

# IS-IS

この章では、Intermediate System to Intermediate System（IS-IS）ルーティング プロトコルについて説明します。


- IS-IS について （1 ページ）
- IS-IS の前提条件 （8 ページ）
- IS-IS のガイドライン （8 ページ）
- IS-IS の設定 （9 ページ）
- IS-IS の監視 （28 ページ）
- IS-IS の履歴 （29 ページ）


## IS-IS について

IS-IS ルーティング プロトコルはリンクステート内部ゲートウェイ プロトコル（IGP）です。リンクステートプロトコルは、各参加デバイス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。IS-IS の実装は、IPv4 と IPv6 をサポートします。

ルーティング ドメインを 1 つ以上のサブドメインに分割することができます。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。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できます。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。

## NET について

IS は ネットワーク エンティティ タイトル（NET）と呼ばれるアドレスで識別されます。NET はネットワーク サービス アクセスポイント（NSAP）のアドレスで、これにより IS で動作す

る IS-IS ルーティング プロトコルのインスタンスを識別できます。NET は、長さが 8 ～ 20 オクテットで、次の 3 つの部分にわかれています。

- エリア アドレス：このフィールドは 1 ～ 13 オクテット長で、アドレスの上位のオクテットで構成されます。

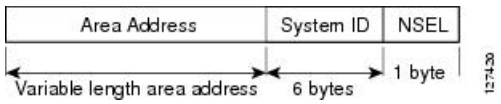
（注） IS-IS インスタンスに複数のエリア アドレスを割り当てることができます。その場合、すべてのエリアアドレスが同義と見なされます。複数の同義エリアアドレスは、ドメインでエリアをマージまたは分割するときに役立ちます。マージまたは分割が完了した後は、複数のエリア アドレスを IS-IS インスタンスに割り当てる必要はありません。

- システム ID：このフィールドは 6 オクテット長で、エリア アドレスの直後に続きます。IS がレベル 1 で動作する場合、システム ID は、同じエリア内のすべてのレベル 1 デバイス間で一意である必要があります。IS がレベル 2 で動作する場合、システム ID は、ドメイン内のすべてのデバイス間で一意である必要があります。

（注） 1 つの IS インスタンスに 1 つのシステム ID を割り当てます。

- NSEL：この N セレクタ フィールドは 1 オクテット長で、システム ID の直後に続きます。このフィールドは 00 に設定する必要があります。

**図 *1: NET* の形式**




# IS-IS ダイナミック ホスト名

IS-IS ルーティング ドメインでは、各 ASA はシステム ID により表されます。システム ID は、IS-IS ASA ごと構成されている NET の一部です。たとえば、NET 49.0001.0023.0003.000a.00 が設定されている ASA のシステム ID が 0023.0003.000a であるとします。ネットワーク管理者にとって、ASA でのメンテナンスやトラブルシューティングの間、ASA 名とシステム ID の対応を覚えているのは難しいことです。

ダイナミック ホスト名メカニズムはリンクステート プロトコル（LSP）フラッディングを使用して、ネットワーク全体に ASA 名に対するシステム ID のマッピング情報を配布します。ネットワーク上の ASA はすべて、このシステム ID に対する ASA 名のマッピング情報をルーティング テーブルにインストールしようと試みます。

ネットワーク上で、ダイナミック名のタイプ、長さ、値（TLV）をアドバタイズしている ASA が突然、アドバタイズメントを停止した場合、最後に受信されたマッピング情報が最大 1 時

間、ダイナミック ホスト マッピング テーブルに残るため、ネットワークに問題が発生している間、ネットワーク管理者はマッピング テーブル内のエントリを表示できます。

# IS-IS での PDU のタイプ

IS では、プロトコル データ ユニット（PDU）を使用してルーティング情報をピアと交換します。PDU の中間システム相互間 Hello PDU（IIH）、リンク状態 PDU（LSP）、およびシーケンス番号 PDU（SNP）タイプが使用されます。

**IIH**

IIH は、IS-IS プロトコルが有効になっている回線の IS ネイバー間で交換されます。IIH には、送信者のシステム ID、割り当てられたエリア アドレス、送信 IS に認識されているその回線上のネイバーのアイデンティティが含まれます。追加のオプションの情報が含まれる場合もあります。

IIH には、次の 2 種類があります。

- レベル 1 LAN IIH：これらは、マルチアクセス回線において、送信 IS がその回線でレベル 1 デバイスとして動作する場合に送信されます。
- レベル 2 LAN IIH：これらは、マルチアクセス回線において、送信 IS がその回線でレベル 2 デバイスとして動作する場合に送信されます。

**LSP**

IS では LSP を生成して、そのネイバーや IS に直接接続されている接続先をアドバタイズします。LSP は、以下のものによって一意に識別できます。

- LSP を生成した IS のシステム ID。
- Pseudonode ID：この値は LSP が pseudonode LSP の場合を除き、常に 0 です
- LSP 番号（0 ～ 255）
- 32 ビットのシーケンス番号

LSP の新しいバージョンが生成されるたびに、シーケンス番号が増加します。

レベル 1 の LSP は、レベル 1 をサポートしている ISで生成されます。レベル 1 の LSP はレベル 1 のエリア全体にフラッディングされます。エリア内のすべてのレベル 1 の IS で生成されたレベル 1 の LSP のセットは、レベル 1 LSP データベース（LSPDB）となります。エリア内のすべてのレベル 1 の IS は同一のレベル 1 の LSPDB を持ちます。したがって、そのエリアの同一のネットワーク接続マップを持つことになります。

レベル 2 の LSP は、レベル 2 をサポートしている ISで生成されます。レベル 2 の LSP は、レベル 2 のサブドメイン全体にフラッディングされます。ドメイン内のすべてのレベル 2 の IS で生成されたレベル 2 の LSP のセットは、レベル 2 LSP データベース（LSPDB）となります。すべてのレベル 2 の IS は同一のレベル 2 の LSPDB を持ちます。したがって、そのレベル 2 のサブドメインの同一の接続マップを持つことになります。

**SNP**

SNP には、1 つ以上の LSP のサマリー説明が含まれます。レベル 1 とレベル 2 の両方について、次の 2 つのタイプの SNP があります。

- Complete Sequence Number PDU（CSNP）は、特定のレベルに関して IS が持つ LSPDB のサマリを送信するために使用されます。
- Partial Sequence Number PDU（PSNP）は、IS がそのデータベースに持つか取得する必要がある特定のレベルに関する LSP のサブセットのサマリを送信するために使用されます。

