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

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。

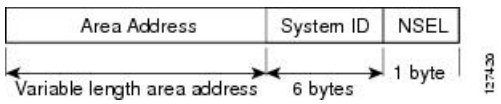
（注） IS-IS インスタンスに複数のエリア アドレスを割り当てることができます。その場合、すべてのエリアアドレスが同義と見なされます。複数の同義エリアアドレスは、ドメインでエリアをマージまたは分割するときに役立ちます。マージまたは分割が完了した後は、複数のエリア アドレスを IS-IS インスタンスに割り当てる必要はありません。

- 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。

show isis hostname コマンドを入力すると、システム ID に対する ASA 名のマッピング テーブルに含まれるエントリが表示されます。

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。

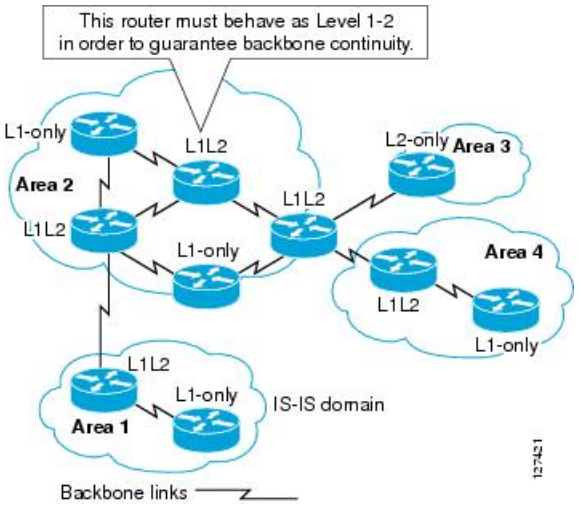
マルチアクセス回線での IS-IS の動作

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。

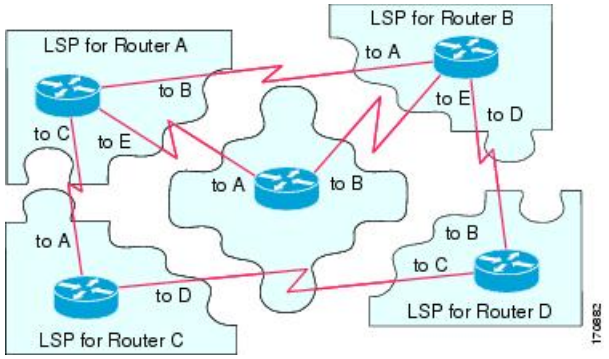
経過期間が同じ LSP の処理

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。

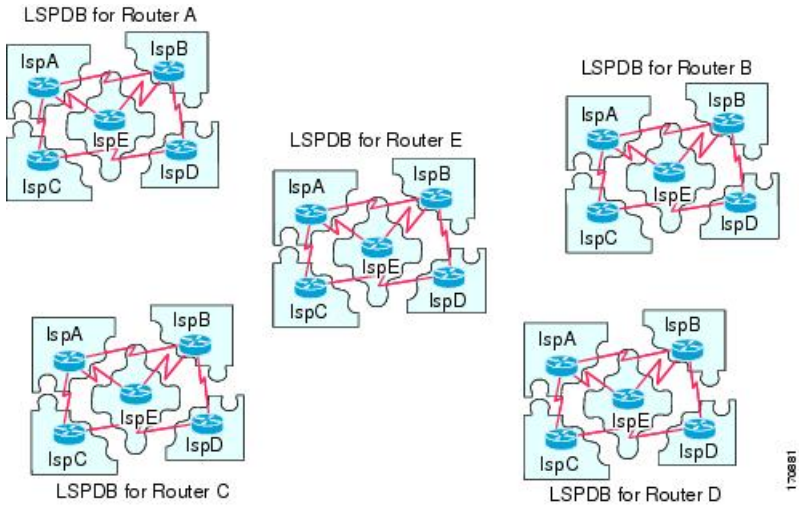
次の図は、LSP を使用してネットワーク マップを作成する方法を示しています。ネットワーク トポロジをジグソー パズルとして想像してください。各 LSP（IS を表す）はジグソー パズルの 1 つのピースに相当します。エリア内のすべてのレベル 1 デバイスまたはレベル 2 サブドメイン内のすべてのレベル 2 デバイスに適用されます。

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 モードでだけ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

個々のインターフェイス 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 （14 ページ）。
ステップ 3 IS-IS LSP の設定 （18 ページ）
ステップ 4 IS-IS サマリー アドレスの設定 （22 ページ）。
ステップ 5 IS-IS パッシブ インターフェイスの設定 （24 ページ）。
ステップ 6 IS-IS インターフェイスの設定 （25 ページ）。
ステップ 7 IS-IS インターフェイス hello パディングの設定 （30 ページ）
ステップ 8 IS-IS IPv4 アドレス ファミリの設定 （33 ページ）。
ステップ 9 IS-IS IPv6 アドレス ファミリの設定 （38 ページ）。

IS-IS ルーティングのグローバルな有効化

IS-IS 設定は 2 段階で行われます。最初に、グローバル コンフィギュレーション モードで IS-IS プロセスを設定し、次にルータ コンフィギュレーション モードで NET および IS-IS のルーティ

ング レベルを指定します。このほかにも、ルータ コンフィギュレーション モードで設定できる一般的なパラメータがあります。そのほうが、インターフェイスごとに設定するよりも、ネットワークにとって合理的です。この項では、それらのコマンドについて説明します。

次に、インターフェイス コンフィギュレーション モードで、インターフェイスごとに IS-IS プロトコルを有効にします。こうすることで、インターフェイスがダイナミック ルーティングに参加し、ネイバーデバイスとの隣接関係（アジャセンシー）を確立できるようになります。隣接関係（アジャセンシー）を確立し、ダイナミック ルーティングを可能にするには、その前に、1 つ以上のインターフェイスでルーティングを有効にしておく必要があります。インターフェイスでの IS-IS の設定手順については、IS-IS インターフェイスの設定 （25 ページ）を参照してください。

この手順では、ルータ コンフィギュレーション モードで、ASA で IP ルーティング プロトコルとして IS-IS を有効にし、その他の一般オプションを有効にする方法について説明します。

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、**changeto context** *name* コマンドを入力します。

手順

ステップ 1 ASA でルーティング プロトコルとして IS-IS を有効にします。

router isis

例：

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

ステップ 2 ルーティング プロセスの NET を指定します。

net *network-entity-title*

例：

```
ciscoasa(config-router)# net 49.1234.aaaa.bbbb.cccc.00
```

NET によって IS-IS のデバイスが特定されます。NET の詳細については、NET について （2 ページ）を参照してください。

ステップ 3 （オプション）IS-IS ルーティング プロセスのルーティング レベルを割り当てます。

is-type [level-1 | level-2-only | level-1-2]

例：

```
ciscoasa(config-router)# is-type level-1
```

- （任意）**level-1**：エリア内ルーティングを示します。ASA は、エリア内の宛先のみを学習します。
- （任意）**level-2-only**：エリア間ルーティングを示します。ASA はバックボーンの一部であり、自分のエリア内にあるレベル 1 ルータとは通信しません。
- （任意）**level-1-2**：ASA は、レベル 1 およびレベル 2 両方のルーティングを実行します。このルータは、ルーティング プロセスのインスタンスを 2 つ実行します。このルータは、エリア内（レベル 1 ルーティング）の宛先について 1 つの LSDB を持っており、SPF の計算を実行してエリア トポロジを検出します。また、他のすべてのバックボーン（レベル 2）ルータの LSP による別の LSDB も備え、別の SPF 計算を実行してバックボーンのトポロジと他のすべてのエリアの存在を検出します。

従来の IS-IS コンフィギュレーションでは、ASA はレベル 1（エリア内）およびレベル 2（エリア間）ルータとしてだけ機能します。マルチエリア IS-IS コンフィギュレーションでは、設定された IS-IS ルーティング プロセスの最初のインスタンスは、デフォルトでレベル 1-2（エリア内およびエリア間）ルータです。設定されている IS-IS プロセスの残りのインスタンスはデフォルトでレベル 1 ルータになります。

（注） IS-IS ルーティング プロセスのタイプを設定することを水晶します。

ステップ 4 ASA で IS-IS ダイナミック ホスト名機能を有効にします。

hostname dynamic

このコマンドは、デフォルトでイネーブルになっています。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 ASA のすべてのインターフェイスで hello パディングを設定します。

hello padding multi-point

このコマンドは、デフォルトでイネーブルになっています。これは、IS-IS hello をフル MTU サイズに設定します。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（IS-IS ルーティング プロセスに対し、ルータ上のすべてのインターフェイスに **no hello padding multi-point** を指定）、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。hello パディングが無効になっても、ASA は、MTU 不一致検出の利点を維持するため、最初の 5 回の IS-IS hello をフル サイズの MTU にパディングして送信します。

ルータ レベルで hello パディングがオフになっていることを確認するには、特権 EXEC モードで **show clns interface** コマンドを入力します。詳細は、IS-IS の監視 （44 ページ）を参照してください。

ステップ 6 （オプション）NLSP IS-IS 隣接関係（アジャセンシー）の状態が変更（アップまたはダウン）されたときに、ASA がログ メッセージを生成できるようにします。

log-adjacency-changes [all]

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。メッセージは次の形式になります。

例：

```
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

all：（オプション）non_IIH イベントによって生成される変更を含みます。

ステップ 7 （オプション）IS-IS プロトコルを無効にして、IS-IS プロトコルがどのインターフェイスでも隣接関係（アジャセンシー）を確立できないようにし、LSP データベースをクリアします。

protocol shutdown

このコマンドにより、既存の IS-IS 設定パラメータを削除することなく、特定のルーティング インスタンスの IS-IS プロトコルを無効にすることができます。このコマンドを入力した場合、IS-IS プロトコルは引き続きルータ上で動作し、ユーザは現在の IS-IS 設定を使用できますが、IS-IS はいずれのインターフェイスでも隣接関係を確立せず、IS-IS LSP データベースをクリアします。特定のインターフェイスについて IS-IS を無効にするには、**isis protocol shutdown** コマンドを使用します。手順については、IS-IS インターフェイスの設定 （25 ページ）を参照してください。

ステップ 8 （オプション）IS-IS IP プレフィックスにハイ プライオリティを割り当てます。

route priority high tag *tag-value*

例：

