮想リンクの追加（*Add Virtual Link*）*][*仮想リンクの編集（*Edit Virtual Link*）*]* ダイアログ ボックス

要素	説明
エリア ID（Area ID）	この読み取り専用エントリは、この仮想リンクが適用されるエリアの ID です。
ピア ルータ ID（Peer Router ID）	仮想リンク ネイバーの IP アドレスを入力します。 **ヒント** [選択（Select）] をクリックすると、ネットワークオブジェクトのリストからネットワークを選択できます。
TTL セキュリティ	仮想リンク上の存続可能時間（TTL）セキュリティホップ数。ホップ数の値は 1 ～ 254 の範囲で指定します。
dead 間隔（Dead Interval）	hello パケットが受信されない場合、ネイバーがデバイスダウンを宣言するまでの時間間隔（秒）。有効値の範囲は1～8192です。このフィールドのデフォルト値は、hello 間隔の 4 倍です。
Hello 間隔（Hello Interval）	インターフェイス上で送信されるhelloパケット間の間隔（秒数）。hello 間隔を小さくすると、トポロジ変更はより高速に検出されますが、インターフェイス上で送信されるトラフィックはより多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバーで同じである必要があります。有効な値の範囲は、1 ～ 8192 秒です。デフォルト値は 10 秒です。
送信間隔	インターフェイスに属する隣接関係へのLSA再送信間の時間（秒数）。デバイスが自身のネイバーに LSA を送信する場合、デバイスは確認応答メッセージを受信するまでその LSA を保持します。デバイスは、確認応答メッセージを受信しないと、LSAを再び送信します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。有効な値の範囲は、1～8192秒です。デフォルト値は 5 秒です。
送信遅延（Transmit Delay）	インターフェイス上で LSA パケットを送信するために必要と推定される時間（秒数）。更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSAがリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。有効な値の範囲は、1 ～ 8192 秒です。デフォルト値は 1 秒です。

Add/Edit Redistribution Dialog Box（OSPFv3）

[再配布の追加（Add Redistribution）]/[再配布の編集（Edit Redistribution）] ダイアログボックスを使用して、このプロセスに再配布ルールを追加するか、または既存の再配布ルールを編集します。

ナビゲーション パス

[プロセス（Process）] タブ （173 ページ）の下の [再配布（Redistribution）] パネルから、[再配布（Redistribution）] ダイアログボックスにアクセスできます。

関連項目

- OSPFv3 の設定 （170 ページ）
- OSPFv3 について （171 ページ）

フィールド リファレンス

表 94 : [Add Redistribution]/[Edit Redistribution] ダイアログボックス

要素	説明
ソース プロトコル	ルート再配布の送信元プロトコルを選択します。 • [接続済み（Connected）]：接続済みルート（インターフェイス上で IP アドレスを有効にすることによって自動的に確立されるルート）を OSPFv3 ルーティングプロセスに再配布します。接続済みルートは、自律システムの外部として再配布されます。 • [OSPF]：別の OSPF ルーティングプロセスからのルートを再配布します。このオプションを選択すると、ルーティング PID と一致オプションが有効になります。 • [スタティック（Static）]：スタティックルートを OSPFv3 ルーティングプロセスに再配布します。
メトリック （Metric）	再配布されるルートのメトリック値。有効値の範囲は 0 ～ 16777214 で、デフォルトは 20 です。 同じデバイス上で 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。
メトリック タイプ	メトリックタイプは、OSPFv3 ルーティングドメインにアドバタイズされるデフォルトルートに関連付けられた外部リンクタイプです。 なし、1、または 2 を選択します。なしはデフォルトルートがないことを示し、1 はメトリックがタイプ 1 外部ルートであることを示し、2 はタイプ 2 外部ルートであることを示します。

要素	説明
Tag（任意）	このタグは、各外部ルートに付加される 32 ビットの 10 進値です。これは OSPF 自体には使用されません。これは、他の境界デバイス間で情報を通信するために使用される場合があります。有効値の範囲は、0 ～ 4294967295 です。
ルート マップ	再配布エントリに適用するルートマップオブジェクトの名前を入力または選択します。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （214 ページ）を参照してください。
ルーティング PID	再配布の対象となるプロセスの ID。（プロセス ID は [プロセス（Process）] タブ （173 ページ）で定義されます。） このオプションは、OSPF が送信元プロトコルとして選択されているときにのみ有効になります。
接続済みを含める	接続済みルートを再配布に含めるには、このチェックボックスをオンにします。
一致 1 つのルーティング プロトコルから別のルーティング プロトコルへのルート再配布に使用される条件。ルートが再配布されるには、選択した条件と一致している必要があります。次の一致条件から 1 つ以上を選択できます。これらのオプションは、OSPF が送信元プロトコルとして選択されているときにのみ有効になります。	
内線	特定の自律システムへの内部ルート。
外部 1	自律システムの外部だが、OSPF にタイプ 1 外部ルートとしてインポートされるルート。
外部 2	自律システムの外部だが、OSPF にタイプ 2 外部ルートとしてインポートされるルート。
NSSA 外部 1	自律システムの外部だが、OSPF にタイプ 2 NSSA ルートとしてインポートされるルート。
NSSA 外部 2	自律システムの外部だが、OSPF にタイプ 2 NSSA ルートとしてインポートされるルート。

[サマリープレフィックスの追加/編集（Add/Edit Summary Prefix）] ダイアログボックス（OSPFv3）

[サマリープレフィックスの追加/編集（Add/Edit Summary Prefix）] ダイアログボックスを使用して、選択したプロセスに新しいルート要約エントリを追加するか、既存のエントリを変更します。

ナビゲーション パス

[サマリープレフィックスの追加/編集（Add/Edit Summary Prefix）] ダイアログボックスには、[プロセス（Process）] タブ （173 ページ）の下の [サマリープレフィックス（Summary Prefix）] パネルからアクセスできます。

関連項目

- OSPFv3 の設定 （170 ページ）
- OSPFv3 について （171 ページ）

フィールド リファレンス

表 *95 : [サマリープレフィックスの追加/編集（Add/Edit Summary Prefix）] ダイアログボックス*

要素	説明
プロセス ID（Process ID）	この読み取り専用の値は、このルールが適用されるプロセスを識別します。
IPv6 Prefix/Length	外部ルート集約の IPv6 プレフィックス/長さを入力します。 ヒント　[選択（Select）] をクリックすると、ネットワークオブジェクトのリストからネットワークを選択できます。
[アドバタイズ（Advertise）]	選択した場合、指定したプレフィックスとマスクのペアに一致する集約ルートはアドバタイズされません。選択解除すると、指定したプレフィックスとマスクのペアに一致するルートは抑制されません。デフォルトでは、このチェックボックスはオンです。
Tag（任意）	このタグは、各外部ルートに付加される 32 ビットの 10 進値です。これは OSPF 自体には使用されません。これは、境界デバイス間で情報を通信するために使用される場合があります。有効値の範囲は、0 ～ 4294967295 です。 このフィールドは、[アドバタイズ（Advertise）] をオンにすると有効になります。

[OSPFv3インターフェイス（OSPFv3 Interface）] タブ

[インターフェイス（Interface）] パネルを使用して、インターフェイスおよびネイバー固有のOSPFv3 ルーティングプロパティを設定します。[インターフェイス（Interface）] パネルは、[インターフェイス（Interface）] と [ネイバー（Neighbor）] の 2 つの定義テーブルで構成されています。

- [インターフェイス（Interface）] テーブルエントリの追加と編集については、 [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（OSPFv3） （189 ページ）を参照してください。
- [ネイバー（Neighbor）] テーブルエントリの追加と編集については、 [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス（OSPFv3） （194 ページ）を参照してください。

Security Manager テーブルの操作に関する基本情報については、テーブルの使用を参照してください。

ナビゲーション パス

[OSPFv3] ページの [インターフェイス（Interface）] タブをクリックして、このパネルを表示します。[OSPFv3] ページの詳細については、 OSPFv3 の設定 （170 ページ）を参照してください。

関連項目

- OSPFv3 について （171 ページ）
- [プロセス（Process）] タブ （173 ページ）

[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（OSPFv3）

[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックスを使用して、個別のインターフェイスの OSPFv3 認証ルーティングプロパティを追加するか、既存のエントリを変更します。

ナビゲーション パス

[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックスには、[OSPFv3インターフェイス（OSPFv3 Interface）] タブ （189 ページ）の [インターフェイス（Interfaces）] パネルからアクセスできます。

関連項目

- OSPFv3 の設定 （170 ページ）
- OSPFv3 について （171 ページ）
- [プロセス（Process）] タブ （173 ページ）

フィールド リファレンス

表 *96 : [Add Interface]/[Edit Interface]* ダイアログボックス

要素	説明
インターフェイス（Interface）	このルーティング設定が適用されるインターフェイスの名前。 ヒント　[選択（Select）] をクリックして、インターフェイスオブジェクトのリストからインターフェイスを選択できます。
[このインターフェイスでOSPFv3を有効にする（Enable OSPFv3 on this interface）]	指定されたインターフェイスでOSPFv3を有効にし、次のフィールドをアクティブにするには、このボックスをオンにします。 • [プロセスID（Process ID）]：このインターフェイスに適用するプロセスを選択します。 OSPFv3 [プロセス（Process）] タブ（173 ページ）で定義されます。 • [エリアID（Area ID）]：割り当てられるエリアを識別します。エリアは OSPFv3 [プロセス（Process）] タブ （173 ページ）でも定義されます。 • [インスタンスID（Instance ID）]：（任意）このプロセスインスタンスの ID を指定します。この設定の有効値の範囲は 0 ～ 255 です。 この機能により、1 つのリンク上に複数の OSPFv3 プロセスを設定できます。他のインスタンス ID を指定された受信パケットは、このプロセスによって無視されます。
Properties	
[発信リンクステートアドバタイズメントのフィルタリング（Filter outgoing link-state advertisements）]	発信LSAをフィルタリングするには、このボックスをオンにします。デフォルトでは、すべての発信LSAがインターフェイスにフラッディングされます。
[MTU不一致検出の無効化（Disable MTU mismatch detection）]	データベース記述子（DBD）パケットが受信された場合のOSPF MTU不一致検出を無効にするには、このボックスをオンにします。
[フラッドリダクション（Flood Reduction）]	安定したトポロジで LSA の不要なフラッディングを抑止するには、このボックスをオンにします。

要素	説明
[ポイントツーポイントネットワーク（Point-to-point Network）]	インターフェイスをポイントツーポイントネットワーク（2つのルーティングデバイス間のネットワーク）へのリンクとして定義するには、このボックスをオンにします。ポイントツーポイントネットワーク上の全ネイバーが隣接関係を確立します。代表ルータは存在しません。 [ブロードキャスト（Broadcast）] オプションが選択されている場合、このオプションは使用できません。
ブロードキャスト	インターフェイスを複数のルーティングデバイスを含むネットワークへのリンクとして定義するには、このボックスをオンにします。このようなネットワークは、代表ルータ（DR）とバックアップ代表ルータ（BDR）を確立し、ネットワークでの LSA フラッディングを制御します。 [ポイントツーポイントネットワーク（Point-to-point Network）] オプションが選択されている場合、このオプションは使用できません。
コスト（Cost）	インターフェイスを介したパケット送信のコスト。リンクコストは、最短パスの最初の計算で使用される任意の数値です。値を割り当てない場合、設定された参照帯域幅をインターフェイスポート速度で割った値が使用されます（デフォルトの参照帯域幅は 40 Gb/秒 です）。
プライオリティ	このインターフェイスに OSPFv3 優先順位を割り当てます。この設定の有効値の範囲は 0 ～ 255 です。この設定に 0 を入力すると、適切でないルータが代表ルータまたはバックアップ代表ルータになります。この設定は、ポイントツーポイントの非ブロードキャスト インターフェイスとして設定されているインターフェイスには適用されません。 2 つのルータがネットワークに接続している場合、両方が代表ルータになろうとします。優先順位の高いデバイスが代表ルータになります。ルータ優先順位が同じ場合は、ルータ ID が高い方が指定ルータになります。
dead 間隔（Dead Interval）	デバイスがこの間隔内にネイバーから hello パケットを受信しなかった場合、そのデバイスは非アクティブに指定されます。有効値の範囲は 1 ～ 65535 です。この設定のデフォルト値は、hello 間隔の 4 倍です。
Poll Interval	ネイバーデバイスが非アクティブな場合、そのネイバーに hello パケットを送信し続けることが必要な場合があります。hello パケットは短縮された間隔で送信されます。この間隔の値は hello 間隔よりも大きな値にする必要があります。

要素	説明
再送信間隔（Retransmit Interval）	隣接ネイバーへのLSA再送信間の時間（秒単位）。ルータがネイバーに LSA を送信する場合、ルータは確認応答を受信するまでその LSA を保持します。この間隔の間に確認応答が受信されなかった場合、ルータは LSA を再送信します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。有効値の範囲は、1 ～ 65535 秒です。
送信遅延（Transmit Delay）	インターフェイス上で LSA パケットを送信するために必要と推定される時間（秒数）。更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。有効値の範囲は、1 ～ 65535 秒です。
認証	
タイプ（Type）	インターフェイス上で有効にする認証のタイプ。次のいずれかを実行します。 • [エリア（Area）]：OSPFv3 は「組み込み」認証を提供せず、代わりにIPv6/IPSecプロトコルに依存します。該当するプロトコルを使用して、エリア内のすべてのインターフェイスでOSPFv3 トラフィックを認証するには、このオプションを選択します。これは、エリア内のすべてのルーティングデバイスがこのオプションを使用する必要があることを意味します。これがデフォルトです。 • [インターフェイス（Interface）]：このインターフェイスを安全な状態に保ち、OSPFv3 仮想リンクを保護するには、このオプションを選択します。このオプションを選択すると、このセクションで追加パラメータが有効になります。 • [なし（None）]：OSPFv3 認証は無効になります。
[セキュリティパラメータインデックス（Security Parameter Index）]	特定の OSPFv3 インターフェイスを区別するために使用される IPSec 識別タグを入力します。指定された認証および暗号化ルールと組み合わせて使用されます。有効値の範囲は、256 ～ 4294967295 です。