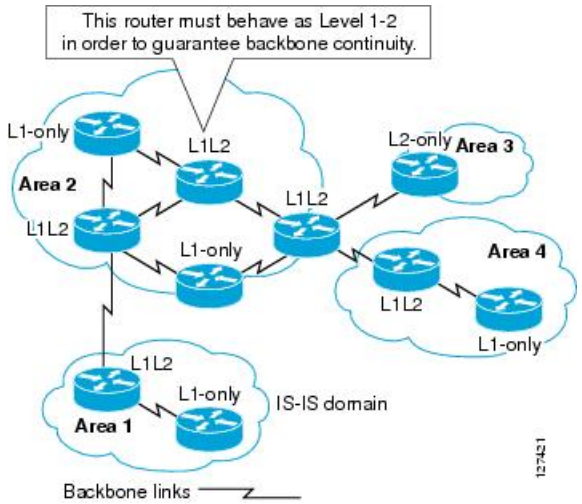
# マルチアクセス回線での IS-IS の動作

マルチアクセス回線では複数の IS がサポートされます。つまり、回線で 2 つ以上の IS が動作します。マルチアクセス回線で必要な前提条件は、マルチキャスト アドレスまたはブロードキャスト アドレスを使用して複数のシステムのアドレスを指定できることです。マルチアクセス回線でレベル 1 をサポートする IS は、レベル 1 の LAN IIH を回線上に送信します。マルチアクセス回線でレベル 2 をサポートする IS は、レベル 2 の LAN IIH を回線上に送信します。IS は、回線上でネイバー IS とレベルごとに別々の隣接関係（アジャセンシー）を形成します。

IS は回線上でレベル 1 をサポートする他の IS とレベル 1 の隣接関係（アジャセンシー）を形成し、同じエリア アドレスを持ちます。同一マルチアクセス回線上で、レベル 1 をサポートするエリア アドレスの整合性のないセットを持つ 2 つの IS は、サポートされていません。IS は回線上でレベル 2 をサポートする他の IS とレベル 2 の隣接関係（アジャセンシー）を形成します。

以下の図の IS-IS のネットワーク トポロジ内のデバイスは、ネットワークのバックボーンに従って、レベル 1、レベル 2、またはレベル 1 と 2 のルーティングを実行します。

**図 *2 : IS-IS* ネットワーク トポロジにおけるレベル *1*、レベル *2*、レベル *1-2* デバイス**



# IS-IS での代表 IS の選択

各 IS が LSP 内のマルチアクセス回線上のすべての隣接関係をアドバタイズする場合、必要なアドバタイズメントの総数は N 2 になります。ここで、N は回線の特定のレベルで動作している IS の数です。この拡張性の問題を解消するため、IS-IS ではマルチアクセス回線を表す擬似ノードを定義します。特定のレベルで動作するすべての IS が、その回線の代表中継システム（DIS）として機能するように IS のいずれかを選定します。DIS は、回線でアクティブな各レベルごとに選定されます。

DIS は擬似ノード LSP を発行する責任を担います。擬似ノード LSP には、その回線で動作するすべての IS のネイバー アドバタイズメントが含まれます。その回線で動作するすべての IS（DIS を含む）が非擬似ノード LSP 内の擬似ノードにネイバーアドバタイズメントを提供し、マルチアクセス回線上のネイバーはアドバタイズしません。このように、必要なアドバタイズメントの総数は、N（回線で動作する IS の数）に応じて変わります。

擬似ノード LSP は次の ID によって一意に分類されます。

- LSP を生成した DIS のシステム ID
- Pseudonode ID（常にゼロ以外）
- LSP 番号（0 ～ 255）
- 32 ビットのシーケンス番号

ゼロ以外の擬似ノード ID は、擬似ノード LSP と擬似ノード以外の LSP を区別するもので、このレベルでも DIS である場合に、他の LAN 回線の間で一意になるように、DIS によって選択されます。

また、DIS は回線上に定期的な CSNP を送信する責任も担っています。これは、DIS 上の LSPDB の現在のコンテンツに関する完全な要約説明を提供します。回線上の他の IS が次のアクティビティを実行できます。これにより、マルチアクセス回線上のすべての IS の LSPDB が効率的かつ確実に同期されます。

- DIS によって送信された CSNP に存在しない LSP、またはその CSNP に記述された LSP より新しい LSP をフラッディングします。
- ローカル データベースに存在しない DIS によって送信された CSNP セットに記述されている LSP、または CSNP セットに記述されている LSP より古い LSP の PSNP を送信することで、LSP を要求します。

# IS-IS LSPDB の同期

IS-IS を適切に動作させるには、各 IS 上の LSPDB を同期するため信頼性の高い効率的なプロセスが必要です。IS-IS では、このプロセスは更新プロセスと呼ばれます。更新プロセスは、各サポート レベルで独立して動作します。ローカルに生成される LSP は常に新しい LSP です。回線上のネイバーから受信した LSP は、他の IS によって生成されているか、またはローカル IS によって生成された LSP のコピーであることがあります。受信した LSP はローカル LSPDB の現在のコンテンツに比べ、古い、同じ、または新しい場合があります。

### 新しい LSP の処理

ローカル LSPDB に追加された新しい LSP は、LSPDB の同じ LSP の古いコピーを置き換えます。新しい LSP は、新しい LSP を受信した回線を除き、IS が現在、新しい LSP に関連付けられているレベルでアップ状態の隣接関係（アジャセンシー）を持つすべての回線に送信されるようにマークされます。

マルチアクセス回線では、IS は新しい LSP を 1 回フラッディングします。IS は、マルチアクセス回線用に DIS によって定期的に送信される一連の CNSP を調べます。ローカル LSPDB に CSNP セットに記述されている LSP より新しい LSP が 1 つ以上含まれている場合は（これには CSNP セットに存在しない LSP も含まれる）、それらの LSP がマルチアクセス回線経由で再度フラッディングされます。ローカル LSPDB に CSNP セットに記述された LSP より古い LSP が 1 つ以上含まれる場合は（これには、ローカル LSPDB に存在しない CSNP セットに記述された LSP も含まれる）、更新が必要な LSP の記述とともに PSNP がマルチアクセス回線上に送信されます。マルチアクセス回線の DIS は、要求された LSP を送信することで応答します。

### 古い LSP の処理

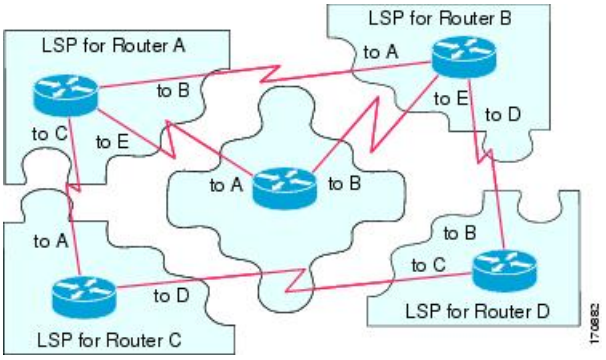
IS でローカルの LSPDB のコピーよりも古い LSP を受信する場合があります。また IS でローカルの LSPDB のコピーよりも古い LSP について説明する SNP（全体または一部）を LSPDB 受信する場合もあります。いずれの場合も、IS によってローカル データベースでその LSP がマークされ、古い LSP が含まれている古い LSP または SNP が受信された回線にフラッディングされます。実行されるアクションは、前述の新しい LSP がローカルデータベースに追加された後のアクションと同じです。

