SSM の設定

SSM の設定の前提条件

次に、Source-Specific Multicast （SSM）および SSM マッピングを設定するための前提条件を示します。

- SSM および SSM マッピングを使用するには、3560-CX スイッチの IP Services フィーチャセットをイネーブルにする必要があります。
- SSM マッピングを設定する前に、次の作業を実行する必要があります。
  - IP マルチキャスト ルーティングをイネーブルにします。
  - PIM スパース モードをイネーブルにします。
  - SSM を設定します。
- スタティック SSM マッピングを設定する場合は、事前にアクセス コントロール リスト（ACL）を設定して、送信元アドレスにマッピングされるグループ範囲を定義する必要があります。
- SSM マッピングを設定し、DNS ルックアップで使用できるようにするには、稼動中の DNS サーバーにレコードを追加する必要があります。稼働中の DNS サーバーがない場合は、DNS サーバーをインストールする必要があります。

（注） 実行中の DNS サーバーにレコードを追加するには、*Cisco Network Registrar* などの製品を使用できます。

SSM 設定の制約事項

次に、SSM を設定する際の制約事項を示します。

- IGMPv3 で SSM を使用するには、Cisco IOS ルータ、アプリケーションが稼働しているホスト、そしてアプリケーション自体が SSM をサポートしている必要があります。
- SSM にまだ対応していないネットワーク内の既存のアプリケーションは、（S, G）チャネルの加入登録をサポートするように変更していない限り、SSM 範囲内では機能しません。そのため、既存のアプリケーションが指定の SSM 範囲内のアドレスを使用する場合、ネットワークで SSM をイネーブルにすると問題が発生することがあります。
- IGMP スヌーピング：IGMPv3 で使用される新しいメンバーシップ レポート メッセージは、旧型の IGMP スヌーピング devicesでは正しく認識されない場合があります。
- SSM をレイヤ 2 スイッチング メカニズムとともに使用する場合は、ある程度のアドレス管理が必要となります。Cisco Group Management Protocol（CGMP）、IGMP スヌーピング、または Router-Port Group Management Protocol（RGMP）でサポートされるのはグループ固有のフィルタリングだけであり、（S, G）チャネル固有のフィルタリングはサポートされていません。同じスイッチドネットワーク内の異なるレシーバーが異なる（S, G）チャネルを要求し、これらのチャネルが同じグループを共有している場合、レシーバーは上記のような既存メカニズムの利点を活用できません。どちらのレシーバーも、すべての（S, G）チャネル トラフィックを受信し、不要なトラフィックを入力から除外します。SSM は、独立した多くのアプリケーションに SSM 範囲のグループ アドレスを再利用できるので、このような状況では、スイッチド ネットワークのトラフィック フィルタリング機能が低下する可能性があります。そのため、アプリケーションに対して SSM 範囲の IP アドレスをランダムに使用し、SSM 範囲内の 1 つのアドレスがさまざまなアプリケーションに再利用される可能性を小さくすることが重要です。たとえば、TV チャネル セットを提供するアプリケーション サービスで、SSM を使用する場合は、各 TV（S, G）チャネルに異なるグループを使用する必要があります。このようにすれば、同じアプリケーション サービス内の異なるチャネルに複数のレシーバが接続されていても、レイヤ 2 デバイスを含むネットワークでトラフィック エイリアシングが発生しなくなります。
- PIM-SSM では、ラストホップ ルータは、そのインターフェイス上に適切な（S, G）加入登録があると、定期的に（S, G）Join メッセージを送信し続けます。このため、レシーバが（S, G）加入を送信する限り、ソースが長時間（または二度と）トラフィックを送信しなくてもレシーバからソースへの最短パス ツリー（SPT）状態が維持されます。

  送信元がトラフィックを送信し、レシーバーがグループに加入している場合にだけ（S, G）ステートが維持される PIM-SM では、これとは対照的な状況が発生します。PIM-SM では、送信元がトラフィックの送信を 3 分以上停止すると、（S, G）ステートは削除され、その送信元からのパケットが RPT を通じて再度到達した場合のみに再確立されます。PI-SSM では、送信元がアクティブであることをレシーバに通知するメカニズムがないので、レシーバが（S, G）チャネルの受信を要求している限り、（S, G）ステートを維持する必要があります。

次に、SSM マッピングを設定する際の制約事項を示します。

- SSM マッピング機能は、完全な SSM の利点を共有しません。SSM マッピングでは、ホストからグループ G の加入が取得され、1 つまたは複数のソースに関連付けられているアプリケーションでこのグループを指定できるため、グループ G ごとにこのようなアプリケーション 1 つのみをサポートできます。それにもかかわらず、完全な SSM アプリケーションは、SSM マッピングにも使用される同じグループを共有することができます。
- 完全な SSM への移行ソリューションとして SSM マッピングだけを使用する場合は、ラストホップ ルータの IGMPv3 をイネーブルにする際に十分に注意してください。

SSM および SSM マッピングに関する情報

SSM コンポーネント

SSM は、1 対多のアプリケーション（ブロードキャスト アプリケーション）に最適なデータグラム配信モデルです。

SSM は、オーディオおよびビデオ ブロードキャスト アプリケーション環境を対象とした IP マルチキャスト ソリューションのシスコによって実装されたコア ネットワーキング テクノロジーで、RFC 3569 に説明されています。次のコンポーネントを組み合わせることで、SSM の実装がサポートされます。

- Protocol Independent Multicast Source-Specific Mode（PIM-SSM）
- インターネット グループ管理プロトコル バージョン 3（IGMPv3）

Protocol Independent Multicast（PIM）SSM（PIM-SSM）は、SSM の実装をサポートするルーティング プロトコルで、PIM スパース モード（PIM-SM）から派生しました。IGMP は、ホストがルータにマルチキャスト グループ メンバーシップを伝えるために使用するインターネット技術特別調査委員会（IETF）標準トラック プロトコルです。IGMP バージョン 3 は、SSM に必要なソース フィルタリングをサポートします。SSM を IGMPv3 と共に実行するには、SSM が IOS ルータ、アプリケーションが実行されるホスト、およびアプリケーション自体でサポートされる必要があります。