要素	説明
認証アルゴリズム（Authentication Algorithm）	使用する認証アルゴリズムのタイプを選択します。 • [md5]：Message Digest 5。128 ビットのハッシュ値を生成します。 • [sha1]：Secure Hash Algorithm バージョン 1。160 ビットのハッシュ値を生成します。
認証キー（Authentication Key）	認証キーを入力します。入力するキーの長さは、認証アルゴリズムとして選択した認証のタイプと、キーを暗号化するかどうかによって異なります（[認証キーの暗号化（Encrypt Authentication Key）] ボックスをオンにすると暗号化されます）。 • md5：32 文字。 • md5（暗号化）：66 文字。 • sha1：40 文字。 • sha1（暗号化）：82 文字。
[認証キーの暗号化（Encrypt Authentication Key）]	送信時に指定した認証キーの暗号化を要求するには、このボックスをオンにします。
[暗号化を含める（Include Encryption）]	OSPFv3 パケットの暗号化を要求するには、このボックスをオンにします。次のオプションが有効になります。
暗号化アルゴリズム（Encryption Algorithm）	使用する暗号化のタイプを選択します。 • [3des]：トリプル DES。Data Encryption Standard の暗号アルゴリズムが各パケットに 3 回適用されます。 • [aes-cbc]：暗号化が暗号ブロックチェーンを使用した Advanced Encryption Standard に基づいており、[キータイプ（Key Type）] パラメータで選択されたサイズのキーを生成します。 [キータイプ（Key Type）] リストは、この暗号化オプションを選択した場合にのみ有効になります。次のオプションのいずれかを選択します。 • [128]：128 ビットキーの場合。 • [192]：192 ビットキーの場合。 • [256]：256 ビットキーの場合。 • [des]：Data Encryption Standard に基づく暗号化で、56 ビットのキーを使用します。

要素	説明
暗号化キー（Encryption Key）	暗号キーを入力します。入力するキーの長さは、暗号化アルゴリズムとして選択した暗号化のタイプと、キーを暗号化するかどうかによって異なります（[キーの暗号化（Encrypt Key）] ボックスをオンにすると暗号化されます）。 • 3des：48 文字（192 ビット）。 • 3des（暗号化）：98 文字（192 ビット）。 • aes-cbc/128：32 文字（128 ビット）。 • aes-cbc/128（暗号化）：66 文字（128 ビット）。 • aes-cbc/192：48 文字（192 ビット）。 • aes-cbc/192（暗号化）：98 文字（192 ビット）。 • aes-cbc/256：64 文字（256 ビット）。 • aes-cbc/256（暗号化）：130 文字（256 ビット）。 • des：16 文字（64 ビット）。 • des（暗号化）：34 文字（64 ビット）。
暗号化キー	送信時に指定した暗号化キーの暗号化を要求するには、このボックスをオンにします。

[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス（OSPFv3）

ポイントツーポイントの非ブロードキャストインターフェイスごとに、スタティック ネイバーを定義する必要があります。この機能により、OSPFv3 アドバタイズメントを GRE トンネルにカプセル化しなくても、既存の VPN 接続でブロードキャストすることができます。次の制約事項に注意してください。

- 異なる 2 つの OSPFv3 プロセスに対して同じスタティック ネイバーを定義できません。
- 各スタティックネイバーにスタティックルートを定義する必要があります

インターフェイステーブルで選択したインターフェイスのスタティックネイバーを定義するか、または既存のスタティックネイバーの情報を変更するには、[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックスを使用します。

ナビゲーション パス

[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックスには、[OSPFv3インターフェイス（OSPFv3 Interface）] タブ （189 ページ）からアクセスできます。

関連項目

- OSPFv3 の設定 （170 ページ）
- OSPFv3 について （171 ページ）
- [プロセス（Process）] タブ （173 ページ）

フィールド リファレンス

表 *97 : [*ネイバーの追加/編集（*Add/Edit Neighbor*）*]* ダイアログボックス

要素	説明
インターフェイス（Interface）	このネイバー定義に関連付けられたインターフェイス（読み取り専用）。
リンクローカルアドレス（Link-local Address）	スタティックネイバーの IPv6 アドレスを入力します。
コストおよびデータベースフィルタ（Cost and Database Filter）	同期およびフラッディング中にインターフェイス上の発信 LSA をフィルタリングを有効にするには、このボックスをオンにします。次のオプションを使用できます。 • [コスト（Cost）] : このフィールドを使用して、ネイバーに任意のコストを割り当てます。値が割り当てられていない場合、インターフェイスのコストが使用されます（この値はインターフェイスのポート速度に基づいており、基準帯域幅をインターフェイス速度で割って計算されます）。有効値の範囲は 1 ～ 65535 です。 • [発信リンクステートアドバタイズメントをフィルタ処理（Filter outgoing link-state advertisements）] : ネイバーへの発信 LSA の転送を無効にするには、このボックスをオンにします。 （注） [コストおよびデータベースフィルタ（Cost and Database Filter）] オプションと [ポーリング間隔（Poll-Interval）] オプションは相互に排他的です。

要素	説明
ポーリング間隔（Poll-Interval）	次のオプションを有効にするには、このボックスをオンにします。 • [ポーリング間隔（Poll Interval）]：「デッド」ネイバーへの hello パケットの送信間隔（秒単位）。デフォルトは 120 です。 ネイバーデバイスが非アクティブになった（hello パケットがルータの dead 間隔期間に受信されなかった）場合でも、低いレートでデッドネイバーに hello パケットを送信し続ける必要がある場合があります。そのため、この値は、インターフェイスの hello 間隔より大きい値にする必要があります。 • [優先順位（Priority）]：ネイバーのルータの優先順位値。デフォルトは 0、有効値の範囲は 1 ～ 255 です。 優先順位値は、OSPFv3 リンクの代表ルータを決定するのに役立ちます。値がゼロの場合、デバイスが代表ルータまたはバックアップ代表ルータになれないことを意味します。 （注） [ポーリング間隔（Poll-Interval）] オプションと [コストおよびデータベースフィルタ（Cost and Database Filter）] オプションは相互に排他的です。また、各オプションの値はポイントツーマルチポイント インターフェイスには適用されません。

RIP の設定

Routing Information Protocol（RIP）は動的ルーティングプロトコルです。より正確には、ディスタンスベクターに基づく内部ゲートウェイプロトコルです。RIP は、パス選択のメトリックとしてホップ カウントを使用します。インターフェイスで RIP がイネーブルになっている場合、インターフェイスは RIP ブロードキャスト パケットをネイバー デバイスと交換し、動的にルートを学習してアドバタイズします。これらの RIP パケットには、ゲートウェイが到達可能な宛先ネットワークに関する情報、およびこれらの宛先に到達するためにパケットが通過しなければならないゲートウェイの数が含まれています。

Cisco Security Manager では、RIP バージョン 1 と RIP バージョン 2 の両方がサポートされます。バージョン 1 では、ルーティング更新でサブネット マスクは送信されません。RIP バージョン 2 では、ルーティング更新でサブネット マスクが送信され、可変長サブネット マスクがサポートされます。また、RIP バージョン 2 では、ルーティング更新の交換時にネイバー認証がサポートされます。この認証によって、セキュリティ アプライアンスは信頼できるソースから信頼できるルーティング情報を受信します。

（注） OSPF プロセスを実行している場合は、RIP をイネーブルにすることはできません。

制限事項

RIP には、次の制限事項があります。

- Cisco Security Manager は、インターフェイス間で RIP 更新を渡すことはできません。
- RIP バージョン 1 では、可変長サブネット マスクがサポートされていません。
- RIP の最大ホップ カウントは 15 です。ホップ カウントが 15 を超えるルートは、到達不能と見なされます。
- RIP の収束は、他のルーティング プロトコルと比べて時間がかかります。

RIP バージョン 2 の注意事項

次の情報は、RIP バージョン 2 だけに適用されます。

- ネイバー認証を使用する場合、認証キーとキー ID は、RIP バージョン 2 更新をインターフェイスに提供するすべてのネイバー デバイスで同じである必要があります。
- RIP バージョン 2 では、セキュリティ アプライアンスは、マルチキャスト アドレス 224.0.0.9 を使用してデフォルトのルート更新を送受信します。パッシブ モードでは、そのアドレスでルート アップデートが受信されます。
- RIP バージョン 2 がインターフェイスで設定されている場合、マルチキャスト アドレス 224.0.0.9 がそのインターフェイス上に登録されます。RIP バージョン 2 構成がインターフェイスから削除されると、そのマルチキャスト アドレスは登録解除されます。

Security Manager を使用したセキュリティ アプライアンスでの RIP の設定

[RIP] ページを使用して、インターフェイスで Routing Information Protocol をイネーブルにします。RIP を設定するときに使用できる設定および機能は、設定しているデバイスのタイプおよび OS のバージョンによって異なります。

- OS バージョンが 7.2 よりも前の PIX ファイアウォールまたは ASA で、あるいは任意の FWSM で RIP を設定するには、PIX/ASA 6.3 - 7.1 および FWSM の [RIP] ページ （198 ページ）を参照してください。
- OS バージョン 7.2 以降を実行している PIX ファイアウォールまたは ASA で RIP を設定するには、PIX/ASA 7.2 以降の RIP ページ （200 ページ）を参照してください。

関連項目

- スタティック ルートの設定 （208 ページ）
- OSPF の設定 （129 ページ）
- [No Proxy ARP] の設定 （1 ページ）
- 「Configuring Routing Information Protocol」：『Cisco IOS IP Configuration Guide, Release 12.2』の章。RIP の詳細情報が記載されています。

PIX/ASA 6.3 - 7.1 および FWSM の [RIP] ページ

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

この [RIP] ページを使用して、任意の FWSM、および 7.2 よりも前のバージョンのオペレーティング システムを実行している PIX/ASA のインターフェイスで Routing Information Protocol（RIP）をイネーブルにします。

このページの [RIP] テーブルには、現在 RIP が定義されているすべてのインターフェイスが一覧表示されます。[Add RIP Configuration]/[Edit RIP Configuration] ダイアログボックスを使用して、これらのエントリを作成および維持します。詳細については、PIX/ASA 6.3 - 7.1 および FWSM の [RIP] ページ （198 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）]>[ルーティング（Routing）] > [RIP] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [RIP] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

共有 RIP ポリシーの作成時には、[Create a Policy] ダイアログボックスで次のバージョンを選択する必要があります。

- **PIX/ASA 6.3-7.1 and FWSM**
- **PIX/ASA 7.2 and Later**

共有 RIP ポリシーの割り当て時には、必ずそのデバイスに適した RIP ポリシーを割り当ててください。たとえば、PIX/ASA 7.2+ RIP ポリシーを FWSM に割り当てることはできません。

関連項目

- スタティック ルートの設定 （208 ページ）
- OSPF の設定 （129 ページ）
- [No Proxy ARP] の設定 （1 ページ）
- PIX/ASA 7.2 以降の RIP ページ （200 ページ）
- 標準のルール テーブルに関する内容：
  - ルール テーブルの使用
  - テーブル カラムおよびカラム見出しの機能

[Add RIP Configuration (PIX/ASA 6.3–7.1 and FWSM)]/[Edit RIP Configuration (PIX/ASA 6.3–7.1 and FWSM)] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

[Add RIP Configuration]/[Edit RIP Configuration] ダイアログボックスを使用して、RIP 設定をセキュリティ アプライアンスに追加するか、既存の RIP 設定を変更します。RIP 設定を追加することによって、指定したインターフェイスで RIP をイネーブルにします。タイトルを除き、2 つのダイアログボックスは同じです。

ナビゲーション パス

[Add RIP Configuration]/[Edit RIP Configuration] ダイアログボックスには、 PIX/ASA 6.3 - 7.1 および FWSM の [RIP] ページ （198 ページ）からアクセスできます。

フィールド リファレンス

表 *98 : [RIP*設定の追加（*PIX/ASA 6.3–7.1*および*FWSM*）（*Add RIP Configuration (PIX/ASA 6.3–7.1 and FWSM)*）*]/[RIP*設定の編集（*PIX/ASA 6.3–7.1*および*FWSM*）（*Edit RIP Configuration (PIX/ASA 6.3–7.1 and FWSM)*）*]* ダイアログボックス

要素	説明
インターフェイス（Interface）	RIP 設定のインターフェイスを入力または選択します。同じインターフェイスで異なる RIP 設定を設定することはできません。
[モード（Mode）]	RIP 更新に関するインターフェイスの動作を選択します。 • [デフォルトルートの送信（Send default routes）]：インターフェイスは RIP ルーティング更新だけを送信します。 • [ルートの受信（Receive routes）]：インターフェイスは RIP ルーティング ブロードキャストを受信し、その情報を使用してルーティング テーブルに読み込みますが、RIP ルーティング更新を送信しません。 • [デフォルトルートの送信とルートの受信（Send default routes and receive routes）]：インターフェイスは RIP ルーティング更新を送受信します。
バージョン	インターフェイスで有効にする RIP バージョンを選択します。 • [RIPバージョン1（RIP Version 1）]：インターフェイスで RIP バージョン 1 をイネーブルにします。 • [RIPバージョン2（RIP Version 2）]：インターフェイスで RIP バージョン 2 をイネーブルにします。RIP バージョン 2 を設定すると、マルチキャスト アドレス 224.0.0.9 がインターフェイス上に登録されます。