### 経過期間が同じ LSP の処理

更新プロセスの分散型の特性のため、IS がローカル LSPDB の現在のコンテンツと同じ LSP のコピーを受信する可能性があります。マルチアクセス回線では、経過期間が同じ LSP の受信は無視されます。回線の DIS によって設定された CSNP が定期的に送信され、LSP を受信した送信者への明示的な確認応答の役割を果たします。

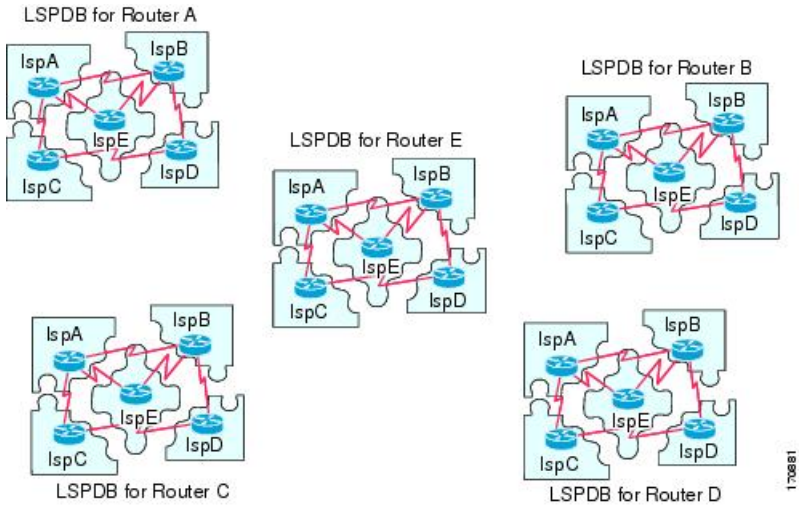
次の図は、LSP を使用してネットワーク マップを作成する方法を示しています。ネットワークトポロジをジグソー パズルとして想像してください。各 LSP（IS を表す）はジグソー パズルの 1 つのピースに相当します。エリア内のすべてのレベル 1 デバイスまたはレベル 2 サブドメイン内のすべてのレベル 2 デバイスに適用されます。

**図 *3 : IS-IS* ネットワーク マップ**



次の図は、ネイバー デバイス間で隣接関係（アジャセンシー）が形成された後に、IS-IS ネットワーク内の各デバイスが完全に更新されたリンクステートデバイスを備えていることを示しています。エリア内のすべてのレベル 1 デバイスまたはレベル 2 サブドメイン内のすべてのレベル 2 デバイスに適用されます。

**図 *4 : LSPDB* が同期された *IS-IS* デバイス**




# IS-IS 最短パスの計算

LSPDB のコンテンツが変更されると、各 IS は独立して最短パスの計算を再実行します。アルゴリズムは、有向グラフに沿って最短パスを見つけるためのよく知られたダイクストラアルゴリズムに基づいています。有向グラフでは、各 IS がグラフの頂点で、IS 間のリンクが非負の重みを持つエッジとなります。2 つの IS 間のリンクをグラフの一部として見なす前に、双方向接続チェックが実行されます。これによって、たとえば、1 つの IS がすでにネットワーク内で動作していないが、動作を停止する前に、生成した LSP セットを消去しなかった場合などに、LSPDB 内で古い情報が使用されるのを防ぎます。

SPF の出力は、一連のタプル（宛先、ネクストホップ）です。宛先は、プロトコルによって異なります。複数のネクスト ホップが同じ宛先に関連付けられている場合は、複数の等コストパスがサポートされます。

IS によってサポートされているレベルごとに、独立した SPF が実行されます。同じ宛先がレベル 1 パスとレベル 2 パスの両方によって到達可能な場合は、レベル 1 パスが優先されます。

他のエリアに 1 つ以上のレベル 2 ネイバーを持つことを示しているレベル 2 IS は、デフォルトルートとも呼ばれる、ラストリゾートのパスとして同じエリア内のレベル 1 デバイスによって使用される場合があります。レベル 2 IS は、レベル 1 LSP 0 に ATT（Attached）bit を設定することで、他のエリアへのアタッチメントを示します。

（注） IS は、各レベルで最大 256 の LSP を生成できます。LSP は、0 ～ 255 の番号によって識別されます。LSP 0 は、他のエリアへのアタッチメントを示すための ATT ビットの設定の意味を含め、特別なプロパティを備えています。番号 1 ~ 255 の LSP に ATT ビットが設定されている場合は、それに意味はありません。

## IS-IS シャットダウン プロトコル

IS-IS をシャットダウンする（管理上のダウン状態にする）ことで、設定パラメータを失うことなく IS-IS プロトコル設定に変更を加えることができます。グローバル IS-IS プロセス レベルまたはインターフェイス レベルで IS-IS をシャットダウンできます。プロトコルがオフになっているときにデバイスが再起動すると、プロトコルは、通常、ディセーブル状態でアップします。プロトコルが管理上のダウン状態に設定されている場合、ネットワーク管理者は、プロトコル設定を失うことなく IS-IS プロトコルを管理上オフにし、中間状態（多くの場合、望ましくない状態）を経てプロトコルの動作を遷移させることなくプロトコル設定に一連の変更を加え、適切なタイミングでプロトコルを再度イネーブルにすることができます。

# IS-IS の前提条件

IS-IS を設定する前に、次の前提条件を満たしている必要があります。

- IPv4 および IPv6 を理解していること。
- IS-IS を設定する前にネットワーク設計およびそれを経由するトラフィックのフロー方法を理解していること。
- エリアを定義し、デバイスのアドレッシング計画を準備し（NET の定義を含む）、IS-IS を実行するインターフェイスを決定していること。
- デバイスを設定する前に、隣接関係テーブルに表示されるネイバーを示す隣接関係のマトリックスを準備しておくこと。これにより検証が容易になります。

# IS-IS のガイドライン

### ファイアウォール モードのガイドライン

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

### クラスタのガイドライン

個別インターフェイスモードでのみサポート：スパンド EtherChannel モードはサポートされません。

### その他のガイドライン

双方向転送で、IS-IS はサポートされていません。

# IS-IS の設定

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

### 手順

**ステップ 1** IS-IS ルーティングのグローバルな有効化 （9 ページ）。
**ステップ 2** IS-IS 認証の有効化 （11 ページ）。
**ステップ 3** IS-IS LSP の設定 （12 ページ）
**ステップ 4** IS-IS サマリー アドレスの設定 （14 ページ）。
**ステップ 5** IS-IS NET の設定 （15 ページ）。
**ステップ 6** IS-IS パッシブ インターフェイスの設定 （16 ページ）。
**ステップ 7** IS-IS インターフェイスの設定 （17 ページ）。
**ステップ 8** IS-IS IPv4 アドレス ファミリの設定 （21 ページ）。
**ステップ 9** IS-IS IPv6 アドレス ファミリの設定 （25 ページ）。