Internet Standard Multicast と SSM の違い

インターネットと多くの企業イントラネットの標準 IP マルチキャスト インフラストラクチャは、PIM-SM プロトコルと Multicast Source Discovery Protocol（MSDP）に基づいています。これらのプロトコルは信頼でき、広範で、効率的であることが証明されています。しかし、インターネット標準マルチキャスト（ISM）サービス モデルの複雑さと機能性の制限があります。たとえば、ISM では、ネットワークは、実際にマルチキャスト トラフィックを送信しているホストについての情報を維持する必要があります。SSM では、この情報は IGMPv3 によって最後のホップ デバイスにリレーされた発信元アドレスを介して受信することで提供されます。SSM は、ISM に関連付けられた問題への対応を強化し、ネットワーク内で ISM 用に開発され

たプロトコルと共存することを目的としています。一般に、SSMはSSMを使用するアプリケーションにIP マルチキャスト サービスを提供します。

ISMサービスはRFC 1112で定義されています。このサービスは、任意のソースからマルチキャスト ホスト グループと呼ばれるレシーバのグループへのIPデータグラムの配信によって構成されています。マルチキャストホスト グループのデータグラム トラフィックは、任意のIPユニキャスト送信元アドレスSとIP宛先アドレスとしてのマルチキャスト グループ アドレスGのデータグラムで構成されます。システムはホストグループのメンバになることによってこのトラフィックを受信します。ホスト グループのメンバーシップにはIGMP バージョン1、2、または3によるホスト グループのシグナリングが必要です。

SSM では、データグラムは（S, G）チャネルに基づいて配信されます。1 つの (S, G) チャネルのトラフィックは、IP宛先アドレスとしてIPユニキャスト ソース アドレスSとマルチキャスト グループ アドレスGを持つデータグラムで構成されています。システムは、（S, G）チャネルのメンバになることによって、このトラフィックを受信します。SSM と ISM のどちらでも、ソースになるためにシグナリングは必要ありません。ただし、SSMでは、レシーバーは特定の送信元からのトラフィックの受信または非受信を決めるために（S, G）への加入または脱退を行う必要があります。つまり、レシーバは加入した（S, G）チャネルからだけトラフィックを受信できます。一方、 ISM では、レシーバは受信するトラフィックの送信元の IP アドレスを知る必要はありません。提案されているチャネル加入シグナリングの標準的な方法では、IGMP INCLUDE モード メンバーシップ レポートを使用します。これは、IGMP バージョン 3 でのみサポートされています。

IP マルチキャスト グループ アドレス範囲の設定済みのサブセットにSSM配信モデルを適用することにより、SSM と ISM サービスを一緒に使用できます。インターネット割り当て番号局（IANA）は、SSMアプリケーションおよびプロトコル用に232.0.0.0～232.255.255.255のアドレス範囲を確保しています。ソフトウェアでは、224.0.0.0 ～ 239.255.255.255 の IP マルチキャスト アドレス範囲の任意のサブセットのSSM設定を許可します。SSM範囲が定義されると、アプリケーションが明示的な (S, G) チャネル加入登録を使用するように変更されているか、URL Rendezvous Directory（URD）によってSSMに対応していない限り、SSM範囲内でアドレスを使用しようとする場合に既存のIPマルチキャスト レシーバアプリケーションはトラフィックを受信しません。

SSM の動作

確立されているネットワークは、IPマルチキャストサービスがPIM SMに基づいているので、SSM サービスをサポートできます。ドメイン間の PIM-SM に必要なプロトコルがすべて揃っていないネットワークでも、SSMを単独で導入できます。つまり、SSMはRPを必要としないため、Auto-RP、MSDP、またはブートストラップ ルータ（BSR）などのRPメカニズムの必要がありません。

SSM がすでに PIM-SM 用に設定済みのネットワークで配備されている場合、ラスト ホップ ルータのみを SSM をサポートするソフトウェア イメージにアップグレードする必要があります。レシーバに直接接続されていないルータを SSM をサポートするソフトウェア イメージにアップグレードする必要はありません。一般的に、これらのラストホップではないルータは、SSM範囲でPIM-SMのみを実行する必要があります。これらは、MSDPシグナリング、登録、

または PIM-SM 共有ツリー動作が SSM 範囲内で発生することを抑制するために、追加のアクセス コントロール設定を必要とする場合もあります。

SSM モードの動作は、**ip pim ssm** グローバル コンフィギュレーション コマンドを使用して SSM 範囲を設定することによってイネーブルできます。この設定による影響は次のとおりです。

- SSM 範囲内のグループの場合、(S, G) チャネル加入は IGMPv3 INCLUDE モード メンバーシップ レポートによって受け入れられます。
- SSM 範囲のアドレスの PIM 動作は、PIM-SM の派生モードである PIM-SSM に変更されます。このモードでは、PIM (S, G) 加入およびプルーニング メッセージのみがルータによって生成されます。ランデブー ポイント ツリー（RPT）動作に関連した着信メッセージは無視されるか、拒否され、着信 PIM 登録メッセージは登録停止メッセージによってただちに応答されます。ラストホップ ルータ以外のルータでは、PIM-SSM は PIM-SM と下位互換性を保ちます。したがって、ラストホップ ルータ以外のルータは SSM グループに PIM-SM を使用できます（SSM をサポートしていない場合など）。
- SSM 範囲内のグループの場合、SSM 範囲内の MSDP Source-Active（SA）メッセージは受け入れ、生成、または転送されません。