要素	説明
Version 2 Authentication	これらのオプションを使用すると、RIP バージョン 2 で使用される認証をイネーブルにし、そのタイプを選択できます。 • [認証の有効化（Enable Authentication）]：このオプションは、上記の [RIP バージョン2（RIP Version 2）] を選択した場合に使用できます。このチェックボックスをオンにすると、RIP ネイバー認証がイネーブルになり、次のオプションが使用可能になります。 • [タイプ（Type）]：認証に MD5 ハッシュアルゴリズムを使用する場合は [MD5] を選択し（推奨）、認証にクリアテキストを使用する場合は [クリア テキスト（Clear text）] を選択します。 • [キーID（Key ID）]：認証キーの識別番号。この番号は、セキュリティ アプライアンスに更新を送信し、セキュリティ アプライアンスから更新を受信する他のすべてのデバイスと共有される必要があります。有効値の範囲は、1 ～ 255 です。 • [キー（Key）]：認証に使用される共有キー。 このキーは、セキュリティ アプライアンスに更新を送信し、セキュリティ アプライアンスから更新を受信する他のすべてのデバイスと共有される必要があります。キーの文字数は最大 16 文字です。

PIX/ASA 7.2 以降の RIP ページ

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

この RIP ページを使用して、オペレーティングシステム 7.2 以降を実行している PIX および ASA デバイスで Routing Information Protocol（RIP）を有効にし、設定します。[RIP] ページは、次のタブ付きパネルで構成されています。

- [RIP] - [Setup] タブ （201 ページ）
- RIP の [再配布（Redistribution）] タブ （203 ページ）
- [RIP] - [Filtering] タブ （205 ページ）
- [RIP] - [Interface] タブ （207 ページ）

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）]>[ルーティング（Routing）] > [RIP] を選択します。

- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [RIP] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

共有 RIP ポリシーの作成時には、[Create a Policy] ダイアログボックスで次のバージョンを選択する必要があります。

- **PIX/ASA 6.3-7.1 and FWSM**
- **PIX/ASA 7.2 and Later**

共有 RIP ポリシーの割り当て時には、必ずそのデバイスに適した RIP ポリシーを割り当ててください。たとえば、PIX/ASA 7.2+ RIP ポリシーを FWSM に割り当てることはできません。

関連項目

- スタティック ルートの設定 （208 ページ）
- OSPF の設定 （129 ページ）
- [No Proxy ARP] の設定 （1 ページ）
- PIX/ASA 6.3 - 7.1 および FWSM の [RIP] ページ （198 ページ）

[RIP] - [Setup] タブ

[Setup] パネルを使用して、セキュリティ アプライアンスで RIP を定義し、グローバル RIP プロトコル パラメータを設定します。セキュリティアプライアンスでは、RIP プロセスを 1 つだけイネーブルにできます。

ナビゲーション パス

[Setup] タブには、 PIX/ASA 7.2 以降の RIP ページ （200 ページ）からアクセスできます。

関連項目

- RIP の [再配布（Redistribution）] タブ （203 ページ）
- [RIP] - [Filtering] タブ （205 ページ）
- [RIP] - [Interface] タブ （207 ページ）

フィールド リファレンス

表 *99 : [Setup]* タブ

要素	説明
ネットワーク	RIP ルーティングに対して 1 つ以上のネットワークを定義します。IP アドレスを入力するか、目的のネットワーク/ホスト オブジェクトを入力または選択します（ネットワーク/ホストオブジェクトについてを参照）。IP アドレスにはサブネット情報を含めないでください。セキュリティ アプライアンスの設定に追加できるネットワーク数に制限はありません。 RIP ルーティング更新は、指定したネットワークのインターフェイスだけを介して送受信されます。また、インターフェイスのネットワークを指定しない場合、インターフェイスは RIP 更新でアドバタイズされません。
パッシブ インターフェイス	このオプションを使用して、セキュリティ アプライアンスで受動インターフェイスを指定してから、アクティブ インターフェイスを指定します。デバイスは、そのルーティング テーブルを入力するための情報を使用して、パッシブ インターフェイスでの RIP ルートのブロードキャストをリッスンしますが、パッシブ インターフェイスでのルーティング更新はブロードキャストしません。パッシブとして指定されていないインターフェイスは、更新を送受信します。次のオプションのいずれかを選択します。 **1.** [なし（None）]：どのインターフェースもパッシブとして指定されません。 **2.** [すべてのインターフェース（All Interfaces）]：デバイス上のすべてのインターフェイスがパッシブとして指定されます。ただし、次の [除外されたインターフェース（Excluded Interfaces）] フィールドに入力したインターフェイスを除きます。 **3.** [指定されたインターフェース（Specified Interfaces）]：以下のインターフェイス フィールドで明示的に指定されたインターフェイスのみが、パッシブとして指定されます。

要素	説明
[Interfaces]/[Excluded Interfaces]	このフィールドを使用して、上記の [Passive Interface] リストからの選択に応じて、受動リストから除外するインターフェイス、または明示的に受動として指定するインターフェイスを指定します。 • [すべてのインターフェース（All Interfaces）] を選択した場合、このフィールドのラベルは [除外されたインターフェース（Excluded Interfaces）] になります。除外するインターフェイス（つまり、パッシブではなくアクティブにするインターフェイス）だけを入力または選択します。 • [Passive Interface] リストで [Specified Interfaces] を選択した場合、受動として指定するインターフェイスだけを入力または指定します。 （注） 同じインターフェイスに対して異なる RIP 設定を指定することはできません。
RIP Version	RIP 更新の送受信対象の RIP バージョンを選択します。 • Receive Version 1 and 2, Send Version 1 • Send and Receive Version 1 • Send and Receive Version 2
デフォルトルートの生成	選択すると、指定した [Route Map] に基づいて、配布のためのデフォルトルートが生成されます。
ルート マップ	デフォルト ルートの生成に使用するルート マップを指定します。 （注） このフィールドにはルートマップ名だけが含まれます。ルートマップは FlexConfig 内で作成および格納されます。詳細については、FlexConfig ポリシーとポリシー オブジェクトについてを参照してください。
Enable Auto-Summary	[RIP Version] として [Send and Receive Version 2] を選択した場合、このオプションが使用可能になります。オンにすると、自動ルート サマライズがイネーブルになります。切断されているサブネット間のルーティングを実行する必要がある場合は、自動サマライズを無効にします。自動サマライズを無効にすると、サブネットがアドバタイズされます。 （注） RIP バージョン 1 では、常に自動サマライズが使用されます。無効にすることはできません。

RIP の [再配布（Redistribution）] タブ

[Redistribution] パネルを使用して、再配布ルートを管理します。これらは、他のルーティング プロセスから RIP ルーティング プロセスに再配布されているルートです。詳細については、

[Add Redistribution]/[Edit Redistribution] ダイアログボックス （47 ページ）を参照してください。

ナビゲーション パス

[Redistribution] タブには、 PIX/ASA 7.2 以降の RIP ページ （200 ページ）からアクセスできます。

関連項目

- [RIP] - [Setup] タブ （201 ページ）
- [RIP] - [Filtering] タブ （205 ページ）
- [RIP] - [Interface] タブ （207 ページ）

[Add Redistribution]/[Edit Redistribution] ダイアログボックス

[Add Redistribution]/[Edit Redistribution] ダイアログボックスを使用して、 RIP の [再配布（Redistribution）] タブ （203 ページ）で再配布ルートを追加および編集します。これらは、他のルーティング プロセスから RIP ルーティング プロセスに再配布されているルートです。タイトルを除き、これら 2 つのダイアログボックスは同一です。

ナビゲーション パス

[Add Redistribution]/[Edit Redistribution] ダイアログボックスには、 PIX/ASA 7.2 以降の RIP ページ （200 ページ）の [Redistribution] タブからアクセスできます。

フィールド リファレンス

表 100 : [Add Redistribution]/[Edit Redistribution] ダイアログボックス

要素	説明
Protocol to Redistribute	RIP ルーティング プロセスに再配布するルーティング プロトコルを選択します。 • [Static]：スタティックルート。 • [Connected）]：直接接続されたネットワーク。 • [OSPF]：OSPF ルーティングプロセスによって検出されたルート。 [OSPF] を選択すると、OSPF の [Process ID]、および任意で [Match] 基準も入力する必要があります。
プロセス ID （Process ID）	OSPF プロトコルを選択した場合、プロセス ID を入力します。

要素	説明
一致（Match）	OSPF ルートを RIP ルーティング プロセスに再配布する場合、再配布する特定のタイプの OSPF ルートを選択できます。複数のタイプを選択するには、Ctrl を押しながらクリックします。 • [内部（Internal）]：自律システム（AS）の内部のルートが再配布されます。 • [外部 1（External 1）]：AS に対して外部のタイプ 1 ルートが再配布されます。 • [外部 2（External 2）]：AS に対して外部のタイプ 2 ルートが再配布されます。 • [NSSA 外部 1（NSSA External 1）]：Not-So-Stubby Area（NSSA）の外部のタイプ 1 ルートが再配布されます。 • [NSSA External 2]：NSSA の外部のタイプ 2 ルートが再配布されます。 [Match] 基準は任意です。デフォルトの一致は、[Internal]、[External 1]、および [External 2] です。
メトリック（Metric）	再配布されるルートに適用される RIP メトリック タイプ。選択肢は次の 2 つです。 • [トランスペアレント（Transparent）]：現在のルートメトリックを使用します。 • [指定値（Specified Value）]：特定のメトリック値を割り当てます。
ルート マップ	ルートが RIP ルーティングプロセスに再配布される前に満たす必要があるルートマップの名前。 （注） このフィールドにはルート マップ名だけが含まれます。ルートマップの内容は、FlexConfig 内で作成および格納されます。詳細については、FlexConfig ポリシーとポリシー オブジェクトについてを参照してください。

[RIP] - [Filtering] タブ

[Filtering] パネルを使用して、RIP ポリシーのフィルタを管理します。フィルタは、着信および発信 RIP アドバタイズメントでネットワーク情報を制限するために使用されます。詳細については、[Add Filter]/[Edit Filter] ダイアログボックス （206 ページ）を参照してください。

ナビゲーション パス

[Filtering] タブには、PIX/ASA 7.2 以降の RIP ページ （200 ページ）からアクセスできます。

関連項目

- [RIP] - [Setup] タブ （201 ページ）
- RIP の [再配布（Redistribution）] タブ （203 ページ）
- [RIP] - [Interface] タブ （207 ページ）

[Add Filter]/[Edit Filter] ダイアログボックス

[Add Filter]/[Edit Filter] ダイアログボックスを使用して、[RIP] - [Filtering] タブ （205 ページ）で RIP フィルタを追加および編集します。フィルタは、着信および発信 RIP アドバタイズメントでネットワーク情報を制限するために使用されます。タイトルを除き、これら 2 つのダイアログボックスは同一です。

ナビゲーション パス

[Add Filter]/[Edit Filter] ダイアログボックスには、PIX/ASA 7.2 以降の RIP ページ （200 ページ）の [Filtering] タブからアクセスできます。

フィールド リファレンス

表 *101 : [Add Filter]/[Edit Filter]* ダイアログボックス

要素	説明
トラフィックの方向	フィルタリングするトラフィックのタイプを、[インバウンド（Inbound）] または [アウトバウンド（Outbound）] から選択します。 （注） [Traffic Direction] が [Inbound] の場合、インターフェイス フィルタだけを定義できます。
フィルタリングする	フィルタが [インターフェイス（Interface）] または [ルート（Route）] のどちらに基づいているかを指定します。 [インターフェイス（Interface）] を選択した場合、ルーティング更新がフィルタリングされるインターフェイスの名前を入力または選択します。 [ルート（Route）] を選択した場合、ルート タイプを選択します。 • [スタティック（Static）]：スタティックルートだけがフィルタリングされます。 • [接続済み（Connected）]：接続されたルートだけがフィルタリングされます。 • [OSPF]：指定した OSPF プロセスによって検出された OSPF ルートだけがフィルタリングされます。フィルタリングされる OSPF プロセスの [プロセス ID（Process ID）] を入力します。

要素	説明
Filter ACLs	許可されるネットワークまたは RIP ルート アドバタイズメントから削除されるネットワークを定義する 1 つ以上のアクセス コントロール リスト（ACL）の名前を入力または選択します。

[RIP] - [Interface] タブ

[Interface] パネルを使用して、RIP ブロードキャストを送受信するように設定されたインターフェイスを管理します。詳細については、 [Add Interface]/[Edit Interface] ダイアログボックス（207 ページ）を参照してください。

ナビゲーション パス

[Interface] タブには、 PIX/ASA 7.2 以降の RIP ページ （200 ページ）からアクセスできます。

関連項目

- [RIP] - [Setup] タブ （201 ページ）
- RIP の [再配布（Redistribution）] タブ （203 ページ）
- [RIP] - [Filtering] タブ （205 ページ）

[Add Interface]/[Edit Interface] ダイアログボックス

[Add Interface]/[Edit Interface] ダイアログボックスを使用して、 [RIP] - [Interface] タブ （207 ページ）で RIP インターフェイス設定を追加および編集します。タイトルを除き、これら 2 つのダイアログボックスは同一です。

ナビゲーション パス

[Add Interface]/[Edit Interface] ダイアログボックスには、 PIX/ASA 7.2 以降の RIP ページ （200 ページ）の [Interface] タブからアクセスできます。

フィールド リファレンス

表 102 : [Add Interface]/[Edit Interface] ダイアログボックス

要素	説明
インターフェイス（Interface）	このアプライアンスで定義されるインターフェイスを入力または選択します。
Send (Version)	これらのオプションを使用して、このインターフェイスについて、[RIP] - [Setup] タブ （201 ページ）で指定したグローバルな送信バージョンを上書きできます。該当するボックスを選択して、RIP バージョン 1、バージョン 2、または両方を使用して更新を送信するように指定します。

要素	説明
Receive (Version)	これらのオプションを使用して、グローバルな受信バージョンを上書きできます。該当するボックスを選択して、RIP バージョン 1 だけ、バージョン 2 だけ、または両方を使用して更新を受信するように指定します。
認証タイプ（Authentication Type）	RIPブロードキャストに対してこのインターフェイスで使用される認証を選択します。 • [なし（None）]：認証されません。 • [MD5]：MD5 を使用します。 • [クリアテキスト（Clear Text）]：クリアテキスト認証を使用します。 [MD5] または [Clear Text] を選択した場合、次の認証パラメータも指定する必要があります。 • [キー ID（Key ID）]：認証キーの ID。有効な値は 0 ～ 255 です。 • [キー（Key）]：選択した認証方式で使用されるキー。最大 16 文字です。 • [確認（Confirm）]：確認のために、認証キーを再度入力します。