# IS-IS ルーティングのグローバルな有効化

### 始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

### 手順

**ステップ 1** **[Configuration]** > **[Device Setup]** > **[Routing]** > **[ISIS]** > **[General]** を選択します。
**ステップ 2** [Configure ISIS] チェックボックスをオンにして、IS-IS を有効にします。
**ステップ 3** [Shutdown protocol] チェックボックスをオンにして、シャットダウン プロトコルを有効にします。

シャットダウン プロトコルの詳細については、IS-IS シャットダウン プロトコル （8 ページ）を参照してください。

**ステップ 4** IS-IS でダイナミック ホスト名が使用されるようにするには、[Use dynamic hostname] チェックボックスをオンにします。

デフォルトでは、ダイナミック ホスト名は有効です。IS-IS のダイナミック ホスト名の詳細については、IS-IS ダイナミック ホスト名 （2 ページ）を参照してください。

**ステップ 5** IS-IS で LAN hello PDU のパディングが行われないようにするには、[Do not pad LAN hello PDUs] チェックボックスをオンにします。

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。これにより、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。hello パディングを無効にして、両方のインターフェイスの MTU が同じである場合や、トランスレーショナル ブリッジングの場合に、ネットワーク帯域幅が浪費されないようにすることができます。

**ステップ 6** パッシブ インターフェイスのみをアドバタイズするには、[Advertise passive only] チェックボックスをオンにします。

これにより、接続されているネットワークの IP プレフィックスが LSP アドバタイズメントから除外され、IS-IS コンバージェンス時間が短縮されます。

**ステップ 7** 該当するオプション ボタンをクリックして、ASA がステーション ルータ（レベル 1）、エリア ルータ（レベル 2）、またはその両方（レベル 1-2）のいずれとして動作するかを選択します。

IS-IS レベルの詳細については、IS-IS について （1 ページ）を参照してください。

**ステップ 8** [Topology priority] フィールドに、トポロジ内での ASA のプライオリティを示す数値を入力します。指定できる範囲は 0 ～ 127 です。

**ステップ 9** [Route priority tag] フィールドに、ASA のルート プライオリティを示すタグを入力します。範囲は 1 ～ 4294967295 です。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、IS-IS システム内のすべてのルータに送信されます。

**ステップ 10** 条件に応じて IS が L2 としてアドバタイズするように設定するには、ドロップダウン メニューからデバイスを選択し、[Manage] をクリックします。

ルート マップの追加手順は、ルート マップの定義を参照してください。

**ステップ 11** [Log changes in adjacency] チェックボックスをオンにすると、IS-IS ネイバーがアップ状態またはダウン状態になるたびに ASA によってログ メッセージが送信されるようになります。

このコマンドは、デフォルトでディセーブルになっています。隣接関係（アジャセンシー）の変更をロギングすると、大規模なネットワークをモニタリングする際に役立ちます。

**ステップ 12** 非 IIH イベントからの変更を含めるには、[Include changes generated by non-IIH events] チェックボックスをオンにします。

**ステップ 13** 懐疑的な時間間隔を設定するには、[Skeptical interval] フィールドに時間（分単位）を入力します。指定できる範囲は 0 ～ 1440 分です。デフォルトは 5 分です。

**ステップ 14** [Apply] をクリックします。

# IS-IS 認証の有効化

IS-IS ルート認証により、未承認の送信元から不正なルーティング メッセージまたは誤ったルーティング メッセージを受信することが防止されます。各 IS-IS エリアまたはドメインにパスワードを設定することで、不正なルータが誤ったルーティング情報をリンクステート データベースに挿入することを阻止できます。あるいは IS-IS 認証タイプ（IS-IS MD5 認証または拡張クリアテキスト認証）を設定できます。インターフェイスごとに認証を設定することもできます。IS-IS メッセージ認証対象として設定されたインターフェイス上にあるすべての IS-IS ネイバーには、隣接関係を確立できるように同じ認証モードとキーを設定する必要があります。

エリアとドメインの詳細については、IS-IS について （1 ページ）を参照してください。

### 始める前に

IS-IS のルート認証を有効にするには、予め IS-IS を有効にしてエリアを設定しておく必要があります。手順については、IS-IS ルーティングのグローバルな有効化 （9 ページ）を参照してください。

### 手順

**ステップ 1** **[Configuration]** > **[Device Setup]** > **[Routing]** > **[ISIS]** > **[Authentication]** の順に選択します。

**ステップ 2** レベル 1 とレベル 2 の認証パラメータを設定します。

- [Key] フィールドに、IS-IS 更新を認証するキーを入力します。このキーの最大長は 16 文字です。
- [Send Only] を有効にするかどうかに応じて、[Enable] または [Disable] オプションボタンをクリックします。

（注） 送信されるパケットだけに認証が挿入され、受信されるパケットではチェックされない場合、各 ASA で、キーの設定に費やせる時間が長くなります。

- 認証モードを選択するため、[Disabled]、[MD5]、[Plaintext] オプションボタンのいずれかをオンにします。

**ステップ 3** [Disabled] をオンにした場合は、レベル 1 エリア（サブドメイン）のエリア パスワードと、レベル 2 ドメインのドメイン パスワードのいずれかまたは両方を入力します。

**ステップ 4** [適用（Apply）] をクリックします。

# IS-IS LSP の設定

IS では LSP を生成して、そのネイバーや IS に直接接続されている接続先をアドバタイズします。LSP の詳細については、IS-IS での PDU のタイプ （3 ページ）を参照してください。

高速コンバージェンス設定となるように LSP を設定するには、次のコマンドを使用します。

### 始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

### 手順

**ステップ 1** **[Configuration ] > [ Device Setup] > [Routing ] > [ISIS] > [Link State Packet]** の順に選択します。

（注） IS-IS を設定する前に LSP パラメータを設定しておく必要があります。手順については、IS-IS ルーティングのグローバルな有効化 （9 ページ）を参照してください。

**ステップ 2** 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するには、[Ignore LSP errors] チェック ボックスをオンにしてください。

**ステップ 3** SPF 実行の前に LSP の高速フラッディングを実行して埋めるには、[Flood LSPs before running SPF] をオンにし、[Number of LSPs to be flooded] フィールドに数値を入力します。指定できる範囲は 1 ～ 15 です。デフォルトは 5 分です。

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。

**ステップ 4** IP プレフィックスを抑制するには、[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:

- [Don't advertise IP prefixes learned form 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。
- [Don't advertise IP prefixes learned form other protocols when ran out of LSP fragments]：ASA 上の再配布ルールを抑制します。

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。

**ステップ 5** レベル 1 とレベル 2 の LSP 生成間隔を設定します。

- [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。

- [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。

- [Minimum wait between first and second LSP calculation]：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。

**ステップ 6** 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。

**ステップ 7** [Maximum LSP size] フィールドには、連続した 2 つの LSP 生成の間の最大秒数を入力します。指定できる範囲は 128 ～ 4352 です。デフォルトは 1492 です。

**ステップ 8** [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）。

**ステップ 9** [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 ～ 65,535 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。