```
ciscoasa(config-router)# route priority high tag 100
```

tag *tag-value*：特定のルート タグが先頭に付加された IS-IS IP にハイ プライオリティを割り当てます。指定できる範囲は 1 ～ 4294967295 です。

グローバル ルーティング テーブルでより高速な処理とインストールを行うために、このコマンドを使用して、より高いプライオリティの IS-IS IP プレフィックスにタグ付けすると、より速くコンバージェンスを達成できます。たとえば、VoIP トラフィックが、その他のタイプのパケットよりも速く更新されるようにするために、VoIP ゲートウェイ アドレスが最初に処理されるようにすることができます。

ステップ 9 （オプション）すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。

metric *default-value* **[level-1 | level-2]**

例：

```
ciscoasa(config-router)# metric 55 level-1
```

- *default-value*：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るメトリック値。指定できる範囲は 1 ～ 63 です。デフォルトは 10 です。

- （任意）**level-1**：レベル 1 IPv4 または IPv6 メトリックを設定します。
- （任意）**level-2**：レベル 2 IPv4 または IPv6 メトリックを設定します。

すべての IS-IS インターフェイスに対してデフォルトのメトリックを変更する必要がある場合は、**metric** コマンドを使用することをお勧めします。こうすることで、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。

ステップ 10 （オプション）新しいスタイル、長さ、値オブジェクト（TLV）を生成し、それらのオブジェクトのみを受け入れるように ASA を設定します。

metric-style narrow | transition | wide [level-1 | level-2 | level-1-2]

例：

```
ciscoasa(config-router)# metric-style wide level-1
```

- **narrow**：旧スタイルの TLV とナロー メトリックを使用します。
- **transition**：旧スタイルおよび新スタイルの TLV の両方を受け入れるように ASA に指示します。
- **wide**：新スタイルの TLV を使用してワイド メトリックを伝送します。
- （任意）**level-1**：ルーティング レベル 1 でこのコマンドをイネーブルにします。
- （任意）**level-2**：ルーティング レベル 2 でこのコマンドをイネーブルにします。
- （任意）**level-1-2**：ルーティング レベル 2 でこのコマンドをイネーブルにします。

このコマンドを使用すると、ASA が新スタイルの TLV のみを生成して受け入れるようになります。こうすることで、旧スタイルと新スタイル両方の TLV を生成した場合よりも、ASA によるメモリおよびその他のリソースの使用量が減少します。

ステップ 11 （オプション）すべてのインターフェイス上で指定した ASA のプライオリティを設定します。

priority *number-value*

例：

```
ciscoasa(config-router)# priority 80
```

number-value：ASA のプライオリティ。指定できる範囲は 0 ～ 127 です。デフォルトは 64 です。

ステップ 12 （オプション）IS-IS エリアの追加のマニュアル アドレスを設定します。

max-area-addresses *number*

例：

```
ciscoasa(config-router)# max-area-addresses 3
```

number：追加するマニュアル アドレスの数。範囲は 3 ～ 254 です。デフォルト値はありません。

このコマンドにより、追加マニュアル アドレスを設定することでIS-IS エリアのサイズを最大化できるようになります。各マニュアルアドレスを作成するには、追加するアドレスの数を指定し、NET アドレスを割り当てます。NET の詳細については、NET について （2 ページ）を参照してください。

ステップ 13 IS-IS のマルチパス ロード シェアリングを設定します。

maximum-paths *number-of-paths*

例：

```
ciscoasa(config-router)# maximum-paths 8
```

number-of-paths：ルーティング テーブルにインストールするルートの数。指定できる範囲は 1 ～ 8 です。デフォルトは 1 です。

maximum-path コマンドは、ASA で ECMP が設定されている場合に IS-IS マルチロード シェアリングを設定するために使用されます。

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 IS-IS ルータ コンフィギュレーション モードを開始し、IS-IS エリア認証パスワードを設定します。

area-password *password* [**authenticate snp {validate | send-only}**]

例：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# area-password track authenticate snp validate
```

- *password*：割り当てるパスワード。
- （オプション）**authenticate snp**：これを指定すると、システムはパスワードを SNP に挿入するようになります。
- **validate**：これを指定すると、システムはパスワードを SNP に挿入し、受け取ったパスワードを SNP で確認するようになります。
- **send-only**：これを指定すると、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。

あるエリアに存在するすべての ASA でこのコマンドを使用することで、不正ルータがリンクステートデータベースへ誤ったルーティング情報を挿入することを阻止できます。ただし、このパスワードはプレーン テキストとしてやり取りされるため、この機能により提供されるセキュリティは限定されています。

パスワードはレベル 1（ステーション ルータ レベル）PDU LSP、CSNP、および PSNP に挿入されます。**authenticate snp** キーワードを **validate** キーワードまたは **send-only** キーワードのいずれかと共に指定しない場合、IS-IS プロトコルはパスワードを SNP に挿入しません。

ステップ 2 IS-IS ルータ コンフィギュレーション モードを開始し、IS-IS ドメイン認証パスワードを設定します。

domain-password *password* [**authenticate snp {validate | send-only}**]

例：

```
ciscoasa(config-router)# domain-password users2j45 authenticate snp validate
```

- *password*：割り当てるパスワード。
- （オプション）**authenticate snp**：これを指定すると、システムはパスワードをシーケンス番号 PDU（SNP）に挿入するようになります。
- **validate**：これを指定すると、システムはパスワードを SNP に挿入し、受け取ったパスワードを SNP で確認するようになります。

- **send-only**：これを指定すると、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。

このパスワードはプレーンテキストとしてやり取りされるため、この機能により提供されるセキュリティは限定されています。

パスワードはレベル 2（エリア ルータ レベル）PDU LSP、CSNP、および PSNP に挿入されます。**authenticate snp** キーワードを **validate** キーワードまたは **send-only** キーワードのいずれかと共に指定しない場合、IS-IS プロトコルはパスワードを SNP に挿入しません。

ステップ 3 送信される IS-IS パケットに対してのみ認証が実行される（受信パケットに対しては実行されない）ように、IS-IS インスタンスをグローバルまたはインターフェイスごとに設定します。

ルータ モード：**authentication send-only [level-1 | level-2]**

例：

```
ciscoasa(config-router)# authentication send-only level-1
```

インターフェイス モード：**isis authentication send-only [level-1 | level-2]**

例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis authentication send-only level-1
```

- （オプション）**level-1**：認証は受信ではなく、送信されるレベル 1 パケットだけに実行されます。
- （オプション）**level-2**：認証は受信ではなく、送信されるレベル 2 パケットだけに実行されます。

このコマンドは、認証モードおよび認証キー チェーンを設定する前に使用します。これにより、認証の実装がスムーズに進むようになります。レベル 1 またはレベル 2 を指定しない場合は、send-only が両方のレベルに適用されます。

（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。このコマンドを使用して、通信を必要とする ASA をすべて設定した後で、ASA ごとに、認証モードとキー チェーンをイネーブルにします。

ステップ 4 IS-IS インスタンスに対する IS-IS パケットで使用される認証モードのタイプをグローバルまたはインターフェイスごとに指定します。

ルータ モード：**authentication mode {md5 | text} [level-1 | level-2]**

例：

```
ciscoasa(config-router)# authentication mode md5 level-1
```

インターフェイス モード：**isis authentication mode {md5 | text} [level-1 | level-2]**

例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)#  isis authentication mode md5 level-1
```

- **md5**：Message Digest 5 認証を有効にします。
- **text**：クリア テキスト認証を使用します。
- （オプション）**level-1**：レベル1パケットについてだけ、指定された認証を有効にします。
- （オプション）**level-2**：レベル2パケットについてだけ、指定された認証を有効にします。

area-password または **domain-password** を使用してクリア テキスト認証が設定されている場合、これらのどちらのコマンドよりも isis authentication mode が優先されます。**isis authentication mode** を設定した場合、**area-password** または **domain-password** を設定しようとしても許可されません。レベル 1 またはレベル 2 を指定しない場合、このモードは両方のレベルに適用されます。

ステップ 5 IS-IS の認証をグローバルまたはインターフェイスごとに有効にします。

ルータ モード：**authentication key [0 | 8]** パスワード **[level-1 | level-2]**

例：

```
ciscoasa(config-router)# authentication key 0 site1 level-1
```

インターフェイス モード：**isis authentication key [0 | 8]** パスワード **[level-1 | level-2]**

例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# router isis
ciscoasa(config-if)# isis authentication key 0 second level-1
```

- **0**：暗号化されていないパスワードが続くことを指定します。
- **8**：暗号化されたパスワードが後に続くことを指定します。
- *password*：認証を有効にし、キーを指定します。
- （オプション）**level-1**：レベル 1 パケットについてだけ認証をイネーブルにします。
- （オプション）**level-2**：レベル 2 パケットについてだけ認証をイネーブルにします。

key コマンド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。キー認証は、クリアテキスト認証またはMD5認証に適用できます。モードを設定するには、ステップ4を参照してください。IS-IS に一度に適用できる認証キーは 1 つだけです。別のキーを設定すると、1 番めのキーは上書きされます。レベル 1 またはレベル 2 を指定しない場合、パスワードは両方のレベルに適用されます。

ステップ 6 インターフェイスの認証パスワードを設定します。

isis password *password* **[level-1 | level-2]**

例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis password analyst level-1
```

- *password*：インターフェイスに割り当てられる認証パスワード。
- （オプション）**level-1**：レベル 1 での認証パスワードを個別に設定します。レベル 1 ルーティングでは、ASA はステーション ルータとしてだけ動作します。
- （オプション）**level-2**：レベル 2 での認証パスワードを個別に設定します。レベル 2 ルーティングでは、ASA はエリア ルータとしてだけ動作します。