スタティック ルートの設定

スタティック ルートは、現在のデバイスで手動で定義されている特定の宛先ネットワークへの特定のパスです。スタティック ルートは、さまざまな状況で使用されます。宛先へのダイナミック ルートがない場合、またはダイナミック ルーティング プロトコルの使用が不可能な場合に、1 つのネットワークから別のネットワークにデータをルーティングする迅速で効果的な方法です。

すべてのルートに、その使用プライオリティを示す値または「メトリック」があります。（このメトリックは「アドミニストレーティブディスタンス」とも呼ばれます）同じ接続先に対して 2 つ以上のルートが使用可能な場合、デバイスはアドミニストレーティブ ディスタンスを使って使用するルートを決定します。

スタティック ルートのデフォルトのメトリック値は 1 であり、ダイナミック ルーティング プロトコルによるルートよりも優先されます。ダイナミック ルートのメトリックよりも大きい値にメトリックを増やすと、スタティック ルートは、ダイナミック ルートに障害が発生した際のバックアップとして動作します。たとえば、Open Shortest Path First（OSPF）から取得されたルートには、100 というデフォルトのアドミニストレーティブディスタンスがあります。OSPF ルートが優先されるバックアップ スタティック ルートを設定するには、スタティック ルートに 100 よりも大きいメトリック値を指定します。これは、「フローティング」スタティック ルートと呼ばれます。

デフォルト ルートと呼ばれる特別な種類のスタティック ルートがあります。宛先アドレスとサブネット マスクの両方にすべて 0 が使用されるため、「0 - 0」ルートとも呼ばれます。デフォルトのスタティック ルートは、catch-all ゲートウェイとして機能します。デバイスのルーティング テーブルで特定の宛先について一致がない場合は、デフォルト ルートが使用されます。一般に、デフォルト ルートにはネクストホップ IP アドレスまたはローカル出口インターフェイスが含まれます。

[Static Route] ページを使用して、手動で定義したスタティック ルートを維持します。このページの [Static Route] テーブルには、現在定義されているすべてのスタティック ルートが一覧表示され、ルートごとに、ルートが定義されているインターフェイスまたはインターフェイス ロールの名前、宛先ネットワーク、ネクスト ホップ ゲートウェイ、ルート メトリック、ルートがトンネリングされるかどうか、ルートのサービス レベル契約トラッキングがあるかどうかが表示されます。これらのフィールドの詳細については、[Add Static Route]/[Edit Static Route] ダイアログボックス （210 ページ）または [IPv6 スタティック ルートの追加/編集（Add/Edit IPv6 Static Route）] ダイアログボックス （212 ページ）を参照してください。

スタティック null0 ルートの設定

通常、トラフィックのフィルタリングには ACL が使用され、ヘッダーに含まれている情報に基づくパケットのフィルタが可能になります。パケット フィルタリングでは、ASA ファイアウォールがパケット ヘッダーを検査してフィルタリングを決定するため、パケット処理のオーバーヘッドが加わり、パフォーマンスに影響します。

スタティック null0 ルーティングは、フィルタリングを補完するソリューションです。スタティック null0 ルートは、不要なトラフィックや望ましくないトラフィックをブラック ホールに転送するために使用されます。ヌル インターフェイスである null0 が、ブラック ホールの作成に使用されます。望ましくない宛先用のスタティック ルートが作成され、そのスタティック ルート コンフィギュレーションで null インターフェイスを指すように設定されます。宛先アドレスに最も一致するルートがブラック ホールのスタティック ルートであるすべてのトラフィックが自動的にドロップされます。ACL の場合とは異なり、スタティック null0 ルートはまったくパフォーマンスを低下させません。

スタティック null0 ルート設定は、ルーティング ループの防止に使用されます。BGP では、Remotely Triggered Black Hole ルーティングのためにスタティック null0 設定を活用します。

ナビゲーション パス

- （デバイス ビュー）デバイス ポリシー セレクタから、[プラットフォーム（Platform）] > [ルーティング（Routing）] > [スタティック ルート（Static Route）] または [プラットフォーム（Platform）] > [ルーティング（Routing）] > [IPv6 スタティック ルート（IPv6 Static Route）] を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから、[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [スタティック ルート（Static Route）] または [PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [IPv6 スタティック ルート（IPv6 Static Route）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- [Add Static Route]/[Edit Static Route] ダイアログボックス （210 ページ）
- [IPv6スタティックルートの追加/編集（Add/Edit IPv6 Static Route）] ダイアログボックス（212 ページ）
- 接続を維持するためのサービス レベル契約（SLA）のモニタリング
- 標準のルール テーブルに関する内容：
  - ルール テーブルの使用
  - テーブル カラムおよびカラム見出しの機能

[Add Static Route]/[Edit Static Route] ダイアログボックス

[Add Static Route]/[Edit Static Route] ダイアログボックスを使用すると、スタティック ルートを追加または編集できます。

ナビゲーション パス

[Add Static Route]/[Edit Static Route] ダイアログボックスには、[Static Routes] ページからアクセスできます。新しいスタティック ルートを追加するには、[Add Row] ボタンをクリックします。既存のスタティック ルートを編集するには、そのルートを選択して [Edit Row] ボタンをクリックします。

関連項目

- スタティック ルートの設定 （208 ページ）

フィールド リファレンス

表 103 : [Add Static Route]/[Edit Static Route] ダイアログボックス

要素	説明
インターフェイス（Interface）	このスタティック ルートが適用されるインターフェイスを入力または選択します。 トラフィックを Null0 インターフェイスへ送信すると、指定したネットワーク宛のパケットはドロップします。この機能は、BGP の Remotely Triggered Black Hole (RTBH) の設定に役立ちます。詳細については、 スタティック ルートの設定 （208 ページ）を参照してください。 （注） インターフェイスとして Null0 が選択されている場合、[ゲートウェイ（Gateway）] と [トンネル化（Tunneled）] のオプションはディセーブルになります。

要素	説明
ネットワーク（Network）	宛先ネットワークを入力または選択します。1 つ以上の IP アドレス/ネットマスク エントリ、1 つ以上のネットワーク/ホスト オブジェクト、または両方の組み合わせを指定できます。エントリはカンマで区切ります。 デフォルトルートを指定するには、「0.0.0.0/0」または「any」を入力します。
ゲートウェイ	このルートのネクスト ホップであるゲートウェイ ルータを入力または選択します。IP アドレスまたはネットワーク/ホスト オブジェクトを指定できます。 （注） セキュリティアプライアンスのインターフェイスのいずれかの IP アドレスがゲートウェイ IP アドレスとして使用される場合、セキュリティアプライアンスはゲートウェイ IP アドレスを解決する代わりに、パケット内の指定された IP アドレスを解決します。
メトリック（Metric）	メトリックは、特定のホストが存在するネットワークへのホップ数（ホップカウント）に基づくルートの「コスト」を示す測定値です。ホップ カウントは、ネットワーク パケットが最終的な宛先に到達するまでに通過する必要があるネットワークの数であり、宛先ネットワークも含まれます。ホップカウントには宛先ネットワークも含まれるため、直接接続されたすべてのネットワークのメトリックは 1 です。 宛先ネットワークへのホップ数を入力します。有効値の範囲は 1 ～ 255 で、デフォルト値は 1 です。 インスタンスごとに定義できる、コストが等しい（メトリックが等しい）ルートの最大数は、3 です。同じネットワーク上にある異なるインターフェイスで、同じメトリックのルートを追加することはできません。
Tunneled	これをトンネル ルートにするには、このオプションを選択します。デフォルト ルートだけに使用できます。設定できるデフォルトのトンネル ゲートウェイは、デバイスごとに 1 つのみです。[Tunneled] オプションは、トランスペアレント モードではサポートされません。PIX/ASA 7.0+ デバイスだけで使用できます。
Route Tracking	ルートの可用性をモニタするには、モニタリング ポリシーを定義する Service Level Agreement（SLA; サービス レベル契約）オブジェクトの名前を入力または選択します。PIX/ASA 7.2+ デバイスだけで使用できます。 ルート トラッキングの詳細については、接続を維持するためのサービス レベル契約（SLA）のモニタリングを参照してください。

[IPv6スタティックルートの追加/編集（Add/Edit IPv6 Static Route）] ダイアログボックス

[IPv6スタティックルートの追加/編集（Add/Edit IPv6 Static Route）] ダイアログボックスを使用すると、IPv6 スタティックルートを追加または編集できます。IPv6 スタティックルートは、次のデバイスでのみサポートされています。

- ASA 7.0 以降（ルーテッドモード）
- ASA 8.2 以降（トランスペアレントモード）
- FWSM 3.1 以降（ルーテッドモード）

ナビゲーション パス

[IPv6スタティックルートの追加/編集（Add/Edit IPv6 Static Route）] ダイアログボックスには、[IPv6スタティックルート（IPv6 Static Route）] ページからアクセスできます。新しいスタティックルートを追加するには、[行の追加（Add Row）] ボタンをクリックします。既存のスタティックルートを編集するには、そのルートを選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- スタティック ルートの設定 （208 ページ）

フィールド リファレンス

表 *104 : [IPv6スタティックルートの追加/編集（Add/Edit IPv6 Static Route）] ダイアログボックス*

要素	説明
インターフェイス（Interface）	このスタティックルートが適用されるインターフェイスを入力または選択します。
IPv6ネットワーク（IPv6 Network）	宛先ネットワークを入力または選択します。1 つ以上の IP アドレスエントリ、1 つ以上のネットワーク/ホストオブジェクト、または両方の組み合わせを指定できます。エントリはカンマで区切ります。 2 つのコロン（::）を入力してデフォルトルートを指定します。

要素	説明
IPv6ゲートウェイ（IPv6 Gateway）	このルートのネクストホップであるゲートウェイ ルータを入力または選択します。IP アドレスまたはネットワーク/ホスト オブジェクトを指定できます。 （注） セキュリティアプライアンスのインターフェイスのいずれかの IP アドレスがゲートウェイ IP アドレスとして使用される場合、セキュリティアプライアンスはゲートウェイ IP アドレスを解決する代わりに、パケット内の指定された IP アドレスを解決します。
メトリック（Metric）	メトリックは、特定のホストが存在するネットワークへのホップ数（ホップカウント）に基づくルートの「コスト」を示す測定値です。ホップカウントは、ネットワーク パケットが最終的な宛先に到達するまでに通過する必要があるネットワークの数であり、宛先ネットワークも含まれます。ホップ カウントには宛先ネットワークも含まれるため、直接接続されたすべてのネットワークのメトリックは 1 です。 宛先ネットワークへのホップ数を入力します。有効値の範囲は 1 ～ 255 で、デフォルト値は 1 です。 インスタンスごとに定義できる、コストが等しい（メトリックが等しい）ルートの最大数は、3 です。同じネットワーク上にある異なるインターフェイスで、同じメトリックのルートを追加することはできません。
Tunneled	ルートを VPN トラフィックのデフォルト トンネル ゲートウェイとして指定するには、このオプションを選択します。設定できるデフォルトのトンネル ゲートウェイは、デバイスごとに 1 つのみです。ルーテッド モードの ASA 7.0 以降のデバイスでのみ使用できます。

ASA ルーティング ポリシーのポリシーオブジェクトの設定

ASA ルーティングポリシーで使用するポリシーオブジェクトがいくつかあります。このリファレンスでは、これらのポリシー オブジェクトの設定について説明します。

ここでは、次の内容について説明します。

- ルートマップオブジェクトについて （214 ページ）
- [ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス （230 ページ）
- [プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （235 ページ）

- [プレフィックスリストIPv6オブジェクトの追加または編集（Add or Edit Prefix List IPv6 Object）] ダイアログボックス （238 ページ）
- [ASパスオブジェクトの追加（（Add AS Path Object））]/[ASパスオブジェクトの編集（Edit AS Path Object）] ダイアログボックス （242 ページ）
- [コミュニティリストオブジェクトの追加または編集（Add or Edit Community List Object）] ダイアログボックス （244 ページ）
- BFD テンプレートの作成 （125 ページ）

ルートマップオブジェクトについて

ルートマップを使用して、1 つのルーティングプロトコルから他のルーティングプロトコルへのルートを再配布するか、またはポリシールーティングを有効にするための条件を定義します。

ルート マップは、広く知られた ACL と共通の機能を数多く持っています。両方に共通する主な特性は次のとおりです。

- いずれも、それぞれが許可または拒否の結果を持つ個々の文を一定の順序で並べたものです。ACL またはルートマップの評価は、事前に定義された順序でのリストのスキャンと、一致する各文の基準の評価で構成されています。リストのスキャンは、文の一致が初めて見つかり、その文に関連付けられたアクションが実行されると中断します。
- これらは汎用メカニズムです。基準の一致と一致の解釈は、その適用方法によって指定されます。異なるタスクに適用される同じルート マップの解釈が異なることがあります。

次のように、ルート マップと ACL には違いがいくつかあります。

- ルート マップでは、一致基準として ACL を頻繁に使用します。

（注） ルートマップは、ユーザ、ユーザーグループ、セキュリティグループ、または完全修飾ドメイン名のオブジェクトを含む ACL をサポートしていません。

- ACL の評価の主な結果は、yes または no の答えとなります。つまり、ACL は入力データを許可するか拒否するかのいずれかです。再配布に適用された ACL は、特定のルートを再配布できるか（ルートが ACL の permit 文に一致）、再配布できないか（deny 文に一致）を判断します。一般的なルートマップでは、（一部の）再配布ルートを許可するだけではなく、別のプロトコルに再配布される場合は、ルートに関連付けられた情報も変更します。
- ルート マップは ACL よりも柔軟性が高く、ACL が確認できない基準に基づいてルートを確認できます。たとえば、ルート マップはルート タイプが内部であるかどうかを確認できます。