**ステップ 10** [Apply] をクリックします。

# IS-IS サマリー アドレスの設定

複数のアドレス グループを特定のレベルに集約できます。他のルーティング プロトコルから学習したルートも集約できます。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。これにより、ルーティングテーブルのサイズを削減することができます。

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。

## 手順

**ステップ 1** **[Configuration]** > **[Device Setup]** > **[Routing]** > **[ISIS ]** > **[Summary Address]** の順に選択します。

[Configure ISIS Summary Address] ペインには、スタティックに定義された IS-IS サマリー アドレスのテーブルが表示されます。デフォルトでは、IS-IS はサブネット ルートをネットワーク レベルに集約します。[Configure ISIS Summary Address] ペインでは、サブネット レベルに集約されるスタティックに定義された IS-IS サマリー アドレスを作成できます。

**ステップ 2** 新しい IS-IS サマリー アドレスを追加するには [Add] をクリックし、テーブル内の既存の IS-IS サマリー アドレスを編集するには [Edit] をクリックします。

[Add Summary Address] または [Edit Summary Address] ダイアログボックスが表示されます。テーブルのエントリをダブルクリックして編集することもできます。

**ステップ 3** [IP Address] フィールドに、サマリー ルートの IP アドレスを入力します。

**ステップ 4** [Netmask] フィールドで、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。

**ステップ 5** 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。

- （オプション）[Level 1]：ルートをレベル 1 およびレベル 2 に再配布するとき、およびレベル 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したときに集約ルートが適用されます。
- （オプション）[Level 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はレベル 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。
- （オプション）[Level 1 and 2]：ルートをレベル 1 およびレベル 2 に再配布するとき、およびレベル 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したときに集約ルートが適用されます。

**ステップ 6** [Tag] フィールドに、タグの番号を入力します。指定できる範囲は 1 ～ 4294967295 です。

[Tag] フィールドには、集約するルートにタグ付けする番号を指定できます。**[Configuration]** > **[Device Setup]** > **[Routing]** > **[SIS]** > **[General]** ペインの [Route priority tag] フィールドですでにタグ付けされているルートは集約されます。集約されない場合、タグは失われます。

**ステップ 7** [Metric] フィールドに、集約ルートに適用するメトリックを入力します。指定できる範囲は 1 ～ 4294967295 です。デフォルト値は 10 です。

[Metric] の値はリンクに割り当てられ、宛先へのリンクを介したパス コストを計算するために使用されます。このメトリックは、レベル 1 またはレベル 2 ルーティングに対してだけ設定できます。

**ステップ 8** [OK] をクリックします。

**ステップ 9** [Apply] をクリックします。

# IS-IS NET の設定

### 始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

IS-IS は、Network Entity Title（NET）と呼ばれるアドレスを使用します。このアドレスの長さの範囲は 8 ～ 20 バイトですが、通常は 10 バイトです。ASA でクラスタリングが設定されていない場合に、[NET] ページで NET エントリを追加できます。ASA でクラスタリングが設定されている場合は、[Configuration] > [Device Management] > [Advanced] > [Address Pools] > [NET Address Pools] ペインで、net プール エントリを作成する必要があります。その後、[NET] ペインで NET アドレス プールを参照できます。

### 手順

**ステップ 1** **[Configuration]** > **[Device Setup]** > **[Routing]** > **[ISIS]** > **[Network Entity Title (NET)]** を選択します。

[Configure Network Entity (NET)] ペインに、NET アドレスのテーブルが表示されます。ASA でクラスタリングが設定されていない場合にはここで NET エントリを追加できます。クラスタリングが設定されている ASA の場合は、**[Configuration]** > **[Device Management]** > **[Advanced]** > **[Address Pools]** > **[Net Address Pools]** で net プール エントリを作成する必要があります。

その後、[Network Entity Title (NET) ] ペインで NET アドレス プールを参照できます。

**ステップ 2** 新しい IS-IS NET アドレスを追加するには [Add] をクリックし、テーブル内の既存の IS-IS NET アドレスを編集するには [Edit] をクリックします。

[Add Network Entity Title (NET)] または [Edit Network Entity Title (NET)] ダイアログボックスが表示されます。テーブルのエントリをダブルクリックして編集することもできます。

**ステップ 3** [Network Entity Title (NET)] ドロップダウンリストから NET を選択します。

**ステップ 4** [Maximum allowed Net] フィールドに、有効な NET の最大数を入力します。範囲は 3 ～ 254 です。デフォルトは 3 です。

ほとんどの場合、必要な NET は 1 つだけですが、複数のエリアをマージする場合や 1 つのエリアを複数のエリアに分割する場合には、複数のエリアアドレスを使用する必要がある可能性があります。

**ステップ 5** [Apply] をクリックします。

# IS-IS パッシブ インターフェイスの設定

トポロジ データベースにインターフェイス アドレスが含まれている間は、インターフェイス上で IS-IS hello パケットおよびルーティング アップデートを無効にできます。これらのインターフェイスは、IS-IS ネイバー隣接関係を形成しません。

IS-IS ルーティングに参加させたくないが、アドバタイズしたいネットワークに接続しているインターフェイスがある場合、インターフェイスが IS-IS を使用しないようにするため、パッシブ インターフェイスを設定します。さらに、ASA がアップデートのために使用する IS-IS のバージョンを指定することもできます。パッシブ ルーティングは、IS-IS 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 IS-IS ルーティング アップデートの送受信を無効にします。

### 手順

**ステップ 1** **[Configuration]** > **[Device Setup]** > **[Routing]** > **[IS-IS]** > **[Passive Interfaces]** の順に選択します。

**ステップ 2** すべてのインターフェイスでルーティング アップデートを抑止するには、[Suppress routing updates on all Interfaces] チェックボックスをオンにします。

これにより、すべてのインターフェイスがパッシブ モードで動作します。

**ステップ 3** ルーティング アップデートを抑止するように個別インターフェイスを設定するには、左側のカラムに示されているルーティング インターフェイスを選択し、[Add] をクリックしてそのインターフェイスを [Suppress routing updates] カラムに追加します。

1 つのインターフェイス名を指定すると、そのインターフェイスだけがパッシブ モードに設定されます。パッシブ モードでは、IS-IS ルーティング アップデートは、指定されたインターフェイスにより受信されますが、そこから送信されることはありません。

（注） ダイナミック ホスト名を指定したインターフェイスだけを、ルーティング アップデートを送信しないように設定できます。詳細については、「IS-IS ダイナミック ホスト名 （2 ページ）」を参照してください。

**ステップ 4** [Apply] をクリックします。

# IS-IS インターフェイスの設定

この手順では、IS-IS ルーティングのための個々の ASA インターフェイスを変更する方法について説明します。

## 手順

**ステップ 1** **[Configuration ] > [ Device Setup] > [Routing ] > [ISIS] > [Interface]** の順に選択します。

[ISIS Interface Configuration] ペインが表示され、IS-IS インターフェイスの設定が表示されます。インターフェイスごとの hello パディングは、[Hello Padding] チェック ボックスをオン/オフにすることによって設定できます。