IGMPv3 ホスト シグナリング

IGMPv3 は、ホストがマルチキャスト グループのラスト ホップ ルータにメンバーシップを伝える IETF 標準トラック プロトコルの第 3 バージョンです。IGMPv3 は、グループ メンバーシップを伝える能力をホストに与えます。これによってソースに関するフィルタリングが可能になります。ホストは、特定のソースを除いて、グループに送信するすべてのソースからトラフィックを受信したい（EXCLUDE と呼ばれるモード）、またはグループに送信する特定のソースからのみトラフィックを受信したい（INCLUDE と呼ばれるモード）と伝えることができます。

IGMPv3 は、ISM および SSM と同時に動作可能です。ISM では、EXCLUDE モードと INCLUDE モードの両方のレポートがラスト ホップ ルータによって受け入れられます。SSM では、INCLUDE モード レポートのみがラスト ホップ ルータによって受け入れられます。

の利点

IP マルチキャスト アドレス管理が不要

ISM サービスで、トラフィック ディストリビューションは使用する IP マルチキャスト グループ アドレスにのみ基づくため、アプリケーションは一意の IP マルチキャスト グループ アドレスを取得する必要があります。異なるソースとレシーバを持つ2つのアプリケーションが同じ IP マルチキャスト グループ アドレスを使用すると、両方のアプリケーションのレシーバが両方のアプリケーションのソースからトラフィックを受信します。適切にプログラムしている場合、レシーバは不要なトラフィックをフィルタできますが、この状態は一般的に許容できないレベルの不要なトラフィックを生み出します。

アプリケーションへの一意の IP マルチキャスト グループ アドレスの割り当ては問題となります。最も短期のアプリケーションはセッション記述プロトコル（SDP）やセッション通知プロトコル（SAP）のようなメカニズムを使用して、ランダムアドレスを取得します。これは、インターネット内のアプリケーションの増加によってうまく機能しないソリューションです。長期アプリケーションの現在のベスト ソリューションは、RFC 2770 に説明されていますが、このソリューションは各自律システムが 255 の使用可能な IP マルチキャスト アドレスのみに限定される制限の影響を受けます。

SSM で、他のソースからのトラフィックとは関係なく、各ソースからのトラフィックはネットワーク内のルータ間で転送されます。このため、異なるソースが SSM 範囲のマルチキャスト グループ アドレスを再利用できます。

望ましくないソースからの DoS 攻撃を防ぐ

SSM で、個別の各ソースからのマルチキャスト トラフィックは、（IGMPv3、IGMP v3lite または URD メンバーシップによって）レシーバから要求された場合にのみネットワーク中に転送されます。これに対し、ISM はマルチキャスト グループに送信するアクティブなソースからそのマルチキャスト グループを要求するすべてのレシーバにトラフィックを転送します。インターネット ブロードキャスト アプリケーションで、トラフィックを同じマルチキャスト グループにただ送信するだけで、望ましくないソースが実際のインターネットブロードキャスト ソースを簡単に妨害できるため、この ISM の動作は非常に望ましくありません。この状況は、レシーバ側で不要なトラフィックによって帯域幅を消耗させるため、インターネットブロードキャストの無停止の受信を妨害します。SSM では、トラフィックをマルチキャスト グループにただ送信するだけでは、このような種類の DoS 攻撃は行えません。

導入と管理が容易

ネットワークがマルチキャスト グループに送信しているアクティブ ソースについての情報を維持する必要がないため、SSM は簡単にインストールし、ネットワークでプロビジョニングできます。この要件は、（IGMPv1、IGMPv2、または IGMPv3 を使用する）ISM でのみ存在します。

ISM サービスの現在の標準ソリューションは PIM-SM と MSDP です。PIM-SM（Auto-RP または BSR の必要性を含む）および MSDP での Rendezvous Point（RP）管理は、ネットワークがアクティブ ソースについて学習するためにのみ必要です。この管理は SSM では必要ありません。このため、SSM は ISM よりインストールや管理が簡単で、配備での動作面の拡張も ISM より簡単です。SSM のインストールが簡単であるその他の要素は、既存の PIM-SM ネットワークを活用でき、ラスト ホップ ルータをアップグレードするだけで IGMPv3、IGMP v3lite、または URD をサポートできる点です。

インターネット ブロードキャスト アプリケーションに最適

上記の 3 つの利点により、次の理由で SSM はインターネット ブロードキャスト スタイルのアプリケーションに理想的です。

- 一意の IP マルチキャスト アドレスなしで SSM によって、インターネット ブロードキャスト サービスを提供できるため、コンテンツ プロバイダーはサービスを簡単に提供でき

ます（コンテンツ プロバイダーにとって、IP マルチキャスト アドレス割り当てはこれまで深刻な問題でした）。

- インターネット ブロードキャスト サービスは多数のレシーバに公開されることにより、DoS 攻撃の最も一般的な対象となるため、このような攻撃の阻止はインターネット ブロードキャスト サービスの重要な要素です。
- SSM はインストールや動作が簡単なため、特に、コンテンツを複数の独立した PIM ドメイン間で転送する必要のある場合（SSM のために PIM ドメイン間で MSDP を管理する必要がないため）、ネットワーク オペレータにとって理想的です。

SSM マッピングの概要

管理上または技術上の理由によりエンド システム上で SSM をサポートすることができない、または望ましくない場合、SSM マッピングは SSM 移行をサポートします。SSM を使用して IGMPv3 をサポートしていないレガシー STB に対して、ライブ ストリーミング ビデオを提供することは、SSM マッピングの一般的な応用例です。

典型的な STB 配置では、各 TV チャネルは独立した 1 つの IP マルチキャスト グループを使用し、その TV チャネルの送信を行うアクティブなサーバは 1 つです。1 つのサーバから複数の TV チャネルへの送信は可能ですが、各チャネルのグループはそれぞれ異なります。このようなネットワーク環境で、ルータが特定のグループ G の IGMPv1 または IGMPv2 のメンバーシップ レポートを受信した場合、レポートの宛先は暗黙的に、そのマルチキャスト グループに関連付けられている TV チャネルの well-known TV サーバになります。