- 各 ACL は、設計の表記法により暗黙的な deny 文で終了しますが、ルート マップには同様の表記法はありません。一致試行の間にルートマップの終わりに達した場合は、そのルートマップの特定のアプリケーションによって結果が異なります。幸いなことに、再配布に適用されたルート マップの動作は ACL と同じです。ルートがルート マップのどの句とも一致しない場合は、ルート マップの最後に deny 文が含まれている場合と同様にルートの再配布は拒否されます。

ルート マップは、再配布中にルート情報を変更する場合や、ACL よりも強力な照合機能が必要な場合に推奨します。プレフィックスまたはマスクに基づいて一部のルートを選択的に許可することだけが必要な場合は、ルートマップを使用して、ACL（または等価のプレフィックス リスト）に直接マップすることをお勧めします。

（注） 標準 ACL をルート マップの一致基準として使用する必要があります。拡張 ACL を使用しても機能しないため、ルートが再配布されなくなります。将来的に句を挿入する必要性が生じたときの番号の間隔を確保するために、10 単位で句に番号を指定することをお勧めします。

permit 句と deny 句

ルート マップでは permit 句と deny 句を使用できます。このルート マップの一致基準が満たされた場合、permit キーワードが指定されていると、設定アクションに従ってルートが再配布されます。一致基準が満たされなかった場合、permit キーワードが指定されていると、同じマップ タグを持つ次のルート マップがテストされます。あるルートが、同じ名前を共有するルート マップ セットの一致基準のいずれをも満たさない場合、そのセットによる再配布は行われません。ルート マップの一致基準が満たされた場合でも、deny キーワードが指定されているとルートは再配布されません。

次のルールが適用されます。

- ルート マップの permit 句で ACL を使用する場合は、その ACL で許可されるルートが再配布されます。
- ルート マップの deny 句で ACL を使用すると、ACL で許可されるルートは再配布されません。
- ルートマップの permit 句または deny 句で ACL を使用する場合に、その ACL でルートが拒否されるときは、そのルートマップ句に一致するものは見つからないことになり、次のルート マップ句が評価されます。

match 句と set 句の値

ルートマップステートメントのエントリごとに、match 句と set 句の組み合わせが含まれています。match 句では、該当するパケットが特定のポリシーを満たす基準（つまり、満たすべき条件）を定義します。set 句は、一致基準を満たしたパケットをどのようにルーティングするかを説明します。

再配布される各ルートについて、ルータは最初にルートマップの句の一致基準を評価します。一致基準が満たされると、そのルートは permit 句または deny 句の指示に従って再配布または拒否され、一部の属性は set 句で定義したように変更されることがあります。一致基準が満たされないと、この句はルートに適用されず、ソフトウェアはルートマップの次の句でルートを評価します。ルートマップのスキャンは、ルートと一致する句が見つかるまで、もしくはルートマップの最後に到達するまで続行します。

次のいずれかの条件が満たされる場合は、各句の match 値または set 値を省略したり、何回か繰り返したりできます。

- 複数の Match 句の値が句に存在する場合、指定したルートが句に一致するためには、そのルートですべての照合に成功しなければなりません（つまり、複数の match コマンドでは論理 AND アルゴリズムが適用されます）。
- 1 つのコマンド内で 1 つの Match 句の値が複数のオブジェクトを参照している場合、そのオブジェクトのいずれかが一致する必要があります（論理 OR アルゴリズムが適用されます）。
- Match 句の値が存在しない場合は、すべてのルートが句に一致します。
- ルートマップの permit 句に Set 値が存在しない場合、そのルートは現在の属性の変更なしに再配布されます。

（注） ルートマップの deny 句では Set 値を設定しないでください。deny 句を指定するとルートの再配布が禁止され、情報が何も変更されないからです。

Match または Set 値がないルートマップ句は、アクションを実行します。空の permit 句を使用すると、変更を加えずに残りのルートの再配布が可能になります。空の deny 句では、他のルートの再配布はできません。これは、ルートマップがすべてスキャンされたときに、明示的な一致が見つからなかったときのデフォルト アクションです。

BGP match 句および BGP set 句

前述の match および set の値に加えて、BGP ではルート マップに対して追加の match および set 機能が提供されています。

次のルートマップの match 句が BGP でサポートされています。

- match AS path access list
- match community
- match policy list

次のルートマップの set 句が BGP でサポートされています。

- set AS path
- set community

- set automatic tag
- set local preference
- set weight
- set origin
- set next hop
- set IP prefix list

ルートマップオブジェクトの作成と使用

ルートマップを識別する必要があるポリシーを設定する場合、[ルートマップ（Route Map）] フィールドの横にある [選択（Select）] ボタンをクリックして、ルートマップオブジェクトを選択または作成できます。[ルートマップオブジェクトセレクタ（Route Map Object Selector ）] ダイアログボックスから新しいルートマップを作成するには、ルートマップリストの下にある [作成（Create）] ボタンをクリックします。オブジェクトタイプセレクタから [ルートマップ（Route Map）] を選択し、[新規オブジェクト（New Object）] ボタンをクリックすることにより、 Policy Object Managerからルートマップオブジェクトを作成することもできます。ルートマップオブジェクトを作成するときに使用できる特定のフィールドについては、[ルートマップオブジェクトの追加または編集（Add or Edit Route Map Object）] ダイアログボックス （218 ページ）を参照してください。

BGP ポリシーでのルートマップオブジェクトの使用に関する注意

ルートマップで使用される一致基準および設定基準の一部は、すべての BGP サブコマンドでサポートされていません。次に例を示します。

次のルートマップの一致基準：

- Match Clause tab > Match first hop interface of route、Match Next Hop (IPv4 and IPv6)、Match Route Source (IPv4 and IPv6)、Match Metric Route Value、および Match Tag
- BGP Match Clause tab > Match AS path access lists

および次のルートマップの設定基準：

- Set Clause tab > Metric Values (all fields) および Metric Type
- BGP Set Clause tab > Set AS path、Prepend AS path、および Prepend last AS to the AS path

は、次の場所ではサポートされていません。

- BGP policy > IPv4 Address Family:
  - Aggregate Address tab > Attribute Map、Advertise Map、および Suppress Map
  - Neighbor tab > Filtering tab
  - Route Injection tab > Inject Map および Exist Map

Security Manager では、ルートマップにサポートされていない一致基準または設定基準が含まれている場合でも、BGP設定でルートマップを使用でき、検証中に警告やエラーを受け取ることはありません。このような場合、展開は失敗し、デバイスから次の形式のエラーを受け取ります：...%"My-Route-map" used as BGP inbound route-map, nexthop match not supported... 。

BGP 設定で使用されるルートマップでサポートされる一致/設定基準に関するガイドラインについては、ASA のドキュメントを参照してください。

関連項目

- [ルートマップオブジェクトの追加または編集（Add or Edit Route Map Object）] ダイアログボックス （218 ページ）
- [ルートマップエントリの追加または編集（Add or Edit Route Map Entry）] ダイアログボックス （220 ページ）
- ポリシーのオブジェクトの選択
- ポリシー オブジェクトの作成
- オブジェクトの編集
- カテゴリ オブジェクトの使用
- オブジェクト オーバーライドの管理
- ポリシー オブジェクトの上書きの許可

[ルートマップオブジェクトの追加または編集（Add or Edit Route Map Object）] ダイアログボックス

[ルートマップオブジェクトの追加または編集（Add/Edit Route Map Object）] ダイアログボックスを使用して、ルートマップポリシーオブジェクトを作成、コピー、および編集します。ルートマップを使用して、1つのルーティングプロトコルから他のルーティングプロトコルへのルートを再配布するか、またはポリシールーティングを有効にするための条件を定義できます。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [ルートマップ（Route Map）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- ルートマップオブジェクトについて （214 ページ）
- [ルートマップエントリの追加または編集（Add or Edit Route Map Entry）] ダイアログボックス （220 ページ）
- Policy Object Manager

- ポリシーのオブジェクトの選択
- ポリシー オブジェクトの作成
- オブジェクトの編集
- カテゴリ オブジェクトの使用
- オブジェクト オーバーライドの管理
- ポリシー オブジェクトの上書きの許可

フィールド リファレンス

表 *105 : [*ルートマップオブジェクトの追加または編集（*Add/Edit Route Map Object*）*]* ダイアログボックス

要素	説明
名前	ルートマップオブジェクト用の意味のある名前を入力します。ルートマップオブジェクト名は 58 文字以下にする必要があります。 **注意** Cisco Security Manager では、デバイスで名前を変更できない場合でもオブジェクトの名前を変更できます。Cisco Security Manager でこれらのオブジェクトの名前を変更する場合、既存の CLI を無効にして、新しい CLI を発行し、新しい名前を使用してオブジェクトを作成して割り当てることで名前を変更します。この最初の無効化により、環境内でルーティングやネットワークの問題を引き起こす可能性があります。オブジェクトの名前を変更しても、Security Manager はこれらの結果に関する警告メッセージを表示しません。
説明	（任意）オブジェクトの説明。
ルートマップテーブル（Route Map table）	オブジェクトで定義されているルートマップエントリ。 • ルートマップエントリを追加するには、[追加（Add）] ボタンをクリックして、[ルートマップエントリの追加または編集（Add or Edit Route Map Entry）] ダイアログボックス （220 ページ）を開きます。 • ルートマップエントリを編集するには、エントリを選択し、[編集（Edit）] ボタンをクリックします。 • ルートマップエントリを削除するには、エントリを選択し、[削除（Delete）] ボタンをクリックします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[ルートマップエントリの追加または編集（Add or Edit Route Map Entry）] ダイアログボックス

[ルートマップエントリの追加または編集（Add/Edit Route Map Entry）] ダイアログボックスを使用して、ルートマップオブジェクトの新しいルートマップエントリを作成したり、既存のルートマップエントリを編集したりします。

ナビゲーション パス

[ルートマップオブジェクトの追加または編集（Add or Edit Route Map Object）] ダイアログボックス （218 ページ）で、[ルートマップ（Route Map）] テーブルの下にある [追加（Add）] ボタンをクリックするか、またはテーブル内のエントリを選択して [編集（Edit）] ボタンをクリックします。

関連項目

- ルートマップオブジェクトについて （214 ページ）
- [ルートマップエントリの追加または編集（Add or Edit Route Map Entry）] ダイアログボックス （220 ページ）
- Policy Object Manager
- ポリシーのオブジェクトの選択
- ポリシー オブジェクトの作成
- オブジェクトの編集
- カテゴリ オブジェクトの使用
- オブジェクト オーバーライドの管理
- ポリシー オブジェクトの上書きの許可

フィールド リファレンス

表 *106 : [*ルートマップエントリの追加または編集（*Add/Edit Route Map Entry*）*]* ダイアログボックス

要素	説明
シーケンス番号（Sequence Number）	このルートマップオブジェクトにすでに設定されているルートマップエントリのリストでの新しいルートマップエントリの位置を示す 0 ～ 65535 の番号。 **ヒント** 将来的に句を挿入する必要性が生じたときの番号の間隔を確保するために、少なくとも 10 単位で句に番号を指定することをお勧めします。
再配布	ルートを再配布するかどうか。一致するルートの再配布を許可するには、[許可（Permit）] をクリックします。一致するルートの再配布を拒否するには、[拒否（Deny）] を選択します。 ルートマップの Permit 句で ACL を使用すると、その ACL で許可されるルートが再配布されます。ルート マップの Deny 句で ACL を使用すると、その ACL で許可されるルートは再配布されなくなります。さらに、ルートマップの Permit または Deny 句で ACL を使用する場合に、その ACL でルートが拒否されたときは、そのルート マップ句に一致するものは見つからなかったことになり、次のルート マップ句が評価されます。
[match 句（Match Clause）] タブ [match 句（Match Clause）] タブを選択して、この句を適用する必要のあるルートを選択し、次のパラメータを設定します。	
[ルートの最初のホップインターフェイスを照合（Match first hop interface of route）]	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の照合を有効または無効にします。照合するインターフェースを入力または選択します。複数のエントリがある場合は、カンマで区切ります。2 つ以上のインターフェイスを指定する場合、ルートはいずれかのインターフェイスと一致します。 省略記号を使用して、1 つ以上のインターフェイスを選択できるインターフェイスセレクタを開きます。インターフェイスセレクタから新しいインターフェイスロールを作成することもできます。詳細については、インターフェイス ロール オブジェクトについてを参照してください。
IPv4	

要素	説明
[アドレスの照合（Match Address）]	指定した、いずれかのアクセスリストによって渡されるルートアドレスまたは一致パケットがあるルートの照合を有効または無効にします。 IPv4 アドレスに対して、照合にアクセス リストまたはプレフィックス リストを使用するかどうかをドロップダウン リストから選択し、照合に使用する ACL オブジェクトまたはプレフィックス リストを入力または選択します。 省略記号を使用して、1 つ以上のオブジェクトを選択できるアクセス制御リストオブジェクトセレクタまたはプレフィックス リスト オブジェクト セレクタを開きます。オブジェクトセレクタから新しいオブジェクトを作成することもできます。詳細については、[Add Access List]/[Edit Access List] ダイアログボックスまたは [プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （235 ページ）を参照してください。
[ネクストホップの照合（Match Address）]	ルートのネクストホップアドレスの照合を有効または無効にします。 IPv4 アドレスに対して、照合にアクセス リストまたはプレフィックス リストを使用するかどうかをドロップダウン リストから選択し、照合に使用する ACL オブジェクトまたはプレフィックス リストを入力または選択します。 省略記号を使用して、1 つ以上のオブジェクトを選択できるアクセス制御リストオブジェクトセレクタまたはプレフィックス リスト オブジェクト セレクタを開きます。オブジェクトセレクタから新しいオブジェクトを作成することもできます。詳細については、[Add Access List]/[Edit Access List] ダイアログボックスまたは [プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （235 ページ）を参照してください。