このコマンドにより、不正ルータによるこの ASA との隣接の形成を阻止し、ネットワークを不正侵入から保護することができます。パスワードはプレーンテキストとしてやり取りされるため、これにより提供されるセキュリティは限定されています。**level-1** キーワードと **level-2** キーワードを使用して、異なるルーティング レベルに対して異なるパスワードを割り当てることができます。

例

次の例は、レベル 1 パケットに対して MD5 認証を実行し、site1 という名前のキーチェーンに属している任意のキーを送信する IS-IS インスタンスを示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0101.0101.0101.00
ciscoasa(config-router)# is-type level-1
ciscoasa(config-router)# authentication send-only level-1
ciscoasa(config-router)# authentication mode md5 level-1
ciscoasa(config-router)# authentication key 0 site1 level-1
```

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、**changeto context** *name* コマンドを入力します。

手順

ステップ 1 ルータ コンフィギュレーション モードを開始します。

router isis

例：

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

ステップ 2 内部チェックサム エラーのある IS-IS LSP を受信した場合に、LSP をパージするのではなく無視するように ASA を設定します。

ignore-lsp-errors

例：

```
ciscoas(config-router)# ignore-lsp-errors
```

IS-IS では、データリンク チェックサムが不正な LSP を受信側がパージすることになっています。これにより、パケットの発信側は LSP を再生成します。正しいデータリンク チェックサムを持つLSPをまだ送信している間にデータ破損を引き起こすリンクがネットワークにあった場合、大量のパケットをパージして再生成する連続サイクルが発生し、ネットワークの機能が停止してしまう可能性があります。LSPをパージするのではなく無視するには、このコマンドを使用します。デフォルトではイネーブルになっています。

ステップ 3 パッシブ インターフェイスに属するプレフィックスだけをアドバタイズするように IS-IS を設定します。

advertise passive-only

このコマンドは、LSPアドバタイズメントから、接続されているネットワークのIPプレフィックスを除外します。これにより、ルータ非擬似ノードLSPでアドバタイズされるプレフィックスが少なくなるため、IS-IS のコンバージェンス時間が短縮されます。

ステップ 4 IS-IS LSP がフルになるように設定します。

fast-flood *lsp-number*

例：

```
ciscoasa(config-router)# fast-flood 7
```

（オプション）*lsp-number*：ここで指定した数の LSP があふれると、SPF が開始されます。

このコマンドでは、指定した数のLSPがASAから送信されます。LSPは、SPFの実行前にSPFを呼び出します。LSPフラッディングプロセスを高速化すると、全体的なコンバージェンス時間が短縮されます。指定できる範囲は 1 ～ 15 です。デフォルトは 5 分です。

（注） ルータがSPF計算を実行する前に、LSPの高速フラッディングを有効にすることをお勧めします。

ステップ 5 IS-IS LSP の MTU サイズを設定します。

lsp-mtu *bytes*

例：

```
ciscoasa(config-router)# lsp-mtu 1300
```

bytes：最大パケット サイズ（バイト単位）。バイト数は、ネットワーク内の任意のリンクの最小 MTU 以下の値に設定する必要があります。指定できる範囲は 128 ～ 4352 です。

ステップ 6 LSP が ASA のデータベースで更新されずに保持される最大時間を設定します。

max-lsp-lifetime *seconds*

例：

```
ciscoasa(config-router)# max-lsp-lifetime 2400
```

seconds：LSP のライフタイム（秒数）。指定できる範囲は 1 ～ 65,535 です。デフォルトは 1200 です。

更新 LSP の着信前にライフタイムを超えると、LSP がデータベースからドロップされます。

ステップ 7 SPF 計算の IS-IS スロットリングをカスタマイズします。

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

例：

```
ciscoasa(config-router)#  spf-interval level-1 5 10 20
```

- （任意） **level-1**：レベル 1 エリアにのみ間隔を適用します。
- （任意）**level-2**：レベル 2 エリアにのみ間隔を適用します。
- *spf-max-wait*：2 つの連続した SPF 計算の間の最大間隔を指定します。範囲は、1 ～ 120 秒です。デフォルトは 10 秒です。
- （オプション）*spf-initial-wait*：トポロジが変更されてから最初の SPF 計算までの初期の待機時間を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5500 ミリ秒（5.5 秒）、

  その後の待機間隔はそれぞれ、その前の間隔の 2 倍の長さになり、指定された SPF 最大待機間隔に達するまでそれが行われます。
- （オプション）*spf-second-wait*：最初と 2 番目の SPF 計算間の間隔を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5500 ミリ秒（5.5 秒）、

SPF 計算が実行されるのは、トポロジが変更されたときだけです。このコマンドは、ソフトウェアが SPF 計算を実行する頻度を制御します。

（注） SPF 計算は、プロセッサに高い負荷を与えます。したがって、特にエリアが大きくてトポロジが頻繁に変更される場合は、これを実行する頻度を制限すると役に立つことがあります。SPF 間隔を大きくすると、ASA のプロセッサ負荷が軽減されますが、コンバージェンス速度が低下する可能性があります。

ステップ 8 LSP 生成の IS-IS スロットリングをカスタマイズします。

lsp-gen-interval [level-1 | level-2] *lsp-max-wait [lsp-intial-wait lsp-second wait]*

例：

```
ciscoasa(config-router)#  lsp-gen-interval level-1 2 50 100
```

- （任意） **level-1**：レベル 1 エリアにのみ間隔を適用します。
- （任意）**level-2**：レベル 2 エリアにのみ間隔を適用します。
- *lsp-max-wait*：2 つの LSP が連続して生成される最大間隔を示します。範囲は、1 ～ 120 秒です。デフォルトは 5 秒です。
- （オプション）*lsp-initial-wait*：最初の LSP を生成する前の初期待機時間を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルト値は 50 ミリ秒です。

  毎回の間隔はその前の間隔の 2 倍の長さになり、指定された LSP 最大待機間隔に達するまでそれが行われます。
- （オプション）*spf-second-wait*：最初と 2 番目の LSP 生成の間の間隔を指定します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5000 ミリ秒（5 秒）、

  このコマンドは、生成された LSP 間の遅延を制御します。

ステップ 9 LSP の更新間隔を設定します。

lsp-refresh-interval *seconds*

例：

```
ciscoasa(config-router)# lsp-refresh-interval 1080
```

（オプション）*seconds*：LSP が更新される頻度。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は 900 秒（15 分）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。

（注） 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-refresh-interval** コマンドに対して設定される値は、**max-lsp-lifetime** コマンドに対して設定され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 間隔と比べて LSP ライフタイムを大幅に少なく設定する場合、ソフトウェアが LSP リフレッシュ間隔を減らして、LSP がタイムアウトしないようにします。

ステップ 10 PRC の IS-IS スロットリングをカスタマイズします。

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

例：

```
ciscoasa(config-router)#  prc-interval 5 10 20
```

- *prc-max-wait*：2 つの連続 PRC 計算の最大間隔を示します。範囲は、1 ～ 120 秒です。デフォルトは 5 秒です。
- （オプション）*prc-initial-wait*：トポロジ変更後の最初の PRC 待機時間を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 2000 ミリ秒です。

  その後の待機間隔はそれぞれ、その前の間隔の 2 倍の長さになり、指定された PRC 最大待機間隔に達するまでそれが行われます。
- （オプション）*prc-second-wait*：最初と 2 番目の PRC 計算間の間隔を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5000 ミリ秒（5 秒）、

  PRC は SPF 計算を実行せずにルートを計算するソフトウェア プロセスです。これは、ルーティング システム自体のトポロジは変更されていないが、特定の IS でアナウンスされた情報で変更が検出されたり、そのようなルートを RIB に再インストールしようとしたりすることが必要な場合に可能です。

ステップ 11 PDU がいっぱいになったらルートを抑制するように設定します。

lsp-full suppress {external [interlevel] | interlevel [external] | none}

例：

```
ciscoasa(config-router)# lsp-full suppress interlevel external
```

- **external**この ASA 上にある再配布済みルートを抑制します。
- **interlevel**他のレベルからの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。
- **none**ルートを抑制しません。

IS-IS への再配布ルート数に制限のない（つまり **redistribute maximum-prefix** コマンドが設定されていない）ネットワークでは、LSP がフルとなり、ルートが廃棄される可能性があります。**lsp-full suppress** コマンドを使用することにより、LSP がフルになった場合にどのルートを抑制するかを事前に定義してください。

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 ルータ コンフィギュレーション モードを開始します。

router isis

例：

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

ステップ 2 IS-IS の集約アドレスを作成します。

summary-address *address mask* **[level-1 | level-1-2 | level-2] tag** *tag-number* **metric** *metric-value*

例：

```
ciscoasa(config-router)# summary-address 10.1.0.0 255.255.0.0 tag 100 metric 110
```

- *address*：IP アドレスの範囲を表すために指定するサマリー アドレス。
- *mask*：集約ルートに使用される IP サブネット マスク。
- （任意）**level-1**：設定済みの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。
- （任意）**level-1-2**：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。
- （任意）**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。
- （任意）**tag** *tag-number*：集約ルートにタグを付けるために使用される番号を指定します。指定できる範囲は 1 ～ 4294967295 です。
- （任意）**metric** *metric-value*：集約ルートに適用されるメトリック値を指定します。**metric** キーワード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。指定できる範囲は 1 ～ 4294967295 です。デフォルト値は 10 です。

インターフェイスのメトリック値を検証するため、**show clns interface** コマンドを入力します。詳細については、IS-IS の監視 （44 ページ） を参照してください。

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、（**passive-interface** コマンドを使用して）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 ルータ コンフィギュレーション モードを開始します。

router isis

例：

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

ステップ 2 ASA でパッシブ インターフェイスを設定します。

passive-interface *interface-name*

例：

```
ciscoasa(config-router)# passive-interface inside
```

- **default**：すべてのインターフェイス上でルーティング アップデートを抑止します。
- **management**：管理 0/1 インターフェイスでアップデートを抑止します。
- **management2**：管理 0/2 インターフェイスでアップデートを抑止します。
- **inside**：内部インターフェイスでアップデートを抑止します。

このコマンドは、インターフェイスが IS-IS ネイバー隣接関係を形成しないが、IS-IS データベースにインターフェイス アドレスを追加するように設定します。

ステップ 3 パッシブ インターフェイスをアドバタイズするように ASA を設定します。

advertise passive-only

例：