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。

**ステップ 2** インターフェイス エントリを選択するには、インターフェイス エントリをダブルクリックするか、そのエントリを選択して [Edit] をクリックします。

[Edit ISIS Interface] ダイアログボックスが表示されます。

**ステップ 3** [General] タブで、次の項目を設定します。

- [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。
- [Enable ISIS on this interface]：このインターフェイス上で IS-IS プロトコルを有効にします。
- [Enable IPv6 ISIS routing on this interface]：このインターフェイス上で IPv6 IS-IS ルーティングを有効にします。
- [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。

（注） IS-IS では、バックアップ指定ルータはありません。プライオリティを 0 に設定すると、そのシステムが DIS になる可能性は低くなりますが、完全には回避できません。プライオリティの高いルータがオンラインになると、現在の DIS からその役割を引き継ぎます。プライオリティ値が同一の場合は、MAC アドレス値が高いルータが優先されます。

- [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。

（注） IS-IS では、バックアップ指定ルータはありません。プライオリティを 0 に設定すると、そのシステムが DIS になる可能性は低くなりますが、完全には回避できません。プライオリティの高いルータがオンラインになると、現在の DIS からその役割を引き継ぎます。プライオリティ値が同一の場合は、MAC アドレス値が高いルータが優先されます。

- [Tag]：この IP プレフィックスが IS-IS 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。
- [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。この間隔は指定 ASA 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。デフォルトを変更する必要はまずありません。

  このオプションは、指定したインターフェイスの指定ルータ（DR）に対してのみ適用されます。DR だけがデータベースの同期を維持するために CSNP パケットを送信します。

- [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。この間隔は指定 ASA 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。デフォルトを変更する必要はまずありません。

  このオプションは、指定したインターフェイスの指定ルータ（DR）に対してのみ適用されます。DR だけがデータベースの同期を維持するために CSNP パケットを送信します。

- **[Adjacency filter]**：**IS-IS 隣接関係（アジャセンシー）の確立をフィルタリングします。**

  着信 IS-IS hello パケットから、hello に含まれる各エリア アドレスと システム ID を組み合わせてNSAPアドレスを作成することにより、フィルタリングが実行されます。その後、これらの各NSAPアドレスがフィルタを通過します。すべてのアドレスが適合することを要求する **Match all area addresses** が指定されていない場合は、いずれかの NSAP が一致するとフィルタに適合したと見なされます。**Match all area addresses** の機能は、特定のアド

レスがない場合にのみ隣接関係を受け入れるといったネガティブテストを実行するときに便利です。

- [Match all area addresses]：（オプション）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。

**ステップ 4** [OK] をクリックします。

**ステップ 5** [Authentication] タブで、レベル 1 やレベル 2 について以下の項目を設定します。

- [Key] フィールドに、IS-IS 更新を認証するキーを入力します。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。

- [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。

- [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 [Text] を選択することによって認証モードを選択し、[Password] フィールドにパスワードを入力します。

**ステップ 6** [OK] をクリックします。

**ステップ 7** [Hello Padding] タブで、次の項目を設定します。

- [Hello Padding]：Hello 埋め込みを有効にします。

  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。

- [Minimal holdtime 1 second for Level-1]：レベル 1 で LSP が有効である保留時間（秒数）を有効にします。

- [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。

  デフォルトでは、送信される hello パケットで、hello インターバル（seconds）の 3 倍の値が保持時間としてアドバタイズされます（[Hello Multiplier] チェック ボックスをオンにすることにより、この乗数（3）を変更できます）。hello インターバルが狭まると、トポロジ変更の検出も速くなりますが、ルーティング トラフィック量は増大します。指定できる範囲は 1 ～ 65535 です。デフォルトは 10 です。

- [Minimal holdtime 1 second for Level-2]：レベル 2 で LSP が有効である保持時間（秒数）を有効にします。

- [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。

デフォルトでは、送信される hello パケットで、hello インターバル（seconds）の 3 倍の値が保持時間としてアドバタイズされます（[Hello Multiplier] チェック ボックスをオンにすることにより、この乗数（3）を変更できます）。hello インターバルが狭まると、トポロジ変更の検出も速くなりますが、ルーティング トラフィック量は増大します。指定できる範囲は 1 ～ 65535 です。デフォルトは 10 です。

- [Hello Multiplier for level-1]：レベル 1 で、ここに指定する数の IS-IS hello パケットがネイバーにおいて欠落すると、ASA が隣接関係（アジャセンシー）がダウンしたと宣言することになります。

  IS-IS hello パケットのアドバタイズされる hold time は、hello 間隔の hello 乗数倍に設定されます。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 ASA への隣接関係（アジャセンシー）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 ASA 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。

- [Hello Multiplier for level-2]：レベル 2 で、ここに指定する数の IS-IS hello パケットがネイバーにおいて欠落すると、ASA が隣接関係（アジャセンシー）がダウンしたと宣言することになります。

  IS-IS hello パケットのアドバタイズされる hold time は、hello 間隔の hello 乗数倍に設定されます。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 ASA への隣接関係（アジャセンシー）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 ASA 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。

- [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。

**ステップ 8** [OK] をクリックします。

**ステップ 9** [LSP Settings] タブで、次の項目を設定します。

- [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。

- [Retransmit Interval]：各 IS-IS LSP の再伝送間の時間を秒数で指定します。

  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。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]：各 IS-IS LSP で再送信間のミリ秒数を指定します。

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 伝送の間の遅延時間をミリ秒で指定します。

  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、ASA 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。

**ステップ 10** [OK] をクリックします。

**ステップ 11** [Metrics] タブで、レベル 1 とレベル 2 について以下の項目を設定します。

両方のレベルのメトリックを同じにするには、[Use the level 1 values also for level 2] チェックボックスをオンにすることができます。

- [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。
- [Default metric]：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。デフォルト値は 10 です。

**ステップ 12** [OK] をクリックします。

**ステップ 13** [適用（Apply）] をクリックします。

# IS-IS IPv4 アドレス ファミリの設定

ルータからは、他の任意のルーティングプロトコル、スタティック設定、または接続されたインターフェイスから学習した外部プレフィックスまたはルートを再配布できます。再配布されたルートはレベル 1 ルータまたはレベル 2 ルータで許可されます。

隣接関係（アジャセンシー）、最短パス優先（SPF）を設定し、IPv4 アドレスに対し、別のルーティング ドメインから ISIS（再配布）にルートを再配布するための条件を定義できます。

### 始める前に

IS-IS のルート認証を有効にするには、予め IS-IS を有効にしてエリアを設定しておく必要があります。手順については、IS-IS ルーティングのグローバルな有効化 （9 ページ）を参照してください。

ネイバーを追加しようとする前に、少なくとも 1 つのインターフェイスで IPv4 が有効になっていることを確認します。IPv4 が有効になっていない場合、ASDM によって、設定が失敗したというエラー メッセージが返されます。