要素	説明
[ルートの送信元の照合（Match Route Source）]	ルートのアドバタイジング ソース アドレスの照合を有効または無効にします。 IPv4 アドレスに対して、照合にアクセス リストまたはプレフィックス リストを使用するかどうかをドロップダウン リストから選択し、照合に使用する ACL オブジェクトまたはプレフィックス リストを入力または選択します。 省略記号を使用して、1 つ以上のオブジェクトを選択できるアクセス制御リストオブジェクトセレクタまたはプレフィックス リスト オブジェクト セレクタを開きます。オブジェクトセレクタから新しいオブジェクトを作成することもできます。詳細については、[Add Access List]/[Edit Access List] ダイアログボックスまたは [プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （235 ページ）を参照してください。
IPv6	
[アドレスの照合（Match Address）]	指定した、いずれかのアクセスリストによって渡されるルートアドレスまたは一致パケットがあるルートの照合を有効または無効にします。 IPv6 アドレスに対して、照合にアクセスリストまたは IPv6 プレフィックスリストを使用するかどうかをドロップダウンリストから選択し、照合に使用する ACL オブジェクトまたは IPv6 プレフィックスリストを入力または選択します。 省略記号を使用して、1 つ以上のオブジェクトを選択できるアクセス制御リストオブジェクトセレクタまたは IPv6 プレフィックス リスト オブジェクト セレクタを開きます。オブジェクトセレクタから新しいオブジェクトを作成することもできます。詳細については、[Add Access List]/[Edit Access List] ダイアログボックスまたは [プレフィックスリスト IPv6 オブジェクトの追加または編集（Add or Edit Prefix List IPv6 Object）] ダイアログボックス （238 ページ）を参照してください。

要素	説明
[ネクストホップの照合（Match Address）]	ルートのネクストホップアドレスの照合を有効または無効にします。 IPv6 アドレスに対して、照合にアクセスリストまたはプレフィックスリストを使用するかどうかをドロップダウンリストから選択し、照合に使用する ACL オブジェクトまたは IPv6 プレフィックスリストを入力または選択します。 省略記号を使用して、1つ以上のオブジェクトを選択できるアクセス制御リストオブジェクトセレクタまたはIPv6プレフィックスリストオブジェクトセレクタを開きます。オブジェクトセレクタから新しいオブジェクトを作成することもできます。詳細については、[Add Access List]/[Edit Access List] ダイアログボックスまたは[プレフィックスリストIPv6オブジェクトの追加または編集（Add or Edit Prefix List IPv6 Object）] ダイアログボックス （238 ページ）を参照してください。
[ルートの送信元の照合（Match Route Source）]	ルートのアドバタイジング ソース アドレスの照合を有効または無効にします。 IPv6 アドレスに対して、照合にアクセスリストまたは IPv6 プレフィックスリストを使用するかどうかをドロップダウンリストから選択し、照合に使用する ACL オブジェクトまたは IPv6 プレフィックスリストを入力または選択します。 省略記号を使用して、1つ以上のオブジェクトを選択できるアクセス制御リストオブジェクトセレクタまたはIPv6プレフィックスリストオブジェクトセレクタを開きます。オブジェクトセレクタから新しいオブジェクトを作成することもできます。詳細については、[Add Access List]/[Edit Access List] ダイアログボックスまたは[プレフィックスリストIPv6オブジェクトの追加または編集（Add or Edit Prefix List IPv6 Object）] ダイアログボックス （238 ページ）を参照してください。
[メトリックルート値の照合（Match Metric Route Value）]	ルートのメトリックの照合を有効または無効にします。[メトリックルート値の照合（Match Metric Route Value）] フィールドに、照合に使用するメトリック値を入力します。複数の値をカンマで区切って入力することもできます。設定したメトリックを持つ任意のルートを照合できます。メトリック値は、0 ～ 4294967295 の範囲で指定します。

要素	説明
[タグの照合（Match Tag）]	ルートのセキュリティグループタグの照合を有効または無効にします。[タグの照合（Match Tag）] フィールドに照合に使用するタグ値を入力します。複数の値をカンマで区切って入力することもできます。指定したセキュリティ グループ タグを持つ任意のルートを照合できます。タグ値は、0 ～ 4294967295 の範囲で指定します。
[ルートタイプの照合（Match Route Type）]	ルートタイプの照合を有効または無効にします。有効なルート タイプは、External1、External2、Internal、Local、NSSA-External1、NSSA-External2 です。イネーブルの場合、複数のルート タイプをリストから選択することができます。
[set 句（Set Clause）] タブ [set 句（Set Clause）] タブを選択して、ターゲットプロトコルに再配布される次の情報を変更します。 （注） 帯域幅の値のみまたはすべての値を指定するか、まったく指定しないこともできます。	
Bandwidth	メトリック値または帯域幅（K ビット/秒単位）。0 ～ 4294967295 の整数値です。
[EIGRP 遅延（EIGRP Delay）]	EIGRP ルート遅延（10 マイクロ秒単位）。有効値の範囲は 1 ～ 4294967295 です。
[EIGRP 信頼性（EIGRP Reliability）]	0 ～ 255 の数値で表される、EIGRP のパケット伝送の成功確率。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを意味します。
[EIGRP 有効（EIGRP Effective）]	1 ～ 255 の数値で表される、ルートの有効な EIGRP 帯域幅。値 255 は、100% のロードを意味します。
[EIGRP MTU]	EIGRP のルートの最小 MTU サイズ（バイト単位）。有効値の範囲は 1 ～ 4294967295 です。
メトリック タイプの設定	宛先ルーティングプロトコルのメトリックタイプを選択して指定し、ドロップダウンリストからメトリックタイプ（[内部（internal）]、[タイプ 1（type-1）]、または[タイプ 2（type-2）]）を選択します。
[BGP match 句（BGP Match Clause）] タブ	

要素	説明
[BGP AS パスアクセスリストの照合（Match AS path access lists）]	BGP 自律システムパスアクセスリストと指定されたパスアクセスリストの照合を有効にする場合は、オンにします。複数のパス アクセス リストを指定した場合、ルートはいずれかのパス アクセス リストと一致します。 省略記号を使用して、1 つ以上の AS パスオブジェクトを選択できる AS パスオブジェクトセレクタを開きます。AS パスオブジェクトセレクタから新しい AS パスオブジェクトを作成することもできます。詳細については、[ASパスオブジェクトの追加（（Add AS Path Object））]/[ASパスオブジェクトの編集（Edit AS Path Object）] ダイアログボックス （242 ページ）を参照してください。
[コミュニティの照合（Match community）]	BGP コミュニティと指定されたコミュニティの照合を有効にするために選択します。複数のコミュニティを指定した場合、ルートはいずれかのコミュニティと一致します。少なくとも 1 つの Match コミュニティと一致しないルートは、アウトバウンドルートマップにアドバタイズされません。 省略記号を使用して、1 つ以上のコミュニティ リスト オブジェクトを選択できるコミュニティリストオブジェクトセレクタを開きます。コミュニティ リスト オブジェクト セレクタから新しいコミュニティ リスト オブジェクトを作成することもできます。詳細については、[コミュニティリストオブジェクトの追加または編集（Add or Edit Community List Object）] ダイアログボックス （244 ページ）を参照してください。 BGP コミュニティと指定したコミュニティの完全一致を有効にするには、[指定したコミュニティと完全に一致（Match the specified community exactly）] チェックボックスをオンにします。
[ポリシーリストの照合（Match policy list）]	BGP ポリシーを評価および処理するためのルートマップを設定する場合は、オンにします。1 つのルート マップ エントリ内で複数のポリシー リストが照合を行う場合、ポリシー リストすべては受信属性だけで照合を行います。 省略記号を使用して、1 つ以上のポリシーリストオブジェクトを選択できるポリシーリストオブジェクトセレクタを開きます。ポリシーリストオブジェクトセレクタから新しいポリシーリストオブジェクトを作成することもできます。詳細については、[ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス （230 ページ）を参照してください。
[BGP set 句（BGP Set Clause）] タブ [BGP set 句（BGP Set Clause）] タブを選択して、BGP プロトコルに再配布される次の情報を変更します。	

要素	説明
[AS パス の設定（Set AS path）]	BGPルートの自律システムパスを変更する場合は、オンにします。 • BGP ルートの前に任意の自律システムパス文字列を付加するには、[AS パスプリペンド（Prepend AS path）] をオンにします。通常、ローカルなAS番号が複数回追加され、自律システム パス長が増します。複数の AS パス番号を指定した場合、ルートはいずれかの AS 番号を付加できます。 • 最後の AS 番号を AS パスの前に付加するには、[最後の AS を AS パスの前に付加（Prepend last AS to the AS path）] をオンにします。AS 番号の値を 1 ～ 10 の範囲で入力します。 • ルートのタグを自律システムパスに変換するには、[ルートタグを AS パスに変換する（Convert route tag into AS path）] をオンにします。
[コミュニティの設定（Set community）]	BGP コミュニティ属性を設定する場合は、オンにします。 • ルートマップをパスするプレフィックスからコミュニティ属性を除去するには、[なし（None）] をオンにします。 • コミュニティ番号を入力するには、[コミュニティの指定（Specify community）] をオンにします（必要な場合）。有効な値は、1 ～ 4294967295 です。 既存のコミュニティにコミュニティを追加するには、[既存のコミュニティに追加する（Add to the existing communities）] をオンにします。 • 既知のコミュニティのいずれかを使用するには、[インターネット（Internet）]、[アドバタイズなし（no-advertise）]、または [エクスポートなし（no-export）] をオンにします。
[自動タグ設定（Set Automatic-tag）]	自動的にタグ値を計算する場合は、オンにします。
[ローカルプリファレンスの設定（Set local preference）]	自律システムパスのプリファレンス値を指定する場合は、オンにします。0 から 4294967295 までの値を入力してください。
[重みの設定（Set weight）]	ルーティングテーブルの BGP 重みを設定する場合は、オンにします。0 ～ 65535 の範囲で値を入力します。
[発信元の設定（Set origin）]	BGP の発信元コードを選択して指定します。有効な値は [Local IGP] および [Incomplete] です。
[ネクストホップ IPv4（Next hop IPv4）]	

要素	説明
[ネクストホップの設定（Set next hop）]	ルートマップの match 句を満たすパケットの出力アドレスを指定する場合は、オンにします。 • パケットが出力されるネクストホップの IPv4 アドレスを入力するには、[IPv4 アドレスを指定（Specify IPv4 address）] をオンにします。隣接ルータである必要はありません。複数の IPv4 アドレスを指定した場合、いずれかの IP アドレスでパケットを出力できます。 • BGP ピアアドレスにするネクストホップを設定するには、[ピアアドレスの使用（Use peer address）] をオンにします。
[ネクストホップ IPv6（Next hop IPv6）]	
[ネクストホップの設定（Set next hop）]	ルートマップの match 句を満たすパケットの出力アドレスを指定する場合は、オンにします。 • パケットが出力されるネクストホップの IPv6 アドレスを入力するには、[IPv6 アドレスを指定（Specify IPv6 address）] をオンにします。隣接ルータである必要はありません。複数の IPv6 アドレスを指定した場合、いずれかの IP アドレスでパケットを出力できます。複数の値をカンマで区切って入力することもできます。 • BGP ピアアドレスにするネクストホップを設定するには、[ピアアドレスの使用（Use peer address）] をオンにします。
プレフィックス リスト	
[IPv4 プレフィックスリストの設定（Set IPv4 prefix list）]	IPv4 プレフィックスリストを設定する場合は、オンにします。 省略記号を使用して、1 つ以上のプレフィックス リスト オブジェクトを選択できるプレフィックスリストオブジェクトセレクタを開きます。プレフィックスリストオブジェクトセレクタから新しいプレフィックス リスト オブジェクトを作成することもできます。詳細については、[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （235 ページ）を参照してください。

要素	説明
[IPv6プレフィックスリストの設定（Set IPv6 prefix list）]	IPv6 プレフィックスリストを設定する場合は、オンにします。 省略記号を使用して、1 つ以上の IPv6 プレフィックス リスト オブジェクトを選択できるプレフィックス リスト オブジェクト IPv6 セレクタを開きます。プレフィックスリストオブジェクトセレクタから新しい IPv6 プレフィックス リスト オブジェクトを作成することもできます。詳細については、[プレフィックスリストIPv6 オブジェクトの追加または編集（Add or Edit Prefix List IPv6 Object）] ダイアログボックス （238 ページ）を参照してください。
[ポリシーベースルーティング（PBR）（Policy Based Routing（PBR））] タブ [Policy Based Routing] タブをクリックして、トラフィック フローにポリシーを設定し、ルーティング プロトコルから派生したルートへの依存を弱めることができます。PBR は、ルーティングプロトコルで提供される既存のメカニズムを拡張および補完することにより、ルーティングの制御を強化します。PBR を使用すると、IP プレジデンスを設定できます。高コストリンク上のプライオリティ トラフィックなど、特定のトラフィックのパスを指定することもできます。	
[デフォルトのネクストホップ IPv4 アドレスの設定（Set Default Next-Hop IPv4 Address）]	ポリシールーティング用のルートマップの match 句を渡すパケットの出力先を指定するには、[デフォルトのネクストホップ IPv4 アドレスの設定（Set default next-hop IPv4 address）] チェックボックスをオンにします。[IPv4 Address] に、宛先アドレスを入力します。
[デフォルトのネクストホップ IPv6 アドレスの設定（Set Default Next-Hop IPv6 Address）]	ポリシールーティング用のルートマップの match 句を渡すパケットの出力先を指定するには、[デフォルトのネクストホップ IPv6 アドレスの設定（Set default next-hop IPv6 address）] チェックボックスをオンにします。[IPv6 アドレス（IPv6 Address）] に宛先アドレスを入力します。
[ネクストホップ IPv4 アドレスの再帰検索および設定（Recursively find and set Next-Hop IPv4 Address）]	[Recursively find and set next-hop IP address] チェック ボックスをオンにして、[IPv4 Address] フィールドで IP アドレスを指定します。この場合、ネクストホップ IP アドレスは直接接続されたサブネットにある必要はありません。
[インターフェイスの設定（Set Interfaces）]	[インターフェイスの設定（Set interfaces）] チェックボックスをオンにして、[インターフェイスセレクタ（Interfaces Selector）] ダイアログボックスから接続先インターフェイスを選択します。
[Null0 インターフェイスをデフォルトインターフェイスとして設定（Set Null0 Interfaces as Default Interface）]	一部のトラフィックを完全にブラック ホール化またはドロップする必要がある場合には、[Set null0 interface as the default interface] チェック ボックスをオンにします。