SSM マッピングは、グループに送信しているソースをラスト ホップ ルータで検出する手段を提供します。SSM マッピングが設定されている場合、特定のグループ G の IGMPv1 または IGMPv2 のメンバーシップ レポートを受信したルータは、レポートを、このグループに関連付けられている既知のソースの 1 つ以上の (S, G) チャネル メンバーシップに変換します。

ルータはグループ G の IGMPv1 または IGMPv2 のメンバーシップ レポートを受信すると、SSM マッピングを使用して、グループ G の 1 つ以上のソース IP アドレスを決定します。その後、SSM マッピングは IGMPv3 レポートの INCLUDE (G, [S1, G], [S2, G]...[Sn, G]) に従ってメンバーシップ レポートを変換し、IGMPv3 レポートを受信したときと同様に続行します。ルータは、IGMPv1 または IGMPv2 メンバーシップ レポートを受信し続ける限り、さらに、グループの SSM マッピングが変更されない限り、PIM Join を（S1, G）から（Sn, G）までに送信し、これらのグループに加入し続けます。このため、SSM マッピングにより、IGMPv3 が未サポートであるレガシー STB への映像配信や、IGMPv3 ホスト スタックを利用しないアプリケーションに SSM を活用できます。

SSM マッピング機能を使用すると、ラスト ホップ ルータはスタティックに設定されたルータ上のテーブルまたは DNS サーバへの問い合わせを通じて、ソース アドレスを決定できます。スタティックに設定されたテーブルが変更された場合や、DNS マッピングが変更された場合、ルータは、現在のソースを加入したグループに関連付けたままにします。

スタティック SSM マッピング

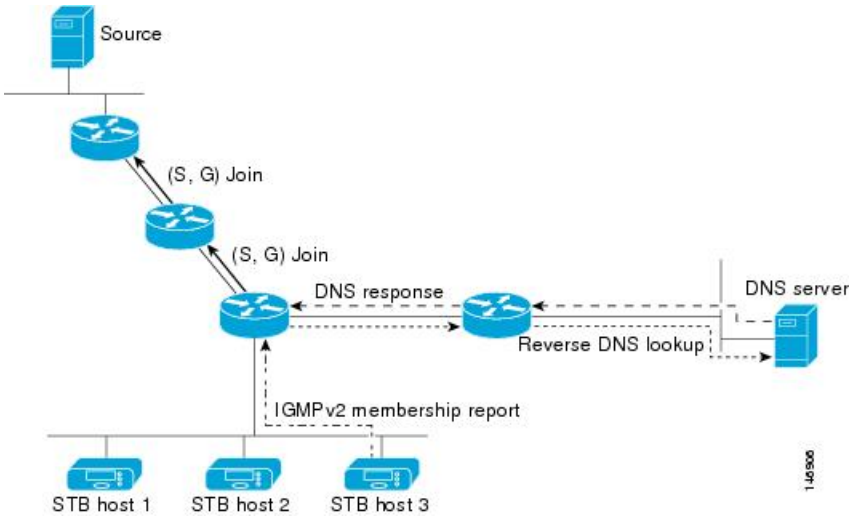
SSM スタティック マッピングを使用して、スタティック マップを使用してグループに送信するソースを決定するようにラスト ホップ ルータを設定できます。スタティック SSM マッピングを使用するには、グループ範囲を定義するアクセス リスト（ACL）を設定する必要があります。これらの ACL によって許可されたグループを **ip igmp static ssm-map** グローバル コンフィギュレーション コマンドを使用してソースにマッピングできます。

DNS が必要ない小規模なネットワークで、または一時的に不正確になった DNS マッピングをローカルに上書きするために、スタティック SSM マッピングを設定できます。設定されたスタティック SSM マッピングは、DNS マッピングよりも優先されます。

DNS ベースの SSM マッピング

DNS ベースの SSM マッピングを使用して、逆 DNS ルックアップを実行してグループを送信するソースを決定するようにラスト ホップ ルータを設定できます（次の図を参照）。DNS ベースの SSM マッピングが設定されると、ルータはグループ アドレス G を含むドメイン名を構築し、DNS への逆ルックアップを実行します。ルータにより、この構築されたドメイン名に戻される IP アドレス リソース レコード（IP ARR）がルックアップされ、戻された IP アドレスが、このグループに関連付けられるソース アドレスとして使用されます。SSM マッピングでサポートできる送信元の数は、グループごとに最大 20 です。ルータは各グループに設定されているすべてのソースに加入します。

図 *1: DNS* ベースの *SSM* マッピング



ラスト ホップ ルータが 1 つのグループの複数のソースに加入できるようにする SSM マッピング メカニズムを使用すると、TV ブロードキャストのソース冗長性を提供できます。このコンテキストでは、同じ TV チャネルで 2 つのビデオ ソースに加入するために、SSM マッピングを使用しているラスト ホップ ルータによって、冗長性が提供されます。ただし、ラスト ホップ ルータでのビデオ トラフィックの重複を防ぐため、ビデオ ソースは、サーバ側のスイッチオーバー メカニズム（1 つのビデオ ソースがアクティブになる間、残りのバックアップ ビデオ ソースがパッシブになる）を使用する必要があります。パッシブの送信元は待機状態にな

り、アクティブな送信元の障害が検出された場合に、そのTVチャネルにビデオ トラフィックを送信します。このため、サーバ側のスイッチオーバー メカニズムによって、1 台のサーバだけが TV チャネルにビデオ トラフィックを実際に送信するようになります。

G1、G2、G3、G4 を含むグループ G について 1 つ以上のソース アドレスをルックアップするには、次の DNS リソース レコード（RR）を DNS サーバで設定する必要があります。