```
ciscoasa(config-router)# advertise passive-only
```

このコマンドは、パッシブインターフェイスに属するプレフィックスだけをアドバタイズするように IS-IS を設定します。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。

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。以下を変更できます。

- 一般設定（IS-IS の有効化、インターフェイス上での IS-IS シャットダウンプロトコル、優先度、タグ、隣接関係（アジャセンシー）フィルタの有効化など）。
- 認証キーとモード（インターフェイス上に認証を設定する手順については、IS-IS 認証の有効化 （14 ページ）を参照してください）。
- hello パディング値（インターフェイスの hello パディングを設定する手順については、IS-IS インターフェイス hello パディングの設定 （30 ページ）を参照してください）。
- LSP の設定。
- IS-iS メトリックの計算で使用されるインターフェイス遅延メトリック。

始める前に

IS-IS ルーティング プロセスを役立てるには、予め NET を割り当てる必要があります。また、いくつかのインターフェイスについて IS-IS を有効にする必要もあります。レベル 2（エリア間）ルーティングを実行するために設定できるプロセスは 1 つだけです。レベル 2 ルーティングが任意のプロセス上に設定されている場合、追加のプロセスは、すべて自動的にレベル 1 に設定されます。このプロセスは、同時にエリア内（レベル 1）ルーティングを実行するように設定できます。1 つのインターフェイスが複数のエリアに属することはできません。ただし、関連するルーティング プロセスがレベル 1 ルーティングおよびレベル 2 ルーティングの両方を実行している場合は例外です。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 インターフェイス コンフィギュレーション モードを開始します。

interface *interface_id*

例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis
```

ステップ 2 IS-IS 隣接の確立をフィルタリングします。

isis adjacency-filter *name* **[match-all]**

例：

```
ciscoasa(config-if)# isis adjacency-filter ourfriends match-all
```

- *name*：適用するフィルタ セットまたは表現の名前。
- （オプション）**match-all**：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。

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** キーワード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** キーワードの機能は、特定のアドレスがない場合にのみ隣接関係（アジャセンシー）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。

ステップ 3 IS-IS インターフェイスでの LSP アドバタイズメントで接続されているネットワークの IS-IS プレフィックスをアドバタイズします。

isis advertise prefix

例：

```
ciscoasa(config-if)# isis advertise prefix
```

IS-IS コンバージェンス時間を改善するには、**no isis advertise prefix** コマンドを使用します。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。デフォルトではイネーブルになっています。

（注） IS-IS インターフェイスごとにこのコマンドの **no** 形式を設定すると、ルータの非擬似ノード LSP でアドバタイズされるプレフィックスの数が少なくなるため、IS-IS コンバージェンス時間の短縮という課題を小規模に解決することができます。**isis advertise prefix** コマンドの代替手段としては、**advertise passive-only** コマンドがあります。これは、IS-IS インスタンスごとに設定されるため、スケーラブルなソリューションです。

ステップ 4 IS-IS インターフェイスで IPv6 を有効化します。

ipv6 router isis

例：

```
ciscoasa(config-if)# ipv6 router isis
```

ステップ 5 連続する IS-IS LSP 送信間の遅延時間をインターフェイスごとに設定します。

isis lsp-interval *milliseconds*

例：

```
ciscoasa(config-if)# isis lsp-interval 100
```

milliseconds：連続する LSP 間の遅延時間。指定できる範囲は 1 ～ 4294967298 です。デフォルトは 33 ミリ秒です。

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。このコマンドにより、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）が低下します。

ステップ 6 IS-IS メトリックの値を設定します。

isis metric {*metric-value* | **maximum**} [**level-1** | **level-2**]

例：

```
ciscoasa(config-if)# isis metric 15 level-1
```

- *metric-value*：リンクに指定されたメトリック。このメトリックは、リンクを通じてネットワーク内の他の各ルータから他の宛先へのコスト計算に使用されます。レベル1またはレベル 2 のルーティングに対してこのメトリックを設定できます。範囲は 1 ～ 63 です。デフォルト値は 10 です。
- **maximum**：SPF の計算からリンクまたは隣接関係（アジャセンシー）を除外します。
- （任意）**level-1**：このメトリックがレベル 1（エリア内）ルーティングの SPF 計算だけで使用されることを表します。オプション キーワードが指定されていない場合、このメトリックはルーティングレベル 1 およびレベル 2 でイネーブルになります。
- （任意）**level-2**：このメトリックがレベル 2（エリア間）ルーティングの SPF 計算だけで使用されることを表します。オプション キーワードが指定されていない場合、このメトリックはルーティングレベル 1 およびレベル 2 でイネーブルになります。

ステップ 7 インターフェイス上の指定 ASA のプライオリティを設定します。

isis priority *number-value* **[level-1 | level-2]**

例：

```
ciscoasa(config-if)# isis priority 80 level-1
```

- *number-value*：ASA の優先順位を設定します。指定できる範囲は 0 ～ 127 です。デフォルトは 64 です。
- （任意）**level-1**：レベル 1 専用の優先順位を設定します。
- （任意）**level-2**：レベル 2 専用の優先順位を設定します。

プライオリティは、LAN 上のどの ASA が指定ルータまたは DIS であるかを決定するために使用されます。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 ASA が DIS になります。

（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。

ステップ 8 指定されたインターフェイスで隣接関係（アジャセンシー）を形成できないようにして、インターフェイスの IP アドレスを ASA によって生成された LSP に配置するように IS-IS プロトコルをディセーブルにします。

isis protocol shutdown

例：

```
ciscoasa(config-if)# isis protocol shutdown
```

このコマンドを使用すると、コンフィギュレーションパラメータを削除せずに、指定されたインターフェイスの IS-IS プロトコルをディセーブルにできます。IS-IS プロトコルは、このコマンドを設定した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。ルータが生成した LSP にインターフェイスの IP アドレスが設定されます。IS-IS がインターフェイスの隣接関係（アジャセンシー）を形成しないようにし、IS-IS LSP データベースをクリアするには、**protocol shutdown** コマンドを使用します。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 9 各 IS-IS LSP の再伝送間の時間を設定します。

isis retransmit-interval *seconds*

例：

```
ciscoasa(config-if)#  isis retransmit-interval 60
```

（オプション）*seconds*：各 LSP の再送信の間隔。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 秒です。

seconds 引数は控えめな値にする必要があります。値が大きすぎると、不要な再送信が発生します。このコマンドは、LAN（マルチポイント）インターフェイスに影響を与えません。

ステップ 10 各 IS-IS LSP の再伝送間の時間を設定します。

isis retransmit-throttle-interval *milliseconds*

例：

```
ciscoasa(config-if)#  isis retransmit-throttle-interval 300
```

（オプション）*milliseconds*：インターフェイスにおけるLSP再送信間の最小遅延。指定できる範囲は0 ～ 65535 です。

このコマンドは、LSP 再送信トラフィックの制御方法と同様に、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。このコマンドは、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。

このコマンドは、LSP がインターフェイス上で送信されるレート（**isis lsp-interval** コマンドで制御）および単一 LSP の再送信間隔（**isis retransmit-interval** コマンドで制御）とは異なります。これらのコマンドを組み合わせて使用することにより、1つのASAからのそのネイバーへのルーティング トラフィックで発生する負荷を制御できます。

ステップ 11 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。

isis tag *tag-number*

例：

```
ciscoasa(config-if)# isis tag 100
```

tag-number：IS-IS ルートでタグとして機能する番号。指定できる範囲は1 ～ 4294967295 です。

タグが使用されないかぎり、タグ付けされたルートではいかなるアクション（ルートの再配布やルートの集約のためのアクションなど）も発生しません。このコマンドを設定すると、タグがパケット内の新規の情報であるため、ASA は新しい LSP をトリガーします。

例

次に、2 つのインターフェイスに異なるタグ値をタグ付けする例を示します。デフォルトでは、これらの 2 つの IP アドレスは IS-IS レベル 1 およびレベル 2 のデータベースに設定されています。ただし、**redistribute** コマンドを使用してルートマップをタグ 110 に一致させると、IP アドレス 172.16. 0.0 だけがレベル 2 データベースに設定されます。

```
ciscoasa (config)# interface GigabitEthernet1/0
ciscoasa (config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa (config-if)# isis
ciscoasa (config-if)# isis tag 120
ciscoasa (config)# interface GigabitEthernet1/1
ciscoasa (config-if)# ip address 172.16.0.0
ciscoasa (config-if)# isis
ciscoasa (config-if)# isis tag 110
```

```
ciscoasa (config-router)# route-map match-tag permit 10
ciscoasa (config-router)# match tag 110
ciscoasa (config)# router isis
ciscoasa (config-router)# net 49.0001.0001.0001.0001.00
ciscoasa (config-router)# redistribute isis ip level-1 into level-2 route-map match-tag
```

IS-IS インターフェイス hello パディングの設定

helloパケットは、ネイバーの検出と維持に使用されます。インターフェイス レベルで次のhelloパディング パラメータを設定できます。IS-IS 全体で hello パディングを有効/無効にする場合は、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 インターフェイス コンフィギュレーション モードを開始します。

interface *interface_id*

例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis
```

ステップ 2 インターフェイス コンフィギュレーション モードを開始し、ASA のすべてのインターフェイスに対して、IS-IS hello プロトコル データ ユニット（PDU）のパディングを設定します。

isis hello padding

例：

```
ciscoasa(config-if)# isis hello padding
```

helloがフルMTUに埋め込まれます。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。IS-IS hello パディングは、デフォルトで有効になっています。

（注） 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は、ネットワーク帯域幅の無駄を省くため、helloパディングをディセーブルにできます。helloパディングがディセーブルになっても、ASA は、MTU 不一致検出の利点を維持するため、最初の 5 回の IS-IS hello をフルサイズの MTU に埋め込みます。

ステップ 3 IS-IS によって送信される連続した hello パケット間の時間を指定します。

isis hello-interval {*seconds* | **minimal**} **[level-1 | level-2]**

例：