要素	説明
do-not-fragment ビットを 0 または 1 に設定します。	[Set do-not-fragment bit to either 1or 0] をオンにして、適切なオプション ボタンを選択します。
[IPv4 パケットの QoS ビットに DiffServ コードポイント（DSCP）を設定（Set Differential Service Code Point (DSCP) value in QOS bits for IPv4 packets）]	[IPv4 パケットの QoS ビットに DiffServ コードポイント（DSCP）を設定（Set differential service code point (DSCP) value in QoS bits for IPv4 packets）] チェックボックスをオンにして、0 ～ 63 の値を入力するか [値の選択（Select Value）] ドロップダウンリストから値を選択します。
[IPv6 パケットの QoS ビットに DiffServ コードポイント（DSCP）を設定（Set Differential Service Code Point (DSCP) value in QOS bits for IPv6 packets）]	[IPv6 パケットの QoS ビットに DiffServ コードポイント（DSCP）を設定（Set differential service code point (DSCP) value in QoS bits for IPv6 packets）] チェックボックスをオンにして、0 ～ 63 の値を入力するか [値の選択（Select Value）] ドロップダウンリストから値を選択します。
[適応型インターフェイスの設定（Set Adaptive Interface）]	[適応型インターフェイスの設定（Set Adaptive Interface）] チェックボックスをオンにして、ドロップダウンリストからメトリックを選択し、[適応型インターフェイスの設定（Set Adaptive Interface）] ダイアログボックスでインターフェイスを指定して、PBR トラフィックをルーティングするためのベストパスを決定します。適応型インターフェイスのメトリックは次のとおりです。 • [コスト（cost）]：トラフィックは、インターフェイスの優先度に基づいて転送されます。 • [ジッター（jitter）]：トラフィックは、ジッター値が最小のインターフェイスに転送されます。 [損失（lost）]：トラフィックは、パケット損失が最小のインターフェイスに転送されます。 • [MOS（mos）]：トラフィックは、平均オピニオン評点（MOS）が最大のインターフェイスに転送されます。 • [RTT（rtt）]：トラフィックは、ラウンドトリップ時間（RTT）が最短のインターフェイスに転送されます。

[ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス

[ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックスを使用して、ポリシーリストのポリシーオブジェクトを作成、コピー、および編集します。

ルートマップの設定時に使用するポリシーリストオブジェクトを作成できます（ルートマップオブジェクトについて （214 ページ）を参照）。

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 リストを設定できます。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。1 つのルート マップ エントリ内で複数のポリシー リストが照合を行う場合、ポリシー リストすべては受信属性だけで照合を行います。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次に、オブジェクトタイプセレクタから [ポリシーリスト（Policy List）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- ルートマップオブジェクトについて （214 ページ）
- Policy Object Manager
- ポリシーのオブジェクトの選択
- ポリシー オブジェクトの作成
- オブジェクトの編集
- カテゴリ オブジェクトの使用
- オブジェクト オーバーライドの管理
- ポリシー オブジェクトの上書きの許可

フィールド リファレンス

表 *107 : [*ポリシーリストオブジェクトの追加/編集（*Add/Edit Policy List Object*）*]* ダイアログボックス

要素	説明
名前	オブジェクトの名前。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成を参照してください。 **注意** Cisco Security Manager では、デバイスで名前を変更できない場合でもオブジェクトの名前を変更できます。Cisco Security Manager でこれらのオブジェクトの名前を変更する場合、既存の CLI を無効にして、新しい CLI を発行し、新しい名前を使用してオブジェクトを作成して割り当てることで名前を変更します。この最初の無効化により、環境内でルーティングやネットワークの問題を引き起こす可能性があります。オブジェクトの名前を変更しても、Security Manager はこれらの結果に関する警告メッセージを表示しません。
説明	（任意）オブジェクトの説明。
[基本（Basic）] タブ	
操作	条件に一致するアクセスを許可するかどうかを指定します。 （注） ポリシーリストオブジェクトの [アクション（Action）] は、オブジェクトの作成後は変更できません。
インターフェイスの照合（Match Interface）	指定したいずれかのインターフェイスをネクストホップとするルートを配布する場合に選択します。照合するインターフェースを入力または選択します。複数のエントリがある場合は、カンマで区切ります。2つ以上のインターフェイスを指定する場合、ルートはいずれかのインターフェイスと一致します。 省略記号を使用して、1つ以上のインターフェイスを選択できるインターフェイスセレクタを開きます。インターフェイスセレクタから新しいインターフェイスロールを作成することもできます。詳細については、インターフェイス ロール オブジェクトについてを参照してください。

要素	説明
アドレスの照合（Match Address）	標準アクセスリストまたはプレフィックスリストで許可された宛先アドレスを持つルートを再配布するために選択します。ドロップダウンリストから [アクセスリスト（Access List）] または [プレフィックスリスト（Prefix List）] を選択し、照合に使用する ACL オブジェクトまたはプレフィックス リスト オブジェクトを入力または選択します。 省略記号を使用して、1つ以上のオブジェクトを選択できるアクセス制御リストオブジェクトセレクタまたはプレフィックス リスト オブジェクトセレクタを開きます。オブジェクトセレクタから新しいオブジェクトを作成することもできます。詳細については、[Add Access List]/[Edit Access List] ダイアログボックスまたは[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （235 ページ）を参照してください。
ネクストホップの照合（Match Next-Hop）	指定したアクセスリストまたはプレフィックスリストの 1 つから渡されたネクストホップルータ アドレスを持つルートを再配布するために選択します。ドロップダウンリストから [アクセスリスト（Access List）] または [プレフィックスリスト（Prefix List）] を選択し、照合に使用する ACL オブジェクトまたはプレフィックス リスト オブジェクトを入力または選択します。 省略記号を使用して、1つ以上のオブジェクトを選択できるアクセス制御リストオブジェクトセレクタまたはプレフィックス リスト オブジェクトセレクタを開きます。オブジェクトセレクタから新しいオブジェクトを作成することもできます。詳細については、[Add Access List]/[Edit Access List] ダイアログボックスまたは[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （235 ページ）を参照してください。
[ルートの送信元の照合（Match Route Source）]	アクセスリストまたはプレフィックスリストで指定されたアドレスのルータおよびアクセスサーバーによってアドバタイズされたルートを再配布するために選択します。ドロップダウンリストから [アクセスリスト（Access List）] または [プレフィックスリスト（Prefix List）] を選択し、照合に使用する ACL オブジェクトまたはプレフィックス リスト オブジェクトを入力または選択します。 省略記号を使用して、1つ以上のオブジェクトを選択できるアクセス制御リストオブジェクトセレクタまたはプレフィックス リスト オブジェクトセレクタを開きます。オブジェクトセレクタから新しいオブジェクトを作成することもできます。詳細については、[Add Access List]/[Edit Access List] ダイアログボックスまたは[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （235 ページ）を参照してください。
[Advanced] タブ	

要素	説明
ASパスの照合（Match AS Path）	BGP 自律システムパスを照合するために選択します。複数の AS パスを指定した場合、ルートはいずれかの AS パスと一致します。 省略記号を使用して、1 つ以上の AS パスオブジェクトを選択できる AS パスオブジェクトセレクタを開きます。AS パスオブジェクトセレクタから新しいASパスオブジェクトを作成することもできます。詳細については、[ASパスオブジェクトの追加（（Add AS Path Object））]/[ASパスオブジェクトの編集（Edit AS Path Object）] ダイアログボックス （242 ページ）を参照してください。
コミュニティルールの照合（Match Community Rules）	BGP コミュニティと指定されたコミュニティの照合を有効にするために選択します。複数のコミュニティを指定した場合、ルートはいずれかのコミュニティと一致します。 省略記号を使用して、1 つ以上のコミュニティ リスト オブジェクトを選択できるコミュニティ リスト オブジェクト セレクタを開きます。コミュニティ リスト オブジェクト セレクタから新しいコミュニティ リスト オブジェクトを作成することもできます。詳細については、[コミュニティリストオブジェクトの追加または編集（Add or Edit Community List Object）] ダイアログボックス （244 ページ）を参照してください。 BGP コミュニティと指定したコミュニティの完全な照合を有効にするには、[exact-match] チェックボックスをオンにします。
メトリックの照合（Match Metric）	ルートのメトリックの照合を有効または無効にします。[メトリックの照合（Match Metric）] フィールドに、照合に使用するメトリック値を入力します。複数の値をカンマで区切って入力することもできます。設定したメトリックを持つ任意のルートを照合できます。メトリック値は、0～4294967295 の範囲で指定します。
[タグの照合（Match Tag）]	ルートのセキュリティグループタグの照合を有効または無効にします。[タグの照合（Match Tag）] フィールドに照合に使用するタグ値を入力します。複数の値をカンマで区切って入力することもできます。指定したセキュリティ グループ タグを持つ任意のルートを照合できます。タグ値は、0 ～ 4294967295 の範囲で指定します。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス

[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックスを使用して、プレフィックスリストのポリシーオブジェクトを作成、コピー、および編集します。ルートマップ（ルートマップオブジェクトについて （214 ページ）を参照）、ポリシーマップ（[ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス （230 ページ）を参照）、OSPF フィルタリング（[Add Filtering]/[Edit Filtering] ダイアログボックス （155 ページ）を参照）または BGP ネイバーフィルタリング（[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （16 ページ）を参照）を設定するときに使用する、プレフィックス リスト オブジェクトを作成できます。

エリア境界ルータ（ABR）のタイプ 3 リンクステートアドバタイズメント（LSA）フィルタリングは、OSPF を実行している ABR の機能を拡張して、異なる OSPF エリア間のタイプ 3 LSA をフィルタリングします。プレフィックス リストが設定されているときは、指定されたプレフィックスのみが OSPF エリア間で送信されます。その他のすべてのプレフィックスは、それぞれの OSPF エリアに制限されます。このタイプのエリア フィルタリングは、OSPF エリアを出入りするトラフィックに対して、またはそのエリアの着信と発信の両方のトラフィックに対して適用できます。

プレフィックス リストの複数のエントリが指定されたプレフィックスと一致する場合、シーケンス番号が最も小さいエントリが使用されます。効率性を高めるため、頻繁に一致するエントリまたは一致しないエントリに、小さいシーケンス番号を手動で割り当てることで、それらをリストの上部に配置することもできます。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）] を選択し、次に、オブジェクト タイプセレクタから [プレフィックスリスト（Prefix List）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- [プレフィックスリストエントリの追加または編集（Add or Edit Prefix List Entry）] ダイアログボックス （237 ページ）
- ルートマップオブジェクトについて （214 ページ）
- [ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス （230 ページ）
- Policy Object Manager
- ポリシーのオブジェクトの選択
- ポリシー オブジェクトの作成
- オブジェクトの編集
- カテゴリ オブジェクトの使用
- オブジェクト オーバーライドの管理
- ポリシー オブジェクトの上書きの許可

フィールド リファレンス

表 *108 : [プレフィックスリストオブジェクトの追加/編集（Add/Edit Prefix List Object）] ダイアログボックス*

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成を参照してください。 **注意** Cisco Security Manager では、デバイスで名前を変更できない場合でもオブジェクトの名前を変更できます。Cisco Security Manager でこれらのオブジェクトの名前を変更する場合、既存の CLI を無効にして、新しい CLI を発行し、新しい名前を使用してオブジェクトを作成して割り当てることで名前を変更します。この最初の無効化により、環境内でルーティングやネットワークの問題を引き起こす可能性があります。オブジェクトの名前を変更しても、Security Manager はこれらの結果に関する警告メッセージを表示しません。
説明	（任意）オブジェクトの説明。

要素	説明
プレフィックスリストテーブル	オブジェクトで定義されているプレフィックス リスト エントリ。 • プレフィックス リスト エントリを追加するには、[追加（Add）] ボタンをクリックして、[プレフィックスリストエントリの追加または編集（Add or Edit Prefix List Entry）] ダイアログボックス （237 ページ）を開きます。 • プレフィックス リスト エントリを編集するには、エントリを選択し、[編集（Edit）] ボタンをクリックします。 • プレフィックス リスト エントリを削除するには、エントリを選択し、[削除（Delete）] ボタンをクリックします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[プレフィックスリストエントリの追加または編集（Add or Edit Prefix List Entry）] ダイアログボックス

[プレフィックスリストエントリの追加または編集（Add or Edit Prefix List Entry）] ダイアログボックスを使用して、新しいプレフィックス リスト エントリを作成するか、既存のエントリを編集します。

ナビゲーション パス

[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （235 ページ）で、[プレフィックスリスト（Prefix Listt）] テーブルの下にある [追加（Add）] ボタンをクリックするか、またはテーブル内のエントリを選択して [編集（Edit）] ボタンをクリックします。

フィールド リファレンス

表 *109 : [*プレフィックスリストエントリの追加または編集（*Add/Edit Prefix List Entry*）*]* ダイアログボックス

要素	説明
操作	[許可（Permit）] または [拒否（Deny）] オプションボタンをクリックして再配布アクセスを指定します。
シーケンス No（Sequence No）	（任意）このオブジェクトですでに設定されているプレフィックス リスト エントリのリストにおける、新しいプレフィックス リストエントリの位置を示す固有の数字。空白にしておくと、現在使用されている最大シーケンス番号より 5 大きいシーケンス番号がデフォルトになります。
IPアドレス	プレフィックス番号をIPアドレス/マスク長の形式で指定します。
プレフィックスの最小長（Minimum Prefix Length）	（任意）プレフィックスの最小長を入力します。 値は、最大プレフィックス長の値が指定されている場合に、マスク長以上、最大プレフィックス長以下でなければなりません。
プレフィックスの最大長（Maximum Prefix Length）	（任意）プレフィックスの最大長を入力します。 値は、最小プレフィックス長の値が指定されている場合に、最小プレフィックス長以上、最小プレフィックス長の値が指定されていない場合に、マスク長以上でなければなりません。