G4.G3.G2.G1 [*multicast-domain*] [*timeout*]	IN A *source-address-1*
	IN A *source-address-2*
	IN A *source-address-n*

multicast-domain 引数は、設定可能な DNS プレフィックスです。デフォルト DNS プレフィックスは、in-addr.arpa です。インストールがインターネットから切り離されている場合、またはマッピングするグループ名が自分の所有するグローバル スコープのグループ アドレス（SSM 用に設定する RFC 2770 タイプのアドレス）である場合にだけ、デフォルトのプレフィックスを使用します。

timeout 引数は、SSM マッピングを実行しているルータが DNS ルックアップをキャッシュする時間を設定します。この引数はオプションで、エントリが設定されているゾーンのタイムアウトのデフォルトです。タイムアウトは、ルータがこのグループについて DNS サーバに問い合わせるまで、現在のマッピングを保持する期間を示します。タイムアウトは DNS RR エントリのキャッシュ時間から導出され、DNS サーバでグループ/ソースごとに設定できます。ルータによって生成される DNS クエリー数を最小にする場合は、この時間に大きな値を設定します。新しいソース アドレスですべてのルータを早く更新する場合は、この時間に小さな値を設定します。

（注） DNS RR の設定に関する詳細については、DNS サーバのマニュアルを参照してください。

ソフトウェアで DNS ベースの SSM マッピングを設定するには、いくつかのグローバル コマンドを設定する必要がありますが、チャネルごとに特定の設定をする必要はありません。追加チャネルが追加された場合も、SSM マッピングの設定は変更しません。DNS ベースの SSM マッピングが設定されるときに、1 つまたは複数の DNS サーバによって、マッピングが全体的に処理されます。DNS ベースの SSM マッピングで、設定および冗長性管理に使用されるすべての DNS テクニックを必要なエントリに適用できます。

SSM マッピングの利点

- SSM マッピング機能は、IGMPv3 に基づく純粋な SSM ソリューションと同じくらいに、ネットワーク導入および管理を簡単にします。SSM マッピングをイネーブルにするために、いくつかの追加設定が必要です。
- SSM の利点である DoS 攻撃の禁止は、SSM マッピングの設定時に適用されます。SSM マッピングを設定した場合、まだ DoS 攻撃に対して脆弱な唯一のネットワーク セグメントが、ラスト ホップ ルータに接続された LAN のレシーバになります。これらのレシーバはまだ IGMPv1 および IGMPv2 を使用しているため、同じ LAN 上の不要なソースからの

攻撃に対して脆弱です。ただし、SSM マッピングは、ネットワーク上のあらゆる不要なソースからのマルチキャスト トラフィックからこれらのレシーバ（およびそれらに繋がるネットワーク パス）を保護します。

- SSMマッピングを使用したネットワーク内でのアドレスの割り当てには、調整が必要ですが、ネットワークからのコンテンツが他のネットワークに転送される場合でも、外部認証局からの割り当ては必要ではありません。

SSM および SSM マッピングの設定方法

SSM の設定

SSM を設定するには、次の手順を実行します。

この手順は任意です。

始める前に

Source Specific Multicast（SSM）範囲の定義にアクセスリストを使用する場合、**ip pim ssm** コマンドでアクセスリストを参照する前にアクセスリストを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip pim ssm** [**default** | **range** *access-list*]
4. **interface** *type number*
5. **ip pim** {**sparse-mode** | **sparse-dense-mode**}
6. **ip igmp version 3**
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	スイッチ# **configure terminal**	
ステップ 3	**ip pim ssm** [**default** | **range** *access-list*] 例： スイッチ(config)# **ip pim ssm range 20**	IP マルチキャスト アドレスの SSM 範囲を定義します。
ステップ 4	**interface** *type number* 例： スイッチ(config)# **interface gigabitethernet 1/0/1**	IGMPv3 をイネーブルに設定可能なホストに接続されているインターフェイスを選択し、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。
ステップ 5	**ip pim** {**sparse-mode** | **sparse-dense-mode**} 例： スイッチ(config-if)# **ip pim sparse-mode**	インターフェイスに対して PIM をイネーブルにします。
ステップ 6	**ip igmp version 3** 例： スイッチ(config-if)# **ip igmp version 3**	このインターフェイス上で IGMPv3 をイネーブルにします。デフォルトでは、IGMP のバージョン 2 が設定されます。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SSM マッピングの設定

スタティック SSM マッピングの設定

スタティック SSM マッピングを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp ssm-map enable**
4. **no ip igmp ssm-map query dns**
5. **ip igmp ssm-map static** *access-list source-address*
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp ssm-map enable** 例： `スイッチ(config)# ip igmp ssm-map enable`	設定されている SSM 範囲で、グループの SSM マッピングをイネーブルにします。 （注） このコマンドでは、デフォルトで、DNS ベースの SSM マッピングがイネーブルにされます。
ステップ 4	**no ip igmp ssm-map query dns** 例：	（任意）DNS ベースの SSM マッピングをディセーブルにします。

	コマンドまたはアクション	目的
	`スイッチ(config)# no ip igmp ssm-map query dns`	（注） スタティック SSM マッピングだけを使用する場合は、DNS ベースの SSM マッピングをディセーブルにします。デフォルトでは、**ip igmp ssm-map** コマンドによって DNS ベースの SSM マッピングがイネーブルになります。
ステップ 5	**ip igmp ssm-map static** *access-list source-address* 例： `スイッチ(config)# ip igmp ssm-map static 11 172.16.8.11`	スタティック SSM マッピングを設定します。 • *access-list* 引数に入力した ACL によって、*source-address* 引数に入力したソース IP アドレスにマッピングされるグループが決まります。 （注） 追加のスタティック SSM マッピングを設定することもできます。SSM マッピングを追加設定した場合、ルータが SSM 範囲のグループの IGMPv1 または IGMPv2 のメンバーシップレポートを受信すると、deviceは、設定されている各 **ip igmp ssm-map static** コマンドに基づいて、そのグループに関連付けられている送信元アドレスを特定します。deviceは各グループに最大 20 の送信元を関連付けます。 必要な場合は、ステップを繰り返して、追加のスタティック SSM マッピングを設定します。
ステップ 6	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `スイッチ# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