```
ciscoasa(config-if)# isis hello-interval 5 level-1
```

- *seconds*：hello パケットの送信間隔。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**isis hello-multiplier** コマンドを設定することにより、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 0 ～ 65535 です。デフォルトは 10 です。
- **minimal**：結果として得られるホールド タイムが 1 秒になるように、**isis hello-multiplier** コマンドで指定された hello 乗数に基づいて hello 間隔を計算することをシステムに指示します。
- （オプション）**level-1**：レベル 1 での hello 間隔を個別に設定します。X.25、Switched Multimegabit Data Service（SMDS）、フレーム リレー マルチアクセス ネットワークでは、これを使用します。
- （オプション）**level-2**：レベル 2 での hello 間隔を個別に設定します。X.25、SMDS、フレーム リレー マルチアクセス ネットワークでは、これを使用します。

（注） hello 間隔を長くすると帯域幅と CPU 使用率を節約できますが、トラフィック エンジニアリング（TE）トンネルを使用する大規模構成などの一部の状況では、短い hello 間隔が推奨されます。TE トンネルが IS-IS を内部ゲートウェイ プロトコル（IGP）として使用する場合、IP ルーティング プロセスがネットワークの入力点のルータ（ヘッドエンド）で再起動されると、すべての TE トンネルがデフォルトの hello 間隔で再シグナル化されます。再シグナル化を回避するには、hello 間隔を短くします。multiplier{1} command.hello 間隔をさらに短く設定するには、**isis hello-multiplier** コマンドを使用して、IS-IS の hello 間隔を手動で増やす必要があります。

ステップ 4 ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接関係（アジャセンシー）がダウンしていると宣言します。

isis hello-multiplier *multiplier* **[level-1 | level-2]**

例：

```
ciscoasa(config-if)# isis hello-multiplier 10 level-1
```

- *multipler*：IS-IS hello パケットのアドバタイズされる保持時間は、hello 間隔に 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 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 間隔）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。
- （オプション）**level-1**：レベル 1 隣接での hello 乗数を個別に設定します。
- （オプション）**level-2**：レベル 2 隣接での hello 乗数を個別に設定します。

hello パケットが頻繁に失われ、IS-IS 隣接が不必要に失敗する場合は、このコマンドを使用します。

（注） hello 乗数を小さくすると、コンバージェンスが高速になりますが、ルーティングが不安定になる可能性があります。必要に応じて、ネットワークの安定性を高めるために hello 乗数の値を変更してください。hello 乗数をデフォルトの 3 未満の値に設定しないでください。

ステップ 5 IS-IS に使用される隣接関係（アジャセンシー）のタイプを設定します。

isis circuit-type [level-1 | level-1-2 | level-2-only]

例：

```
ciscoasa(config-if)# isis circuit-type level-2-only
```

- （オプション）**level-1**：レベル 1 の隣接関係に対してのみ ASA を設定します。
- （オプション）**level-1-2**：レベル 1 およびレベル 2 の隣接関係に対して ASA を設定します。
- （オプション）**level-2**：レベル 2 の隣接関係に対してのみ ASA を設定します。

通常、このコマンドを設定する必要はありません。ASA でレベルを設定するのが適切な方法です。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。エリア（レベル1 ～ 2 ルータ）間にある ASA でのみ、一部のインターフェイスをレベル 2 として設定する必要があります。これにより、未使用の レベル1 hello パケットを送信することで帯域幅を節約できます。

ステップ 6 ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。

isis csnp-interval *seconds* **[level-1 | level-1-2 | level-2]**

例：

```
ciscoasa(config-if)#  isis csnp-interval 30 level-1
```

- *seconds*：マルチアクセス ネットワークでの CSNP の転送間隔。この間隔は指定 ASA だけに適用されます。指定できる範囲は 0 ～ 65,535 です。デフォルトは 10 秒です。
- （オプション）**level-1**：レベル 1 での CSNP の転送間隔を個別に設定します。
- （オプション）**level-2**：レベル 2 での CSNP の転送間隔を個別に設定します。

このコマンドのデフォルト値を変更する必要はほとんどありません。

このコマンドは、指定したインターフェイスの 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。レベル 1 とレベル 2 で個別に CSNP 間隔を設定できます。

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。

手順

ステップ 1 IPv4 アドレス ファミリを設定するには、ルータ コンフィギュレーション モードを開始します。

router isis

例：

```
ciscoasa(config)# router isis
cisco(config-router)#
```

ステップ 2 隣接関係（アジャセンシー）チェックを実行して、IS-IS プロトコル サポートを確認します。

adjacency-check

例：

```
cisco(config-router)# adjacency-check
```

ステップ 3 IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。

distance *weight*

weight：IS-IS ルートに割り当てられるアドミニストレーティブ ディスタンス。指定できる範囲は 1 ～ 255 です。デフォルトは 115 です。

例：

```
ciscoasa(config-router)# distance 20
```

このコマンドは、IS-IS ルートが RIB に挿入されるときに適用される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に影響を与えます。

（注） 通常は、アドミニストレーティブディスタンスの値が大きいほど、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。重み値は主観的に選択します。重み値を選択するための定量的方法はありません。

ステップ 4 IS-IS のマルチパス ロード シェアリングを設定します。

maximum-paths *number-of-paths*

例：

```
ciscoasa(config-router)# maximum-paths 8
```

number-of-paths：ルーティング テーブルにインストールするルートの数。指定できる範囲は 1 ～ 8 です。デフォルトは 1 です。

maximum-path コマンドは、ASA で ECMP が設定されている場合に IS-IS マルチロード シェアリングを設定するために使用されます。

ステップ 5 IS-IS ルーティング ドメインへのデフォルト ルートを生成します。

default-information originate [**route-map** *map-name*]

例：

```
ciscoasa(config-router)# default-information originate route-map RMAP
```

（任意）**route-map** *map-name*：ルーティング プロセスは、ルート マップが満たされている場合にデフォルト ルートを生成します。

このコマンドを使用して設定された ASA がルーティング テーブルに 0.0.0.0 へのルートを持っている場合、IS-IS は LSP で 0.0.0.0 に対するアドバタイズメントを発信します。ルート マップが存在しない場合、デフォルトではレベル 2 LSP だけでアドバタイズされます。レベル 1 ルーティングでデフォルト ルートを発見するメカニズムには、最も近いレベル 1 またはレベル 2 ルータを探すというものがあります。最も近いレベル 1 またはレベル 2 ルータは、レベル 1 LSP で ATT を調べることにより検出できます。**match ip address** *standard-access-list* コマンドを使用することで、ASA が 0/0 をアドバタイズする前に存在している必要がある 1 つ以上の IP ルートを指定できます。

ステップ 6 IS-IS メトリックをレベル 1 およびレベル 2 に対しグローバルに設定します。

metric *default-value* **[level-1 | level-2]**

例：

```
ciscoasa(config-router)# metric 55 level-1
ciscoasa(config-router)# metric 45 level-2
```

- *default-value*：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るメトリック値。指定できる範囲は 1 ～ 63 です。デフォルトは 10 です。
- （任意）**level-1**：レベル 1 IPv4 または IPv6 メトリックを設定します。
- （任意）**level-2**：レベル 2 IPv4 または IPv6 メトリックを設定します。

ステップ 7 メトリック スタイルおよび適用するレベルを指定します。

metric-style [narrow | transition | wide] [level-1 | level-2 | level-1-2]

例：

```
ciscoasa(config-router)# metric-style wide level-1
```

- **narrow**：旧スタイルの TLV とナロー メトリックを使用するように ASA に指示します。
- **transition**：移行時に旧スタイルおよび新スタイルの TLV の両方を受け入れるように ASA に指示します。
- **wide**：新スタイルの TLV を使用してワイド メトリックを伝送するように ASA に指示します。
- （任意）**level-1**：レベル 1 IPv4 または IPv6 メトリックを設定します。
- （任意）**level-2**：レベル 2 IPv4 または IPv6 メトリックを設定します。
- （任意）**level-1-2**：レベル 1 とレベル 2 の IPv4 または IPv6 メトリックを設定します。

ステップ 8 レベル 1 - レベル 2 ルータがその接続ビットを設定する必要がある場合の制約を指定します。

set-attached-bit route-map *map-tag*

例：

```
ciscoasa(config-router)# set-attached-bit route-map check-for-L2_backbone_connectivity
```

route-map *map-tag*：設定したルート マップの識別情報。指定されたルート マップが一致した場合、ルータはその接続ビットを引き続き設定します。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。

ISO 10589 に指定されているように、現在の IS-IS 実装で、レベル 1 - レベル 2 ルータは、自ドメイン内の他のエリアを認識する際や、他のドメインを認識する際に、レベル 1 LSP 接続ビットを設定します。ただし、ネットワーク トポロジの中には、別のエリアにある隣接レベル 1 - レベル 2 ルータとレベル 2 バックボーンとの接続が失われている可能性のあるものもあります。レベル 1 ルータは、エリアやドメイン外の宛先へのトラフィックを、レベル 2 バックボーンとの接続がない可能性のあるレベル 1 - レベル 2 ルータへ送信できます。

このコマンドによって、レベル 1 - レベル 2 ルータの接続ビット設定に対し、より詳細な制御が可能になります。ルート マップは、1 つ以上の CLNS ルートを指定できます。少なくとも 1 つの match address route map 句がレベル 2 CLNS ルーティング テーブル内のルートと一致し、接続ビットを設定するためのその他すべての要件が合致する場合、レベル 1 - レベル 2 ルータはレベル 1 LSP に接続ビットを設定し続けます。要件に合致しない場合や、match address route map 句がレベル 2 CLNS ルーティング テーブル内のルートと一致しない場合、接続ビットは設定されません。

ステップ 9 SPF 計算の中間ホップとして使用しないように、ASA が他のルータに通知するように ASA を設定します。

set-overload-bit [on-startup {*seconds* | **wait-for bgp**}] [**suppress [[interlevel] [external**]]]

例：