手順

**ステップ 1** [Configuration] > [Device Setup] > [Routing] > [ISIS] > [IPv4 Address Family] > [General] を選択します。

a) 近接する IS ルータをルータによりチェックするには、[Perform adjacency check] チェックボックスをオンにします。

b) [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 1 です。

distance オプションは、IS-IS ルートがルーティング情報ベース（RIB）に挿入されるときに適用されるアドミニストレーティブディスタンスを設定し、他のプロトコルによって検出された同じ宛先アドレスへのルートよりもこれらのルートが優先される可能性を調整します。

c) [Maximum number of forward paths] フィールドに、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。

d) [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、ドロップダウン リストからデフォルト ルートを選択するか、[Manage] をクリックして新しいルートを作成します。新しいルートの作成手順については、ルート マップの定義を参照してください。

**ステップ 2** IS-IS メトリックを設定します。

a) [Global ISIS metric for level 1] に、メトリックを指定する数値を入力します。

指定できる範囲は 1 ～ 63 です。デフォルトは 10 です。

すべての IS-IS インターフェイスのデフォルト メトリック値を変更する必要がある場合、すべてのインターフェイスをグローバルで設定するために、[Global ISIS metric for level 1] オプションを使用することを推奨します。メトリック値がグローバルに設定されている場合、新規値を設定せずに誤って設定済みのメトリックをインターフェイスから削除したり、デフォルト メトリック 10 に戻るよう誤ってインターフェイスに許可したりするなどの、ユーザーのエラーを防ぐことができるため、ネットワーク内で優先度の高いインターフェイスとなります。

b) [Global ISIS metric for level 2] に、メトリックを指定する数値を入力します。

指定できる範囲は 1 ～ 63 です。デフォルトは 10 です。

すべての IS-IS インターフェイスのデフォルト メトリック値を変更する必要がある場合、すべてのインターフェイスをグローバルで設定するために、[Global ISIS metric for level 1] オプションを使用することを推奨します。メトリック値がグローバルに設定されている場

合、新規値を設定せずに誤って設定済みのメトリックをインターフェイスから削除したり、デフォルト メトリック 10 に戻るよう誤ってインターフェイスに許可したりするなどの、ユーザーのエラーを防ぐことができるため、ネットワーク内で優先度の高いインターフェイスとなります。

c) 次のいずれかを選択して、タイプ、長さ、および値（TLV）を設定します。

- [Send and accept both styles of TLVs during transition] チェックボックスをオンにします。
- [Use old style of TLVs with narrow metric] オプション ボタンをオンにします。
- [Use new style TLVs to carry wider metric] オプション ボタンをオンにします。

  いずれかのオプション ボタンをオンにする場合は、[Accept both styles of TLVs during transition] チェックボックスもオンにできます。

  新スタイルの TLV を使用することを強く推奨します。これは、LSP で IPv4 情報をアドバタイズするために使用される TLV は、拡張メトリックのみを使用するように定義されているためです。ソフトウェアは、24 ビット メトリック フィールド（ワイド メトリック）のサポートを提供します。新しいメトリック形式を使用すると、リンク メトリックの最大値は 16777214、総パスメトリックは 4261412864 になります。

d) [Apply metric style to] チェックボックスをオンにし、[Level-1]、[Level-2]、またはその両方のチェックボックスをオンにします。

**ステップ 3** [Apply] をクリックします。

**ステップ 4** **[Configuration] > [Device Setup] > [Routing] > [ISIS]> [IPv4 Address Family] > [SPF]** の順に選択します。

a) SPF 計算に外部メトリックを含めるには、[Honour external metrics during SPF calculations] チェックボックスをオンにします。

b) このデバイスを除外する場合は、[Signal other routers not to use this router as an intermediate hop in their SPF calculations] チェックボックスをオンにし、次のように設定します。

- [Specify on-startup behavior] チェックボックスをオンにして、次のいずれかを選択します。
  - **[Advertise ourself as overloaded until BGP has converged]**
  - **[Specify time to advertise ourself as overloaded after reboot]**

    [Time to advertise ourself as overloaded] フィールドに、ルータが過負荷になっていることをアドバタイズするまでに待機する秒数を入力します。値の範囲は 5 ～ 86400 秒です。

- IP プレフィックスを除外するには、[Don't advertise IP prefixes learned from other protocols when overload bit it set] チェックボックスをオンにします。
- IP プレフィックスを除外するには、[Don't advertise IP prefixes learned from another ISIS level when overload bit is set] チェックボックスをオンにします。

c) 部分ルート計算（PRC）間隔を設定します。

- [PRC Interval] フィールドに、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。
- [Initial wait for PRC] フィールドに、トポロジ変更後の最初の PRC 計算遅延（ミリ秒）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。
- [Minimum wait between first and second PRC] フィールドに、ルータが PRC 間で待機するミリ秒数を入力します。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。

d) レベル 1 およびレベル 2 の SPF 計算間隔を設定します。

（注） 両方のレベルに同じ値を設定する場合は、[Use level 1 values also for level 2] チェックボックスをオンにします。

- [SPF Calculation Interval] フィールドに、ルータが SPF 計算間で待機する時間数を入力します。範囲は、1 ～ 120 秒です。デフォルトは 10 秒です。
- [Initial wait for SPF calculation] フィールドに、ルータが SPF 計算を待機する時間数を入力します。有効値は 1 ～ 120.000 ミリ秒です。デフォルトは 5500 ミリ秒です。
- [Minimum wait between first and second SPF calculation] フィールドに、ルータが SPF 計算間で待機するミリ秒数を入力します。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。

**ステップ 5** [Apply] をクリックします。

**ステップ 6** [Configuration] > [Device Setup] > [Routing] > [ISIS] > [IPv6 Address Family] > [Redistribution] を選択します。

[Redistribution] ペインに、再配布ルートのテーブルが表示されます。

**ステップ 7** 新しい再配布ルートを追加するには [Add] をクリックします。テーブル内の再配布ルートを編集するには [Edit] をクリックします。

[Add Redistribution] ダイアログボックスまたは [Edit Redistribution] ダイアログボックスが表示されます。テーブルのエントリをダブルクリックして編集することもできます。

a) [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。
b) [Process ID] ドロップダウン リストから、ソース プロトコルのプロセス ID を選択します。
c) [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。
d) （オプション）[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。
e) [Metric Type] で、[internal] または [external] オプション ボタンをクリックします。

f) [Route Map] ドロップダウン リストから、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、[Manage] 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。ルートマップの設定手順は、ルート マップの定義を参照してください。

g) [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。

この手順は、OSPF ネットワークからの再配布にのみ適用できます。

**ステップ 8** [OK] をクリックします。

**ステップ 9** [Apply] をクリックします。

### 接続ビットの設定

次の例では、ルータが L2 CLNS ルーティング テーブル内の 49.00aa と一致する際に接続ビットが設定されたままになります。

```
ciscoasa(config)# router isis
 ciscoasa(config-router)# clns filter-set L2_backbone_connectivity permit 49.00aa
 ciscoasa(config-router)# route-map check-for-L2_backbone_connectivity
 ciscoasa(config-router)# match clns address L2_backbone_connectivity
ciscoasa(config)# router isis
 ciscoasa(config-router)#set-attached-bit route-map check-for-L2_backbone_connectivity
 ciscoasa(config-router)# end
 ciscoasa# show clns route 49.00aa

Known via "isis", distance 110, metric 30, Dynamic Entry
Routing Descriptor Blocks:
 via tr2, Serial0
   isis, route metric is 30, route version is 58
```