DNS ベースの SSM マッピングの設定（CLI）

DNS ルックアップを実行してグループに送信を実行しているソースの IP アドレスを認識するよう、ラスト ホップ ルータを設定する場合は、この作業を実行します。

始める前に

- このタスクを実行する前に、IP マルチキャスト ルーティングをイネーブルにし、PIM スパース モードをイネーブルにし、SSM を設定します。詳細については、「Configuring Basic Multicast」モジュールを参照してください。
- SSM マッピングを設定し、DNS ルックアップで使用できるようにするためには、実行中の DNS サーバにレコードを追加できるようになる必要があります。稼働中の DNS サーバがない場合は、DNS サーバをインストールする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp ssm-map enable**
4. **ip igmp ssm-map query dns**
5. **ip domain multicast** *domain-prefix*
6. **ipname-server** *server-address1* [*server-address2server-address6*]
7. 冗長性のために追加の DNS サーバーを設定する場合は、必要に応じて、ステップ 6 を繰り返します。
8. **end**
9. **show running-config**
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp ssm-map enable** 例： `Device(config)# ip igmp ssm-map enable`	設定されている SSM 範囲で、グループの SSM マッピングをイネーブルにします。
ステップ 4	**ip igmp ssm-map query dns** 例：	（任意）DNS ベースの SSM マッピングをイネーブルにします。

	コマンドまたはアクション	目的
	`Device(config)# ip igmp ssm-map query dns`	• デフォルトでは、**ip igmp ssm-map** コマンドによってDNSベースのSSMマッピングがイネーブルになります。実行コンフィギュレーションに保存されるのは、このコマンドを **no** 形式で使用した場合だけです。 （注） DNSベースのSSMマッピングがディセーブルの場合、このコマンドを使用してDNS ベースの SSM マッピングを再度イネーブルにします。
ステップ 5	**ip domain multicast** *domain-prefix* 例： `Device(config)# ip domain multicast ssm-map.cisco.com`	（任意）Cisco IOS XE ソフトウェアが DNS ベースの SSM マッピングに使用するドメイン プレフィックスを変更します。 • デフォルトでは、ip-addr.arpa ドメイン プレフィックスが使用されます。
ステップ 6	**ipname-server** *server-address1* [*server-address2server-address6*] 例： `Device(config)# ip name-server 10.48.81.21`	名前とアドレスの解決に使用する 1 つまたは複数のネーム サーバーのアドレスを指定します。
ステップ 7	冗長性のために追加の DNS サーバーを設定する場合は、必要に応じて、ステップ 6 を繰り返します。	--
ステップ 8	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

SSM マッピングを使用したスタティック トラフィック転送の設定

ラスト ホップ ルータ上の SSM マッピングでスタティック トラフィック転送を設定する場合は、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip igmp static-group** *group-address* **source ssm-map**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet 1/0/1**	SSM マッピングを使用してマルチキャスト グループにスタティックにトラフィックを転送するインターフェイスを選択し、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。 （注） SSM マッピングを使用したトラフィックのスタティック転送は、DNSベースのSSMマッピングとスタティックに設定されたSSMマッピングのいずれかで機能します。
ステップ 4	**ip igmp static-group** *group-address* **source ssm-map** 例： スイッチ(config-if)# **ip igmp static-group 239.1.2.1 source ssm-map**	そのインターフェイスから（S, G）チャネルへのスタティック転送用のSSMマッピングを設定します。 このコマンドは、特定グループに SSM トラフィックをスタティックに転送する場合に使用します。チャネルの送信元アドレスを決定するにはDNSベースの SSM マッピングを使用します。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

SSM マッピングの設定と動作の確認

SSM マッピングの設定と動作を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show ip igmp ssm-mapping**
3. **show ip igmp ssm-mapping** *group-address*
4. **show ip igmp groups** [*group-name* | *group-address* | *interface-type interface-number*] [**detail**]
5. **show host**
6. **debug ip igmp** *group-address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip igmp ssm-mapping** 例： スイッチ# **show ip igmp ssm-mapping** SSM Mapping : Enabled DNS Lookup : Enabled Mcast domain : ssm-map.cisco.com Name servers : 10.0.0.3 10.0.0.4	（任意）SSMマッピングの設定に関する情報を表示します。
ステップ 3	**show ip igmp ssm-mapping** *group-address* 例：	（任意）SSMマッピングが特定のグループに使用するソースを表示します。

	コマンドまたはアクション	目的
	スイッチ# **show ip igmp ssm-mapping 232.1.1.4** Group address: 232.1.1.4 Database : DNS DNS name : 4.1.1.232.ssm-map.cisco.com Expire time : 860000 Source list : 172.16.8.5 : 172.16.8.6	次に、設定済みの DNS ベースの SSM マッピングに関する情報の例を示します。ルータはソース 172.16.8.5 および 172.16.8.6 にグループ 232.1.1.4 をマッピングする DNS ベースのマッピングを使用しています。このエントリのタイムアウトは、860000 ミリ秒（860 秒）です。
ステップ 4	**show ip igmp groups** [*group-name* | *group-address* | *interface-type interface-number*] [**detail**] 例： スイッチ# **show ip igmp group 232.1.1.4 detail** Interface: GigabitEthernet2/0/0 Group: 232.1.1.4 SSM Uptime: 00:03:20 Group mode: INCLUDE Last reporter: 0.0.0.0 CSR Grp Exp: 00:02:59 Group source list: (C - Cisco Src Report, U - URD, R - Remote, S - Static, M - SSM Mapping) Source Address Uptime v3 Exp CSR Exp Fwd Flags 172.16.8.3 00:03:20 stopped 00:02:59 Yes CM 172.16.8.4 00:03:20 stopped 00:02:59 Yes CM 172.16.8.5 00:03:20 stopped 00:02:59 Yes CM 172.16.8.6 00:03:20 stopped 00:02:59 Yes CM	（任意）ルータに直接接続されているレシーバと IGMPによって学習されたレシーバを持つマルチキャスト グループを表示します。 この例の「M」フラグは、SSMマッピングが設定されることを示します。
ステップ 5	**show host** 例： スイッチ# **show host** Default domain is cisco.com Name/address lookup uses domain service Name servers are 10.48.81.21 Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate temp - temporary, perm - permanent NA - Not Applicable None - Not defined Host Port Flags Age Type Address(es) 10.0.0.0.ssm-map.cisco.c None (temp, OK) 0 IP 172.16.8.5 172.16.8.6 172.16.8.3	（任意）デフォルト ドメイン名、名前のルックアップ サービスのスタイル、ネーム サーバ ホストのリスト、および、ホスト名とアドレスのキャッシュにあるリストを表示します。