```
ciscoasa(config-router)# set-overload-bit on-startup wait-for-bgp suppress interlevel
external
```

- （任意）**on-startup**：システム起動時の過負荷ビットを設定します。過負荷ビットは、後続の指定引数またはキーワードに応じて、設定された秒数、または BGP が収束するまで設定されたままになります。
- （オプション）*seconds*：システム起動時に過負荷ビットが設定され、設定された状態が続く秒数。指定できる範囲は 5 ～ 86400 です。
- （任意）**wait-for-bgp**：**on-startup** キーワードが設定されている場合、過負荷ビットがシステム起動時に設定され、BGP が収束するまで設定されたままになります。
- （任意）**suppress**：後続キーワードによって指定されるプレフィックスのタイプが抑制されます。
- （任意）**interlevel**：**suppress** キーワードが設定されている場合、別の IS-IS レベルから学習された IP プレフィックスがアドバタイズされるのを防ぎます。
- （任意）**external**：**suppress** キーワードが設定されている場合、他のプロトコルから学習された IP プレフィックスがアドバタイズされるのを防ぎます。

このコマンドは、ASA に対して、非疑似 LSP に過負荷ビット（「hippity bit」とも呼ばれる）を強制的に設定させます。通常、過負荷ビットの設定は、ASA で問題が発生した場合にのみ許可されます。たとえば、ASA でメモリ不足が発生した場合、リンクステート データベースが不完全であり、その結果不完全または不正確なルーティング テーブルが生成されている可能性があります。LSP に過負荷ビットを設定することにより、ルータが問題から復旧するまで、他のルータがその SPF 計算で信頼できないルータを無視することができます。その結果、このルータを通過するパスは、IS-IS エリア内の他のルータから見えなくなります。ただし、IP および CLNS プレフィックスはこのルータに直接接続されます。

ステップ 10 PRC の IS-IS スロットリングをカスタマイズします。

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

例：

```
ciscoasa(config-router)#  prc-interval 5 10 20
```

- *prc-max-wait*：2 つの連続 PRC 計算の最大間隔を示します。範囲は、1 ～ 120 秒です。デフォルトは 5 秒です。
- （オプション）*prc-initial-wait*：トポロジ変更後の最初の PRC 待機時間を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 2000 ミリ秒です。

  その後の待機間隔はそれぞれ、その前の間隔の 2 倍の長さになり、指定された PRC 最大待機間隔に達するまでそれが行われます。

- （オプション）*prc-second-wait*：最初と 2 番目の PRC 計算間の間隔を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5000 ミリ秒（5 秒）、

  PRC は SPF 計算を実行せずにルートを計算するソフトウェア プロセスです。これは、ルーティング システム自体のトポロジは変更されていないが、特定の IS でアナウンスされた情報で変更が検出されたり、そのようなルートを RIB に再インストールしようとしたりすることが必要な場合に可能です。

ステップ 11 SPF 計算の IS-IS スロットリングをカスタマイズします。

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

例：

```
ciscoasa(config-router)#  spf-interval level-1 5 10 20
```

- （任意） **level-1**：レベル 1 エリアにのみ間隔を適用します。
- （任意）**level-2**：レベル 2 エリアにのみ間隔を適用します。
- *spf-max-wait*：2 つの連続 SPF 計算間の最大間隔を示します。範囲は、1 ～ 120 秒です。デフォルトは 10 秒です。
- （オプション）*spf-initial-wait*：トポロジが変更されてから、最初の SPF 計算までの初期の待機時間を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5500 ミリ秒（5.5 秒）、

  その後の待機間隔はそれぞれ、その前の間隔の 2 倍の長さになり、指定された SPF 最大待機間隔に達するまでそれが行われます。

- （オプション）*spf-second-wait*：最初と 2 番目の SPF 計算間の間隔を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5500 ミリ秒（5.5 秒）、

SPF 計算が実行されるのは、トポロジが変更されたときだけです。このコマンドは、ソフトウェアが SPF 計算を実行する頻度を制御します。

（注） SPF 計算は、プロセッサに高い負荷を与えます。したがって、特にエリアが大きくてトポロジが頻繁に変更される場合は、これを実行する頻度を制限すると役に立つことがあります。SPF 間隔を大きくすると、ASA のプロセッサ負荷が軽減されますが、コンバージェンス速度が低下する可能性があります。

ステップ 12 SFP 計算中は外部メトリックを使用するように IS-IS を設定します。

use external-metrics

ステップ 13 BGP、接続、IS-IS、OSPF、またはスタティック ルート再配布を設定します。

redistribute bgp | connected | isis | ospf | static | level-1 | level-2 | level 1-2 metric-type internal | external metric *number*

例：

```
ciscoasa(config-router)# redistribute static level-1 metric-type internal metric 6
```

metric *number*：メトリックの値。指定できる範囲は 1 ～ 4294967295 です。

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。

手順

ステップ 1 ルータ コンフィギュレーション モードを開始します。

router isis

例：

```
cisco(config-router)#
```

ステップ 2 メトリック スタイルを以下の範囲で指定します。

metric-style wide [transition] [level-1 | level-2 | level-1-2]

例：

```
ciscoas(config)# router isis
ciscoasa(config-router)# metric-style wide level-1
```

- （任意）**transition**：旧スタイルおよび新スタイルの TLV の両方を受け入れるようにルータに指示します。
- （任意）**level-1**：レベル 1 IPv4 または IPv6 メトリックを設定します。
- （任意）**level-2**：レベル 2 IPv4 または IPv6 メトリックを設定します。
- （任意）**level-1-2**：レベル 1 とレベル 2 の IPv4 または IPv6 メトリックを設定します。

すべての IS-IS インターフェイスのデフォルト メトリックを変更する必要がある場合は、**metric** コマンドを使用することをお勧めします。これは、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人的ミスを防げるため、ネットワーク内で優先的に使用してください。

ステップ 3 標準 IPv4 または IPv6 アドレス プレフィックスを使用する IS-IS ルーティング セッションを設定するために、アドレス ファミリ コンフィギュレーション モードを開始します。

address-family ipv6 [unicast]

例：

```
ciscoasa(config-router)# address-family ipv6 unicast
cisco(config-router-af)#
```

ステップ 4 隣接関係（アジャセンシー）チェックを実行して、IS-IS プロトコル サポートを確認します。

adjacency-check

例：

```
cisco(config-router-af)# adjacency-check
```

ステップ 5 IS-IS のマルチパス ロード シェアリングを設定します。

maximum-paths *number-of-paths*

例：

```
ciscoasa(config-router-af)# maximum-paths 8
```

number-of-paths：ルーティング テーブルにインストールするルートの数。指定できる範囲は 1 ～ 8 です。デフォルトは 1 です。

maximum-path コマンドは、ASA で ECMP が設定されている場合に IS-IS マルチロード シェアリングを設定するために使用されます。

ステップ 6 IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。

distance *weight*

weight：IS-IS ルートに割り当てられるアドミニストレーティブ ディスタンス。指定できる範囲は 1 ～ 255 です。デフォルトは 115 です。

例：

```
ciscoasa(config-router-af)# distance 20
```

このコマンドは、IS-IS ルートが RIB に挿入されるときに適用される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に影響を与えます。

（注） 通常は、アドミニストレーティブディスタンスの値が大きいほど、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。重み値は主観的に選択します。重み値を選択するための定量的方法はありません。

ステップ 7 IS-IS ルーティング ドメインへのデフォルト ルートを生成します。

default-information originate [**route-map** *map-name*]

例：

```
ciscoasa(config-router-af)# default-information originate route-map TEST7
```

（任意）**route-map** *map-name*：ルーティング プロセスは、ルート マップが満たされている場合にデフォルト ルートを生成します。

このコマンドを使用して設定された ASA がルーティング テーブルに 0.0.0.0 へのルートを持っている場合、IS-IS は LSP で 0.0.0.0 に対するアドバタイズメントを発信します。ルート マップが存在しない場合、デフォルトではレベル 2 LSP だけでアドバタイズされます。レベル 1 ルーティングでデフォルト ルートを発見するメカニズムには、最も近いレベル 1 またはレベル 2 ルータを探すというものがあります。最も近いレベル 1 またはレベル 2 ルータは、レベル 1 LSP で ATT を調べることにより検出できます。**match ip address** *standard-access-list* コマンドを使用することで、ASA が 0/0 をアドバタイズする前に存在している必要がある 1 つ以上の IP ルートを指定できます。

ステップ 8 SPF 計算の中間ホップとして使用しないように、ASA が他のルータに通知するように ASA を設定します。

set-overload-bit [on-startup {*seconds* | **wait-for bgp**}] [**suppress [[interlevel] [external]**]]

例：

```
ciscoasa(config-router-af)# set-overload-bit on-startup wait-for-bgp suppress interlevel
 external
```

- （任意）**on-startup**：システム起動時の過負荷ビットを設定します。過負荷ビットは、後続の指定引数またはキーワードに応じて、設定された秒数、または BGP が収束するまで設定されたままになります。
- （オプション）*seconds*：システム起動時に過負荷ビットが設定され、設定された状態が続く秒数。指定できる範囲は 5 ～ 86400 です。
- （任意）**wait-for-bgp**：**on-startup** キーワードが設定されている場合、過負荷ビットがシステム起動時に設定され、BGP が収束するまで設定されたままになります。
- （任意）**suppress**：後続キーワードによって指定されるプレフィックスのタイプが抑制されます。
- （任意）**interlevel**：**suppress** キーワードが設定されている場合、別の IS-IS レベルから学習された IP プレフィックスがアドバタイズされるのを防ぎます。
- （任意）**external**：**suppress** キーワードが設定されている場合、他のプロトコルから学習された IP プレフィックスがアドバタイズされるのを防ぎます。

このコマンドは、ASA に対して、非疑似 LSP に過負荷ビット（「hippity bit」とも呼ばれる）を強制的に設定させます。通常、過負荷ビットの設定は、ASA で問題が発生した場合にのみ許可されます。たとえば、ASA でメモリ不足が発生した場合、リンクステート データベースが不完全であり、その結果不完全または不正確なルーティング テーブルが生成されている可能性があります。LSP に過負荷ビットを設定することにより、ルータが問題から復旧するまで、他のルータがその SPF 計算で信頼できないルータを無視することができます。その結果、このルータを通過するパスは、IS-IS エリア内の他のルータから見えなくなります。ただし、IP および CLNS プレフィックスはこのルータに直接接続されます。

ステップ 9 PRC の IS-IS スロットリングをカスタマイズします。

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

例：