# IS-IS IPv6 アドレス ファミリの設定

隣接関係（アジャセンシー）、SPF を設定し、IPv6 アドレスに対し、別のルーティング ドメインから IS-IS（再配布）にルートを再配布するための条件を定義できます。

### 始める前に

IS-IS のルート認証を有効にするには、予め IS-IS を有効にしてエリアを設定しておく必要があります。手順については、IS-IS ルーティングのグローバルな有効化 （9 ページ）を参照してください。

ネイバーを追加しようとする前に、少なくとも 1 つのインターフェイスで IPv6 がイネーブルになっていることを確認します。そうしないと、ASDM によって、設定が失敗したというエラー メッセージが返されます。

手順

**ステップ 1** [Configuration] > [Device Setup] > [Routing] > [ISIS] > [IPv6 Address Family] > [General] を選択します。

a) 近接する IS ルータをルータによりチェックするには、[Perform adjacency check] チェックボックスをオンにします。

b) [Administrative Distance] フィールドに、ルートのディスタンスを入力します。指定できる範囲は 1 ～ 255 です。デフォルトは 1 です。

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 1 です。

distance オプションは、IS-IS ルートがルーティング情報ベース（RIB）に挿入されるときに適用されるアドミニストレーティブディスタンスを設定し、他のプロトコルによって検出された同じ宛先アドレスへのルートよりもこれらのルートが優先される可能性を調整します。

c) [Maximum number of forward paths] フィールドに、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。

d) [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、ドロップダウン リストからデフォルト ルートを選択するか、[Manage] をクリックして新しいルートを作成します。新しいルートの作成手順については、ルート マップの定義を参照してください。

**ステップ 2** [Apply] をクリックします。

**ステップ 3** **[Configuration] > [Device Setup] > [Routing] > [ISIS]> [IPv6 Address Family] > [SPF]** の順に選択します。

a) このデバイスを除外する場合は、[Signal other routers not to use this router as an intermediate hop in their SPF calculations] チェックボックスをオンにし、次のように設定します。

- [Specify on-startup behavior] チェックボックスをオンにして、次のいずれかを選択します。
  - **[Advertise ourself as overloaded until BGP has converged]**
  - **[Specify time to advertise ourself as overloaded after reboot]**

    [Time to advertise ourself as overloaded] フィールドに、ルータが過負荷になっていることをアドバタイズするまでに待機する秒数を入力します。値の範囲は 5 ～ 86,400 秒です。

- IP プレフィックスを除外するには、[Don't advertise IP prefixes learned from other protocols when overload bit it set] チェックボックスをオンにします。

- IP プレフィックスを除外するには、[Don't advertise IP prefixes learned from another ISIS level when overload bit is set] チェックボックスをオンにします。

b) 部分ルート計算（PRC）間隔を設定します。

- [PRC Interval] フィールドに、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。
- [Initial wait for PRC] フィールドに、ルータが PRC を待機する時間数を入力します。有効値は 1 ～ 120.000 ミリ秒です。デフォルトは 2000 ミリ秒です。
- [Minimum wait between first and second PRC] フィールドに、ルータが PRC 間で待機するミリ秒数を入力します。有効値は 1 ～ 120.000 ミリ秒です。デフォルトは 5000 ミリ秒です。

c) レベル 1 およびレベル 2 の SPF 計算間隔を設定します。

（注） 両方のレベルに同じ値を設定する場合は、[Use level 1 values also for level 2] チェックボックスをオンにします。

- [SPF Calculation Interval] フィールドに、ルータが SPF 計算間で待機する時間数を入力します。範囲は、1 ～ 120 秒です。デフォルトは 10 秒です。
- [Initial wait for SPF calculation] フィールドに、ルータが SPF 計算を待機する時間数を入力します。有効値は 1 ～ 120.000 ミリ秒です。デフォルトは 5500 ミリ秒です。
- [Minimum wait between first and second SPF calculation] フィールドに、ルータが SPF 計算間で待機するミリ秒数を入力します。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。

**ステップ 4** [Apply] をクリックします。

**ステップ 5** [Configuration] > [Device Setup] > [Routing] > [ISIS] > [IPv6 Address Family] > [Redistribution] を選択します。

[Redistribution] ペインに、再配布ルートのテーブルが表示されます。

**ステップ 6** 新しい再配布ルートを追加するには [Add] をクリックします。テーブル内の再配布ルートを編集するには [Edit] をクリックします。

[Add Redistribution] ダイアログボックスまたは [Edit Redistribution] ダイアログボックスが表示されます。テーブルのエントリをダブルクリックして編集することもできます。

a) [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。
b) [Process ID] ドロップダウン リストから、ソース プロトコルのプロセス ID を選択します。
c) [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。

d) （オプション）[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。

e) [Metric Type] で、[internal] または [external] オプション ボタンをクリックして、宛先ルーティング プロトコルのメトリック タイプを指定します。

f) [Route Map] ドロップダウン リストから、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、[Manage] 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。ルートマップの設定手順は、ルート マップの定義を参照してください。

g) [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。

この手順は、OSPF ネットワークからの再配布にのみ適用できます。

**ステップ 7** [OK] をクリックします。

**ステップ 8** [Apply] をクリックします。

# IS-IS の監視

次の画面を使用して、IS-IS ルーティング プロセスをモニターできます。

- [Monitoring] > [Routing] > [ISIS Neighbors] このペインには、各 IS-IS ネイバーに関する情報が表示されます。

  各行は 1 つの IS-IS ネイバーを表します。リストには、ネイバーごとに、システム ID、タイプ、インターフェイス、IP アドレス、状態（アクティブ、アイドルなど）、保留時間、および回路 ID が含まれます。

- [Monitoring] > [Routing] > [ISIS Rib] このペインには、ローカル IS-IS ルーティング情報ベース（RIB）テーブルが表示されます。

- [Monitoring] > [Routing] > [ISIS IPv6 Rib] このペインには、ローカル IPv6 IS-IS RIB テーブルが表示されます。

# IS-IS の履歴

表 *1 : IS-IS* の機能の履歴

| 機能名 | プラットフォームリリース | 機能情報 |
|---|---|---|
| IS-IS ルーティング | 9.6(1) | ASA で Intermediate System to Intermediate System（IS-IS）のルーティングプロトコルがサポートされました。IS-IS ルーティングプロトコルを使用した、データのルーティング、認証の実行、およびルーティング情報の再配布とモニターについて、サポートが追加されました。<br>次の画面が導入されました。<br>**[Configuration] > [Device Setup] > [Routing] > [ISIS]**<br>**[Monitoring] > [Routing] > [ISIS]** |

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。

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。

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。