	コマンドまたはアクション	目的
ステップ 6	**debug ip igmp** *group-address* 例： スイッチ# **debug ip igmp** IGMP(0): Convert IGMPv2 report (*,232.1.2.3) to IGMPv3 with 2 source(s) using STATIC. スイッチ# **debug ip igmp** IGMP(0): Convert IGMPv2 report (*,232.1.2.3) to IGMPv3 with 2 source(s) using DNS. スイッチ# **debug ip igmp** IGMP(0): DNS source lookup failed for (*, 232.1.2.3), IGMPv2 report failed	（任意）受信および送信した IGMP パケットとホスト関連イベントを表示します。 最初の例の出力は、ルータによってグループ G の IGMPv2 加入が IGMPv3 加入に変換されていることを示しています。 2 番目の例の出力は、DNS ルックアップが成功したことを示しています。 3 番目の例の出力は、DNS ベースの SSM マッピングがイネーブルで、DNS ルックアップが失敗したことを示しています。

SSM および SSM マッピングのモニタリング

SSM のモニタリング

SSM をモニタするには、必要に応じて特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
スイッチ# **show ip igmp groups detail**	IGMPv3 で（S, G）チャネル加入を表示します。
スイッチ# **show ip mroute**	マルチキャスト グループが SSM サービスをサポートしているかどうか、または送信元固有のホスト レポートが受信されたかどうかを表示します。

SSM マッピングのモニタリング

SSM マッピングをモニターするには、次の表の特権 EXEC コマンドを使用します。

表 *1 : SSM* マッピングをモニターするコマンド

コマンド	目的
スイッチ# **show ip igmp ssm-mapping**	SSMマッピングについての情報を表示します。
スイッチ#**show ip igmp ssm-mapping** *group-address*	SSM マッピングが特定のグループに使用する送信元を表示します。

コマンド	目的
スイッチ#**show ip igmp groups** [*group-name* | *group-address* | *interface-type interface-number*] [**detail**]	ルータに直接接続されているレシーバと IGMP によって学習されたレシーバを持つマルチキャスト グループを表示します。
スイッチ#**show host**	デフォルトのドメイン名、名前ルックアップ サービス、ネーム サーバー ホストのリスト、およびホスト名とアドレスのキャッシュされたリストを表示します。
スイッチ#**debug ip igmp** *group-address*	送受信された IGMP パケットと IGMP ホスト関連イベントを表示します。

SSM および SSM マッピングの設定例

IGMPv3 を使用した SSM の例

次に、SSM 用に（IGMPv3 を実行する）デバイスを設定する例を示します。

```
ip multicast-routing
!
interface GigabitEthernet3/1/0
 ip address 172.21.200.203 255.255.255.0
 description backbone interface
 ip pim sparse-mode
!
interface GigabitEthernet3/2/0
 ip address 131.108.1.2 255.255.255.0
 ip pim sparse-mode
 description ethernet connected to hosts
 ip igmp version 3
!
ip pim ssm default
```

SSM フィルタリング例

次に、SSM ルーティングをサポートしないソフトウェア リリースを実行しているレガシー RP ルータでフィルタリングを設定する例を示します。このフィルタリングは SSM 範囲で不要な PIM-SM および MSDP トラフィックをすべて抑制します。このフィルタリングがなくても SSM は動作しますが、レガシーのファースト ホップ ルータとラスト ホップ ルータがネットワークに存在する場合、追加の RPT トラフィックがある場合があります。

```
ip access-list extended  no-ssm-range
  deny   ip any 232.0.0.0 0.255.255.255 ! SSM range
  permit ip any any
! Deny registering in SSM range
ip pim accept-register list no-ssm-range
ip access-list extended msdp-nono-list
```

```
  deny   ip any 232.0.0.0 0.255.255.255 ! SSM Range
  ! .
  ! .
  ! .
  ! See ftp://ftpeng.cisco.com/ipmulticast/config-notes/msdp-sa-filter.txt for other SA
  ! messages that typically need to be filtered.
  permit ip any any
! Filter generated SA messages in SSM range. This configuration is only needed if there
! are directly connected sources to this router. The "ip pim accept-register" command
! filters remote sources.
ip msdp redistribute list msdp-nono-list
! Filter received SA messages in SSM range. "Filtered on receipt" means messages are
! neither processed or forwarded. Needs to be configured for each MSDP peer.
ip msdp sa-filter in msdp-peer1 list msdp-nono-list
! .
! .
! .
ip msdp sa-filter in msdp-peerN list msdp-nono-list
```

SSM マッピングの例

次に、SSMマッピング用にルータを設定する設定例を示します。この例では、機能間の互換性を示すために、他の IGMP および SSM 設定オプションの範囲も示します。例で使用されている機能のすべてを理解していない場合、この設定例をモデルとして使用しないでください。