```
ciscoasa(config-router-af)#  prc-interval 5 10 20
```

- *prc-max-wait*：2 つの連続 PRC 計算の最大間隔を示します。範囲は、1 ～ 120 秒です。デフォルトは 5 秒です。
- （オプション）*prc-initial-wait*：トポロジ変更後の最初の PRC 待機時間を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 2000 ミリ秒です。

  その後の待機間隔はそれぞれ、その前の間隔の 2 倍の長さになり、指定された PRC 最大待機間隔に達するまでそれが行われます。
- （オプション）*prc-second-wait*：最初と 2 番目の PRC 計算間の間隔を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5000 ミリ秒（5 秒）、

  PRC は SPF 計算を実行せずにルートを計算するソフトウェア プロセスです。これは、ルーティング システム自体のトポロジは変更されていないが、特定の IS でアナウンスされた

情報で変更が検出されたり、そのようなルートをRIBに再インストールしようとしたりすることが必要な場合に可能です。

ステップ 10 SPF 計算の IS-IS スロットリングをカスタマイズします。

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

例：

```
ciscoasa(config-router-af)#  spf-interval level-1 5 10 20
```

- （任意） **level-1**：レベル 1 エリアにのみ間隔を適用します。
- （任意）**level-2**：レベル 2 エリアにのみ間隔を適用します。
- *spf-max-wait*：2 つの連続 SPF 計算間の最大間隔を示します。範囲は、1 ～ 120 秒です。デフォルトは 10 秒です。
- （オプション）*spf-initial-wait*：トポロジが変更されてから、最初のSPF計算までの初期の待機時間を示します。値の範囲は1～120,000ミリ秒です。デフォルトは5500ミリ秒（5.5秒）、

  その後の待機間隔はそれぞれ、その前の間隔の2倍の長さになり、指定されたSPF最大待機間隔に達するまでそれが行われます。
- （オプション）*spf-second-wait*：最初と 2 番目の SPF 計算間の間隔を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5500 ミリ秒（5.5 秒）、

SPF 計算が実行されるのは、トポロジが変更されたときだけです。このコマンドは、ソフトウェアが SPF 計算を実行する頻度を制御します。

（注） SPF計算は、プロセッサに高い負荷を与えます。したがって、特にエリアが大きくてトポロジが頻繁に変更される場合は、これを実行する頻度を制限すると役に立つことがあります。SPF間隔を大きくすると、ASAのプロセッサ負荷が軽減されますが、コンバージェンス速度が低下する可能性があります。

ステップ 11 BGP、接続、IS-IS、OSPF、またはスタティック ルート再配布を設定します。

redistribute bgp | connected | isis | ospf | static | level-1 | level-2 | level 1-2 metric-type internal | external metric *number*

例：

```
ciscoasa(config-router-af)# redistribute static level-1 metric-type internal metric 6
```

metric *number*：メトリックの値。指定できる範囲は 1 ～ 4294967295 です。

ステップ 12 特にレベル 1 からレベル 2 またはレベル 2 からレベル 1 へ IS-IS ルートを再配布します。

redistribute isis {level-1 | level-2} into {level-2 | level-1} [[distribute-list *list-number* | **[route-map** *map-tag***]]**

例：

```
ciscoasa(config-router-af)# redistribute isis level-1 into level-2
distribute-list 100
```

- **level-1 | level-2**：IS-IS ルートを再配布するレベル元とレベル先。
- **into**：ルートが再配布されるレベル元と、ルートを再配布するレベル先を区別するキーワード。
- （任意）**distribute-list** *list-number*：IS-IS 再配布を制御する配布リスト番号。配布リストまたはルート マップのいずれかを指定できますが、両方を指定できません。
- （任意）**route-map** *map-tag*：IS-IS 再配布を制御するルート マップ名。配布リストまたはルート マップのいずれかを指定できますが、両方を指定できません。

（注） **redistribute isis** コマンドを機能させるためには、**metric-style wide** コマンドを指定する必要があります。この手順のステップ 1 を参照してください。

IS-IS では、すべてのエリアがスタブ エリアで、バックボーン（レベル 2）からエリア（レベル 1）へルーティング情報がリークしません。レベル 1 だけのルートは、そのエリア内にある最も近いレベル 1 - レベル 2 ルータへのデフォルト ルートを使用します。このコマンドにより、レベル 2 IP ルートをレベル 1 エリアに再配布することができます。この再配布により、レベル 1 だけのルータが IP プレフィックスのエリア外への最良パスを選択することができるようになります。これは IP のみの機能であり、CLNS ルーティングはまだスタブ ルーティングです。

（注） 制御と安定性を増すために、配布リストまたはルートマップを設定して、どのレベル 2 IP ルートをレベル 1 に再配布できるのかを制御できます。これを使用すると、大規模な IS-IS-IP ネットワークは、スケーラビリティを向上させるためにエリアを使用できます。

ステップ 13 IS-IS IPv6 ルートの集約プレフィックスを作成します。

summary-prefix *ipv6-prefix* **[level-1 | level-1-2 | level-2]**

例：

```
cisco(config-router-af)# summary-prefix 2001::/96 level-1
```

- *ipv6 address*：X.X.X.X.::X/0-128 形式の IPv6 プレフィックス。
- （任意）**level-1**：設定済みの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。
- （任意）**level-1-2**：ルートをレベル 1 およびレベル 2 IS-IS に再配布するとき、およびレベル 2 IS-IS がレベル 1 のルートをエリア内で到達可能なものとしてアドバタイズするときに、サマリー ルートが適用されます。

- （任意）**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。

IS-IS の監視

次のコマンドを使用して、IS-IS ルーティング プロセスをモニタできます。コマンド出力の例と説明については、コマンド リファレンスを参照してください。

IS-IS データベースのモニタリング

IS-IS データベースをモニタリングするには、次のコマンドを使用します。

- **show isis database [level-1 | l1] [level-2 | l2] [detail]** ：レベル 1、レベル 2、および各 LSP の詳細な内容について、IS-IS リンクステート データベースを表示します。
- **show isis database verbose** ：IS-IS データベースに関する詳細情報（LSP のシーケンス番号、チェックサム、保留時間など）を表示します。

IS-IS マッピング テーブル エントリのモニタリング

IS-IS ホスト名をモニタリングするには、次のコマンドを使用します。

show isis hostname：IS-IS ルータの、ルータ名とシステム ID のマッピング テーブル エントリを表示します。

IS-IS IPv4 のモニタリング

IS-IS IPv4 をモニタリングするには、次のコマンドを使用します。

- **show isis ip rib**：IS-IS ルーティング プロセスの、IPv4 アドレス ファミリ固有の RIB を表示します。
- **show isis ip spf-log**：IS-IS ルーティング プロセスの、IPv4 アドレス ファミリ固有の SPF ログを表示します。
- **show isis ip topology**：IS-IS ルーティング プロセスの、IPv4 アドレス ファミリ固有のトポロジを表示します。
- **show isis ip redistribution** [**level-1** | **level-2**] [*network-prefix*]：IS-IS によって学習され、インストールされた IPv6 ルートを表示します。
- **show isis ip unicast**：IPv4 アドレス ファミリ固有の RIB、SPF ログ、および IS へのパスを表示します。

IS-IS IPv6 のモニタリング

IS-IS IPv6 をモニタリングするには、次のコマンドを使用します。

- **show isis ipv6 rib**：IS-IS ルーティング プロセスの、IPv6 アドレス ファミリ固有の RIB を表示します。
- **show isis ipv6 spf-log**：IS-IS ルーティング プロセスの、IPv6 アドレス ファミリ固有の SPF ログを表示します。
- **show isis ipv6 topology**：IS-IS ルーティング プロセスの、IPv6 アドレス ファミリ固有のトポロジを表示します。
- **show isis ipv6 redistribution** [**level-1** | **level-2**] [*network-prefix*]：IS-IS によって学習され、インストールされた IPv6 ルートを表示します。
- **show isis ipv6 unicast**：IPv6 アドレス ファミリ固有の RIB、SPF ログ、および IS へのパスを表示します。

IS-IS ログのモニタリング

IS-IS ログをモニタリングするには、次のコマンドを使用します。

- **show isis lsp-log**：新しい LSP をトリガーしたインターフェイスのレベル 1 およびレベル 2 の IS-IS LSP ログを表示します。
- **show isis spf-log**：ASA が SPF 計算を実行した頻度と、実行理由を表示します。

IS-IS プロトコルのモニタリング

IS-IS プロトコルをモニタリングするには、次のコマンドを使用します。

show clns protocol ：ASA での各 IS-IS ルーティング プロセスのプロトコル情報を表示します。

IS-IS ネイバーおよびルートのモニタリング

IS-IS ネイバーをモニタリングするには、次のコマンドを使用します。

- **show isis topology** ：すべてのエリア内の接続されたルータすべてのリストを表示します。このコマンドは、すべてのエリア内のすべてのルータの存在と接続を確認します。
- **show isis neighbors [detail]** ：IS-IS 隣接関係（アジャセンシー）情報を表示します。
- **show clns neighbors** [*process-tag*] [*interface-name*] [**detail**]：エンド システム（ES）、中継システム（IS）およびマルチトポロジ IS-IS（M-ISIS）ネイバーを表示します。このコマンドは、IPv6 のマルチトポロジ IS-IS を介して学習された隣接関係（アジャセンシー）を表示します。
- **show clns is-neighbors** *[interface-name]* **[detail]** ：IS-IS デバイス隣接関係の IS-IS 情報を表示します。

IS-IS RIB のモニタリング

IS-IS RIB をモニタリングするには、次のコマンドを使用します。

- **show isis rib** [*ip-address* | *ip-address-mask*]：RIB に保存されている主要なネットワークの特定のルートのパス、またはすべてのルートのパスを表示します。
- **show isis rib redistribution** [**level-1** | **level-2**] [*network-prefix*]：ローカル再配布キャッシュのプレフィックスを表示します。
- **show route isis** ルーティング テーブルの現在の状態を表示します。

IS-IS トラフィックのモニタリング

IS-IS トラフィックをモニタリングするには、次のコマンドを使用します。

show clns traffic [since {bootup | show}] ：ASA が認識した CLNS トラフィック統計情報を表示します。

IS-IS のデバッグ

IS-IS をデバッグするには、次のコマンドを使用します。

debug isis [adj-packets | authentication | checksum-errors | ip | ipv6 | local-updates | [rptpcp;-errors | rob | snp-packets | spf-events | spf-statistics | spf-triggers | update-packets]：IS-IS ルーティング プロトコルのさまざまな要素をデバッグします。

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について、サポートが追加されました。 次のコマンドが導入されました。**advertise passive-only, area-password, authentication key, authentication mode, authentication send-only, clear, debug isis, distance, domain-password, fast-flood, hello padding, hostname dynamic, ignore-lsp-errors, isis adjacency-filter, isis advertise prefix, isis authentication key, isis authentication mode, isis authentication send-only, isis circuit-type, isis csnp-interval, isis hello-interval, isis hello-multiplier, isis hello padding, isis lsp-interval, isis metric, isis password, isis priority, isis protocol shutdown, isis retransmit-interval, isis retransmit-throttle-interval, isis tag, is-type, log-adjacency-changes, lsp-full suppress, lsp-gen-interval, lsp-refresh-interval, max-area-addresses, max-lsp-lifetime, maximum-paths, metric, metric-style, net, passive-interface, prc-interval, protocol shutdown, redistribute isis, route priority high, router isis, set-attached-bit, set-overload-bit, show clns, show isis, show route isis, spf-interval, summary-address**.

IS-IS の例

このセクションでは、IS-IS のさまざまな要素についてトポロジによる設定例を示します。

IS-IS ルーティングの設定