[プレフィックスリストIPv6オブジェクトの追加または編集（AddorEdit Prefix List IPv6 Object）] ダイアログボックス

[プレフィックスリストIPv6オブジェクトの追加/編集（Add or Edit Prefix List IPv6 Object）] ダイアログボックスを使用して、IPv6 プレフィックスリスト のポリシーオブジェクトを作成、コピー、および編集します。ルートマップ（ルートマップオブジェクトについて （214 ページ）を参照）、ポリシーマップ（[ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス （230 ページ）を参照）、OSPF フィルタリング（[Add Filtering]/[Edit Filtering] ダイアログボックス （155 ページ）を参照）または BGP ネイバーフィルタリング（[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （36 ページ）を参照）を設定するときに使用する、IPv6 プレフィックス リスト オブジェクトを作成できます。

エリア境界ルータ（ABR）のタイプ 3 リンクステートアドバタイズメント（LSA）フィルタリングは、OSPF を実行している ABR の機能を拡張して、異なる OSPF エリア間のタイプ 3 LSA をフィルタリングします。プレフィックス リストが設定されているときは、指定されたプレフィックスのみが OSPF エリア間で送信されます。その他のすべてのプレフィックスは、それぞれの OSPF エリアに制限されます。このタイプのエリア フィルタリングは、OSPF エリアを

出入りするトラフィックに対して、またはそのエリアの着信と発信の両方のトラフィックに対して適用できます。

プレフィックスリストの複数のエントリが指定されたプレフィックスと一致する場合、シーケンス番号が最も小さいエントリが使用されます。効率性を高めるため、頻繁に一致するエントリまたは一致しないエントリに、小さいシーケンス番号を手動で割り当てることで、それらをリストの上部に配置することもできます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次に、オブジェクトタイプセレクタから [プレフィックスリストIPv6（Prefix ListIPv6）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- [プレフィックスリストエントリの追加または編集（Add or Edit Prefix List Entry）] ダイアログボックス （237 ページ）
- ルートマップオブジェクトについて （214 ページ）
- [ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス （230 ページ）
- Policy Object Manager
- ポリシーのオブジェクトの選択
- ポリシー オブジェクトの作成
- オブジェクトの編集
- カテゴリ オブジェクトの使用
- オブジェクト オーバーライドの管理
- ポリシー オブジェクトの上書きの許可

フィールド リファレンス

表 *110 : [IPv6*プレフィックスリストオブジェクトの追加/編集（*Add/Edit IPv6 Prefix List Object*）*]* ダイアログボックス

要素	説明
名前	IPv6プレフィックス リスト オブジェクト名、最大 128 文字。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成を参照してください。 **注意** Cisco Security Manager では、デバイスで名前を変更できない場合でもオブジェクトの名前を変更できます。Cisco Security Manager でこれらのオブジェクトの名前を変更する場合、既存の CLI を無効にして、新しい CLI を発行し、新しい名前を使用してオブジェクトを作成して割り当てることで名前を変更します。この最初の無効化により、環境内でルーティングやネットワークの問題を引き起こす可能性があります。オブジェクトの名前を変更しても、Security Manager はこれらの結果に関する警告メッセージを表示しません。
説明	（任意）オブジェクトの説明。
IPv6 プレフィックス リスト テーブル	オブジェクトで定義されている IPv6 プレフィックス リスト エントリ。 • IPv6 プレフィックス リスト エントリを追加するには、[追加（Add）] ボタンをクリックして [IPv6プレフィックスリストエントリの追加または編集（Add or Edit IPv6 Prefix List Entry）] ダイアログボックス（241 ページ）を開きます。 • IPv6 プレフィックス リスト エントリを編集するには、エントリを選択し、[編集（Edit）] ボタンをクリックします。 • IPv6 プレフィックス リスト エントリを削除するには、エントリを選択し、[削除（Delete）] ボタンをクリックします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[IPv6プレフィックスリストエントリの追加または編集（Add or Edit IPv6 Prefix List Entry）] ダイアログボックス

[IPv6プレフィックスリストエントリの追加または編集（Add/Edit IPv6 Prefix List Entry）] ダイアログボックスを使用して、新しい IPv6 プレフィックス リスト エントリを作成するか、既存のエントリを編集します。

ナビゲーション パス

[IPv6プレフィックスリストエントリの追加または編集（Add or Edit IPv6 Prefix List Entry）] ダイアログボックス （241 ページ）で、[プレフィックスリスト（Prefix Listt）] テーブルの下にある [追加（Add）] ボタンをクリックするか、またはテーブル内のエントリを選択して [編集（Edit）] ボタンをクリックします。

フィールド リファレンス

表 *111 : [プレフィックスリストエントリの追加または編集（Add/Edit Prefix List Entry）] ダイアログボックス*

要素	説明
操作	[許可（Permit）] または [拒否（Deny）] オプションボタンをクリックして再配布アクセスを指定します。
シーケンス No（Sequence No）	（任意）このオブジェクトですでに設定されている IPv6 プレフィックス リスト エントリのリストにおける、新しい IPv6 プレフィックス リスト エントリの位置を示す固有の数字。空白にしておくと、現在使用されている最大シーケンス番号より 5 大きいシーケンス番号がデフォルトになります。 （注） シーケンス番号は 1 から 4294967295 の範囲で指定する必要があります。
IPv6 アドレス	プレフィックス番号は、IPv6 アドレス/マスク長の形式で指定します。マスク長は 128 以下です。
プレフィックスの最小長（Minimum Prefix Length）	（任意）プレフィックスの最小長を 1 ～ 128 の範囲で入力します。 値は、最大プレフィックス長の値が指定されている場合に、マスク長以上、最大プレフィックス長以下でなければなりません。
プレフィックスの最大長（Maximum Prefix Length）	（任意）プレフィックスの最大長を 1 ～ 128 の範囲で入力します。 値は、最小プレフィックス長の値が指定されている場合に、最小プレフィックス長以上、最小プレフィックス長の値が指定されていない場合に、マスク長以上でなければなりません。

[ASパスオブジェクトの追加（（Add AS Path Object））]/[ASパスオブジェクトの編集（Edit AS Path Object）] ダイアログボックス

[ASパスオブジェクトの追加（（Add AS Path Object））]/[ASパスオブジェクトの編集（Edit AS Path Object）] ダイアログボックスを使用して、自律システム（AS）パスのポリシーオブジェクトを作成、コピー、編集します。ルートマップ（ルートマップオブジェクトについて （214 ページ）を参照）、ポリシーマップ（[ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス （230 ページ）を参照）、またはBGP ネイバーフィルタリング（[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （16 ページ）を参照）を設定するときに使用する、AS パスオブジェクトを作成できます。

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。

（注） AS パスオブジェクト名は、1 ～ 500 の一意の整数である必要があります。既存の AS パスオブジェクトと同じ名前を使用するデバイスまたは構成ファイルから AS パスオブジェクトが検出された場合、Security Manager の [検出されたポリシーオブジェクトに対するデバイスのオーバーライドを許可（Allow Device Override for Discovered Policy Objects）] 設定（[Security Manager 管理（Security Manager Administration）] > [検出（Discovery）] ページ）に関係なく、Security Manager の AS パスオブジェクトは上書きされます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [ASパス（AS Path）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- [パス エントリとして追加または編集] ダイアログボックス （244 ページ）
- ルートマップオブジェクトについて （214 ページ）
- [ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス （230 ページ）
- Policy Object Manager
- ポリシーのオブジェクトの選択
- ポリシー オブジェクトの作成
- オブジェクトの編集

- カテゴリ オブジェクトの使用
- オブジェクト オーバーライドの管理
- ポリシー オブジェクトの上書きの許可

フィールド リファレンス

表 *112 : [AS*パスオブジェクトの追加（（*Add AS Path Object*））*]/[AS*パスオブジェクトの編集（*Edit AS Path Object*）*]* ダイアログボックス

要素	説明
名前	AS パスフィルタの名前を入力します。1 ～ 500 の一意の値を指定します。
説明	（任意）オブジェクトの説明。
[ASパス（AS Path）] テーブル	オブジェクトで定義されている AS パスエントリ。 • AS パスエントリを追加するには、[追加（Add）] ボタンをクリックして、[パス エントリとして追加または編集] ダイアログボックス （244 ページ）を開きます。 • AS パスエントリを編集するには、エントリを選択し、[編集（Edit）] ボタンをクリックします。 • AS パスエントリを削除するには、エントリを選択し、[削除（Delete）] ボタンをクリックします。 • エントリを並べ替えるには、エントリを選択してから、[上へ移動（Move Up）] または [下へ移動（Move Down）] ボタンをクリックします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[パス エントリとして追加または編集] ダイアログボックス

[ASパスエントリの追加（Add As Path Entry）]/[ASパスエントリの編集（Edit As Path Entry）] ダイアログボックスを使用して、新しい自立システム（AS）パスエントリを作成するか、既存のエントリを編集します。

ナビゲーション パス

[ASパスオブジェクトの追加（（Add AS Path Object））]/[ASパスオブジェクトの編集（Edit AS Path Object）] ダイアログボックス （242 ページ）で、[ASパス（As Path）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、エントリを選択して [行の編集（Edit Row）] ボタンをクリックします。

フィールド リファレンス

表 *113 : [AS*パスエントリの追加（*Add As Path Entry***）***]/[AS*パスエントリの編集（***Edit As Path Entry***）***]*ダイアログボックス**

要素	説明
操作	[許可（Permit）] または [拒否（Deny）] オプションボタンをクリックして再配布アクセスを指定します。
正規表現（Reg Exp）	AS パスフィルタを定義する正規表現を指定します。正規表現の作成に使用できるメタ文字の詳細については、正規表現の作成に使用されるメタ文字を参照してください。

[コミュニティリストオブジェクトの追加または編集（Add or Edit Community List Object）] ダイアログボックス

[プレフィックスリストオブジェクトの追加/編集（Add/Edit Prefix List Object）] ダイアログボックスを使用して、プレフィックスリストのポリシーオブジェクトを作成、コピー、および編集します。ルートマップ（ルートマップオブジェクトについて （214 ページ）を参照）またはポリシーマップ（[ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス （230 ページ）を参照）を設定するときに使用する、コミュニティ リスト ポリシー オブジェクトを作成できます。

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。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）] を選択し、次に、オブジェクト タイプセレクタから [コミュニティリスト（Community List）] を選択します。作業領域内を右

クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- [コミュニティ リスト エントリの追加または編集] ダイアログボックス （246 ページ）
- ルートマップオブジェクトについて （214 ページ）
- [ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス （230 ページ）
- Policy Object Manager
- ポリシーのオブジェクトの選択
- ポリシー オブジェクトの作成
- オブジェクトの編集
- カテゴリ オブジェクトの使用
- オブジェクト オーバーライドの管理
- ポリシー オブジェクトの上書きの許可

フィールド リファレンス

表 *114 : [コミュニティリストオブジェクトの追加/編集（Add/Edit Community List Object）] ダイアログボックス*

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成を参照してください。
説明	（任意）オブジェクトの説明。

要素	説明
[コミュニティリスト（Community List）] テーブル	オブジェクトで定義されているコミュニティリストエントリ。 • コミュニティリストエントリを追加するには、[追加（Add）] ボタンをクリックして、[コミュニティ リスト エントリの追加または編集] ダイアログボックス （246 ページ）を開きます。 • コミュニティリストエントリを編集するには、エントリを選択し、[編集（Edit）] ボタンをクリックします。 • コミュニティリストエントリを削除するには、エントリを選択し、[削除（Delete）] ボタンをクリックします。 • エントリを並べ替えるには、エントリを選択してから、[上へ移動（Move Up）] または [下へ移動（Move Down）] ボタンをクリックします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[コミュニティ リスト エントリの追加または編集] ダイアログボックス

[コミュニティリストエントリの追加/編集（Add/Edit Community List Entry）] ダイアログボックスを使用して、新しいコミュニティ リスト エントリを作成するか、既存のエントリを編集します。

ナビゲーション パス

[コミュニティリストオブジェクトの追加または編集（Add or Edit Community List Object）] ダイアログボックス （244 ページ）で、[コミュニティリスト（Community List）] テーブルの下にある [追加（Add）] ボタンをクリックするか、テーブル内のエントリを選択して [編集（Edit）] ボタンをクリックします。

フィールド リファレンス

表 *115 : [*コミュニティリストエントリの追加/編集（*Add/Edit Community List Entry*）*]* ダイアログボックス

要素	説明
タイプ	[標準（Standard）] または [拡張（Expanded）] オプションボタンを選択して、コミュニティルールの種類を表示します。 （注） 標準を使用したエントリ、コミュニティ ルールの拡張種類を使用したエントリを、同じコミュニティ リスト オブジェクトに含めることはできません。
操作	[許可（Permit）] または [拒否（Deny）] オプションボタンをクリックして再配布アクセスを指定します。
コミュニティ（Communities）	コミュニティ番号を指定します。有効な値は 1 ～ 4294967295 または 0:1 ～ 65534:65535 です。
internet	インターネットのウェルノウンコミュニティを指定するには、これを選択します。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。
no-advertise	非アドバタイズのウェルノウンコミュニティを指定するには、これを選択します。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。
no-export	非エクスポートのウェルノウンコミュニティを指定するには、これを選択します。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。
式	拡張コミュニティリストの場合は、正規表現を指定します。正規表現の作成に使用できるメタ文字の詳細については、正規表現の作成に使用されるメタ文字を参照してください。

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。