（注） グローバル SSM 範囲 232.0.0.0/8 のアドレス割り当てはランダムです。この設定例の一部またはすべてをコピーする場合、この例で示されているように、232.1.1.x ではなくランダムアドレス範囲を選択してください。ランダムなアドレス範囲を使用することで、SSM マッピングの使用時に他の SSM の内容をインポートしたときに、アドレスの衝突が発生する可能性を最小限に抑え、競合を防ぐことができます。

```
!
no ip domain lookup
ip domain multicast ssm.map.cisco.com
ip name-server 10.48.81.21
!
!
ip multicast-routing distributed
ip igmp ssm-map enable
ip igmp ssm-map static 10 172.16.8.10
ip igmp ssm-map static 11 172.16.8.11
!
!
.
.
.
!
interface GigabitEthernet0/0/0
 description Sample IGMP Interface Configuration for SSM-Mapping Example
 ip address 10.20.1.2 255.0.0.0
 ip pim sparse-mode
 ip igmp last-member-query-interval 100
 ip igmp static-group 232.1.2.1 source ssm-map
 ip igmp version 3
 ip igmp explicit-tracking
```

```
 ip igmp limit 2
 ip igmp v3lite
 ip urd
!
.
.
.
!
ip pim ssm default
!
access-list 10 permit 232.1.2.10
access-list 11 permit 232.1.2.0 0.0.0.255
!
```

次の表で、SSM マッピング設定例に示されている重要なコマンドについて説明します。

表 *2: SSM* マッピングの設定例で使用されているコマンドの説明

コマンド	説明
no ip domain lookup	IP DNS に基づいたホスト名からのアドレス変換をディセーブルにします。 （注） **no ip domain-list** コマンドは、IP DNS ベースのホスト名/アドレス間変換をディセーブルにすることにより、SSM マッピングの設定に矛盾が生じないことを示すためにのみ、設定に表示されます。このコマンドがイネーブルの場合、Cisco IOS XE ソフトウェアは、ホスト名として未知の文字列の解決を試みます。
ip domain multicast ssm-map.cisco.com	SSM マッピングのドメイン プレフィックスとして ssm-map.cisco.com を指定します。
ip name-server 10.48.81.21	SSM マッピングおよび DNS が利用されるソフトウェアの他のすべてのサービスで使用される DNS サーバの IP アドレスとして、10.48.81.21 を指定します。
ip multicast-routing	IP マルチキャスト ルーティングをイネーブルにします。
ip igmp ssm-map enable	SSM マッピングをイネーブルにします。
ip igmp ssm-map static 10 172.16.8.10	ソース アドレス 172.16.8.10 を使用するよう、ACL 10 によって許可されるグループを設定します。 • この例では、ACL 10 によって、232.1.2.10 を除く 232.1.2.0/25 範囲ですべてのグループが許可されます。
ip igmp ssm-map static 11 172.16.8.11	ソース アドレス 172.16.8.11 を使用するよう、ACL 11 によって許可されるグループを設定します。 • この例では、ACL 11 によって、グループ 232.1.2.10 が許可されます。

コマンド	説明
ip pim sparse-mode	PIM スパース モードをイネーブルにします。
ip igmp last-member-query-interval 100	IGMPv2 ホストの脱退遅延を減らします。 （注） このコマンドは、SSMマッピングの設定には必要ではありません。ただし、SSM マッピングに依存しているIGMPv2 ホストでは、このコマンドは効果的です。
ip igmp static-group 232.1.2.1 source ssm-map	グループ 232.1.2.1 に関連付けられているソースを特定するために使用されるよう、SSMマッピングを設定します。その結果得られる (S, G) チャネルは、静的に転送されます。
ip igmp version 3	このインターフェイス上で IGMPv3 をイネーブルにします。 （注） このコマンドは、IGMPv3 が SSM マッピングと同時に設定できることを示すためにのみ、設定で使用されますが、必須ではありません。
ip igmp explicit-tracking	マルチキャスト チャネルから脱退する IGMPv3 ホストの脱退遅延を最小限に抑えます。 （注） このコマンドは、SSMマッピングの設定には必要ではありません。
ip igmp limit 2	1 つのインターフェイス当たりのベースで、IGMP メンバーシップ状態から生じる IGMP 状態の数を制限します。 （注） このコマンドは、SSMマッピングの設定には必要ではありません。
ip igmp v3lite	このインターフェイスで IGMP v3lite メンバーシップ レポートの受け入れと処理をイネーブルにします。 （注） このコマンドは、IGMP v3lite が SSM マッピングと同時に設定できることを示すためにのみ、設定で使用されますが、必須ではありません。
ip urd	インターフェイスで確保された URD ポート 465 に送信された TCP パケットの代行受信と URD チャネル加入レポートの処理をイネーブルにします。 （注） このコマンドは、URD が SSM マッピングと同時に設定できることを示すためにのみ、設定で使用されますが、必須ではありません。

コマンド	説明
ip pim ssm default	SSM サービスを設定します。 **default** キーワードは SSM 範囲のアクセスリストを 232/8 と定義します。
access-list 10 permit 232.1.2.10 access-list 11 permit 232.1.2.0 0.0.0.255	スタティック SSM マッピングに使用されるよう、ACL を設定します。 （注） これらは、この設定例で **ip igmp ssm-map static** コマンドによって参照される ACL です。

DNS サーバの設定例

DNS ベースの SSM マッピングを設定するには、DNS サーバ ゾーンを作成するか、または既存のゾーンにレコードを追加する必要があります。DNS ベースの SSM マッピングを使用しているルータで、SSM マッピング以外の目的で DNS も使用している場合、通常設定の DNS サーバを使用する必要があります。そのルータで使用されている DNS 実装が DNS ベースの SSM マッピングだけの場合は、ルート ゾーンが空であるか、またはそれ自身を指すような疑似 DNS セットアップが可能です。

次に、ゾーンを作成し、Network Registrar を使用してゾーン データをインポートする例を示します。

```
Router> zone 1.1.232.ssm-map.cisco.com. create primary file=named.ssm-map
100 Ok
Router> dns reload
100 Ok
```

次に、BIND 8 の named.conf ファイルからゾーン ファイルをインポートする例を示します。

```
Router> ::import named.conf /etc/named.conf
Router> dns reload
100 Ok:
```

（注） ネットワーク レジストラ バージョン 8.0 およびそれ以降では、インポート BIND 8 形式の定義がサポートされます。

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。