```
router isis
   net 49.1234.aaaa.bbbb.cccc.00

interface GigabitEthernet0/0
   nameif outside
   security-level 0
   ip address 192.16.32.1 255.255.255.0
   isis
```

IS-IS IPv6 ルーティングの設定

```
router isis
   net 49.1234.aaaa.bbbb.cccc.00

interface GigabitEthernet0/0
   ipv6 address 2001:192:16:32::1/64
   ipv6 router isis
```

同一エリア内でのダイナミック ルーティング

```
iRouter --------(inside G0/1) ASA (G0/0 outside)------------ oRouter

ASA Configuration
  interface GigabitEthernet0/0
   nameif outside
   security-level 0
   ip address 192.16.32.1 255.255.255.0
   ipv6 address 2001:192:16:32::1/64
   isis
   ipv6 router isis

  interface GigabitEthernet0/1
   nameif inside
   security-level 100
   ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
   ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
   isis
   ipv6 router isis

  router isis
   net 49.1234.2005.2005.2005.00
   is-type level-1
   metric-style wide

  interface GigabitEthernet0/0
   ip address 172.16.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:172:16:32::3/64
   ipv6 router isis
   isis priority 120

  interface GigabitEthernet0/1
```

```
   ip address 172.26.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:172:26:32::3/64
   ipv6 router isis

IOS Configuration
  iRouter
  router isis
   net 49.1234.2035.2035.2035.00
   is-type level-1
   metric-style wide

  oRouter
  interface GigabitEthernet0/0
   ip address 192.16.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:192:16:32::3/64
   ipv6 router isis

  oRouter
  interface GigabitEthernet0/1
   ip address 192.26.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:192:26:32::3/64
   ipv6 router isis

  oRouter
  router isis
   net 49.1234.2036.2036.2036.00
   is-type level-1
   metric-style wide
```

複数エリアでのダイナミック ルーティング

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
  ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
  isis
  ipv6 router isis

 interface GigabitEthernet0/1.201
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
  ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
  isis
  ipv6 router isis

 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  maximum-paths 5
 !
 address-family ipv6 unicast
  maximum-paths 5
  exit-address-family
 !

IOS Configuration
```

```
iRouter
interface GigabitEthernet0/0
 ip address 172.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:16:32::3/64
 ipv6 router isis
 isis priority 120


iRouter
interface GigabitEthernet0/1
 ip address 172.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:26:32::3/64
 ipv6 router isis


iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 metric-style wide

oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis


oRouter
interface GigabitEthernet0/1
 ip address 192.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:26:32::3/64
 ipv6 router isis


oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide

oRouter
 interface GigabitEthernet0/0
  ip address 192.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:16:32::3/64
  ipv6 router isis


 oRouter
 interface GigabitEthernet0/1
  ip address 192.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:26:32::3/64
  ipv6 router isis


 oRouter
 router isis
```

```
  net 49.1234.2036.2036.2036.00
  is-type level-1
  metric-style wide
```

重複するエリアでのダイナミック ルーティング

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0
 ipv6 address 2001:172:16:32::1/64
 isis
 ipv6 router isis

interface GigabitEthernet0/0.301
 nameif outside
 security-level 80
 ip address 192.16.32.1 255.255.255.0
 ipv6 address 2001:192:16:32::1/64
 isis
 ipv6 router isis

router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 maximum-paths 5
!
 address-family ipv6 unicast
  redistribute static level-1-2
  maximum-paths 6
 exit-address-family

IOS Configuration
iRouter
interface GigabitEthernet0/0
 ip address 172.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:16:32::3/64
 ipv6 enable
 ipv6 router isis
 isis priority 120
 isis ipv6 metric 600


interface GigabitEthernet0/1
 ip address 172.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:26:32::3/64
 ipv6 router isis


iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 authentication mode md5
```

```
 authentication key-chain KeyChain level-2
 metric-style wide
 maximum-paths 6
!
 address-family ipv6
 summary-prefix 2001::/8 tag 301
 summary-prefix 6001::/16 level-1-2 tag 800
 redistribute static metric 800 level-1-2
exit-address-family


oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip pim sparse-dense-mode
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis
 isis tag 301


oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide

ASA Configuration
router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 maximum-paths 5
!
 address-family ipv6 unicast
  redistribute static level-1-2
  maximum-paths 6
 exit-address-family
!
```

ルートの再配布

```
iRouter ---------- ASA ------------ oRouter


 ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
  ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
  isis
  ipv6 router isis


 interface GigabitEthernet0/1.201
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
  ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
  isis
  ipv6 router isis
```

```
 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  redistribute isis level-2 into level-1 route-map RMAP
  maximum-paths 5
 !
 address-family ipv6 unicast
  maximum-paths 6
 exit-address-family
!

IOS Configuration
iRouter
 interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
  isis priority 120


 iRouter
 interface GigabitEthernet0/1
  ip address 172.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:26:32::3/64
  ipv6 router isis


 iRouter
 router isis
  net 49.1234.2035.2035.2035.00
  net 49.2001.2035.2035.2035.00
  is-type level-2-only
  metric-style wide

oRouter
 interface GigabitEthernet0/0
  ip address 192.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:16:32::3/64
  ipv6 router isis


 oRouter
 interface GigabitEthernet0/1
  ip address 192.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:26:32::3/64
  ipv6 router isis


 oRouter
 router isis
  net 49.1234.2036.2036.2036.00
  is-type level-1
  metric-style wide
```

サマリー アドレス

```
iRouter ---------- ASA ------------ oRouter
```

```
ASA Configuration

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0
 ipv6 address 2001:172:16:32::1/64
 isis
 ipv6 router isis
 isis authentication key cisco#123 level-2
 isis authentication mode md5


interface GigabitEthernet0/0
 nameif outside
 security-level 80
 ip address 192.16.32.1 255.255.255.0
 ipv6 address 2001:192:16:32::1/64
 isis
 ipv6 router isis


router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 redistribute static
 maximum-paths 5
address-family ipv6 unicast
 maximum-paths 6
exit-address-family
```

Passive Interfaces

```
 iRouter ---------- ASA ------------ oRouter


 ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0
  ipv6 address 2001:192:16:32::1/64
  isis
  ipv6 router isis


 interface GigabitEthernet0/1
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0
  ipv6 address 2001:172:16:32::1/64
  isis
  ipv6 router isis


 interface GigabitEthernet0/2
  nameif dmz
  security-level 0
  ip address 40.40.50.1 255.255.255.0
  ipv6 address 2040:95::1/64
```

```
 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  redistribute isis level-2 into level-1 route-map RMAP
  passive-interface default

IOS Configuration
 iRouter
  interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
  isis priority 120

 iRouter
 interface GigabitEthernet0/1
  ip address 172.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:26:32::3/64
  ipv6 router isis

 iRouter
 router isis
  net 49.1234.2035.2035.2035.00
  net 49.2001.2035.2035.2035.00
  is-type level-2-only
  metric-style wide

 oRouter
 interface GigabitEthernet0/0
  ip address 192.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:16:32::3/64
  ipv6 router isis

 oRouter
 interface GigabitEthernet0/1
  ip address 192.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:26:32::3/64
  ipv6 router isis

 oRouter
 router isis
  net 49.1234.2036.2036.2036.00
  is-type level-1
  metric-style wide
```

認証

```
ASA ------------ Router

ASA Configuration

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
 ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
 isis
```

```
 ipv6 router isis
 isis authentication key cisco#123 level-2
 isis authentication mode md5


interface GigabitEthernet0/0.301
 nameif outside
 security-level 80
 ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
 ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
 isis
 ipv6 router isis


router isis
 net 49.1234.2005.2005.2005.00
 metric-style wide
 authentication mode md5
 authentication key cisco#123 level-2

IOS Configuration
iRouter
interface GigabitEthernet0/0
 ip address 172.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:16:32::3/64
 ipv6 enable
 ipv6 router isis
 isis authentication mode md5
 isis authentication key-chain KeyChain level-2
 isis priority 120
 isis ipv6 metric 600


iRouter
key chain KeyChain
 key 1
  key-string cisco#123


iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 authentication mode md5
 authentication key-chain KeyChain level-2
```