CHAPTER 11

マルチキャスト ルーティングの設定

この章では、マルチキャスト ルーティングの設定方法について説明します。この項では、次のトピックについて取り上げます。

マルチキャスト ルーティングの概要

セキュリティ アプライアンスは、スタブ マルチキャスト ルーティングと PIM マルチキャスト ルーティングの両方をサポートしています。ただし、1 つのセキュリティ アプライアンスに両方を同時に設定できません。

スタブ マルチキャスト ルーティングは、ダイナミック ホスト登録の機能を提供して、マルチキャスト ルーティングを容易にします。スタブ マルチキャスト ルーティングを設定すると、セキュリティ アプライアンスは IGMP のプロキシ エージェントとして動作します。セキュリティ アプライアンスは、マルチキャスト ルーティングに全面的に参加するのではなく、IGMP メッセージをアップストリームのマルチキャスト ルータに転送し、そのルータがマルチキャスト データの送信をセットアップします。スタブ マルチキャスト ルーティングを設定する場合は、セキュリティ アプライアンスを PIM として設定できません。

セキュリティ アプライアンスは、PIM-SM および双方向 PIM の両方をサポートしています。PIM-SM は、基盤となるユニキャスト ルーティング情報ベースまたは別のマルチキャスト対応ルーティング情報ベースを使用するマルチキャスト ルーティング プロトコルです。このプロトコルは、マルチキャスト グループあたり 1 つのランデブー ポイントをルートにした単方向の共有ツリーを構築し、オプションでマルチキャストの発信元ごとに最短パス ツリーを作成します。

双方向 PIM は PIM-SM の変形で、マルチキャストの発信元と受信者を接続する双方向の共有ツリーを構築します。双方向ツリーは、マルチキャスト トポロジの各リンクで動作する DF 選定プロセスを使用して構築されます。DF に支援されたマルチキャスト データは発信元からランデブー ポイントに転送されます。この結果、マルチキャスト データは発信元固有の状態を必要とせず、共有ツリーをたどって受信者に送信されます。DF 選定はランデブー ポイントの検出中に行われ、これによってデフォルト ルートがランデブー ポイントに提供されます。

（注）　セキュリティ アプライアンスが PIM RP である場合は、セキュリティ アプライアンスの未変換の外部アドレスを RP アドレスとして使用します。

マルチキャスト ルーティングのイネーブル化

マルチキャスト ルーティングをイネーブル化すると、セキュリティ アプライアンス でマルチキャスト パケットを転送できます。マルチキャスト ルーティングをイネーブル化すると、すべてのインターフェイスで PIM と IGMP が自動的にイネーブルになります。マルチキャスト ルーティングをイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# multicast-routing
```

マルチキャスト ルーティング テーブルのエントリの数は、システムに搭載されているメモリの量によって制限されます。表 11-1 に、セキュリティ アプライアンス上のメモリの量に基づく特定のマルチキャスト テーブルのエントリの最大数を示します。この上限に達すると、新しいエントリは廃棄されます。

表 11-1　マルチキャスト テーブルのエントリの制限

テーブル	16 MB	128 MB	128 + MB
MFIB	1000	3000	5000
IGMP グループ	1000	3000	5000
PIM ルート	3000	7000	12000

IGMP 機能の設定

IP ホストは、自身のグループ メンバーシップを直接接続されているマルチキャスト ルータに報告するために IGMP を使用します。IGMP は、グループ アドレス（Class D IP アドレス）をグループ識別子として使用します。ホスト グループ アドレスは、224.0.0.0 ～ 239.255.255.255 の範囲で使用できます。アドレス 224.0.0.0 がグループに割り当てられることはありません。アドレス 224.0.0.1 は、サブネットのシステムすべてに割り当てられます。アドレス 224.0.0.2 は、サブネットのルータすべてに割り当てられます。

セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにすると、IGMP バージョン 2 がすべてのインターフェイスで自動的にイネーブルになります。

（注）　**show run** コマンドを使用すると、インターフェイス コンフィギュレーションには **no igmp** コマンドだけが表示されます。デバイス コンフィギュレーションに **multicast-routing** コマンドがあると、すべてのインターフェイスで IGMP が自動的にイネーブルになります。

ここでは、インターフェイス単位で任意の IGMP 設定を行う方法について説明します。この項では、次のトピックについて取り上げます。

- 「インターフェイスにおける IGMP のディセーブル化」（P.11-15）
- 「グループ メンバーシップの設定」（P.11-15）

インターフェイスにおける IGMP のディセーブル化

IGMP は、特定のインターフェイスでディセーブルにできます。この機能は、マルチキャスト ホストが存在しないことがわかっている特定のインターフェイスにセキュリティ アプライアンスからホスト クエリー メッセージを送信しないようにする場合に便利です。

インターフェイスで IGMP をディセーブルにするには、次のコマンドを入力します。

```
hostname(config-if)# no igmp
```

インターフェイス上で IGMP を再びイネーブルにするには、次のコマンドを入力します。

```
hostname(config-if)# igmp
```

（注）　インターフェイス コンフィギュレーションには、**no igmp** コマンドだけが表示されます。

グループ メンバーシップの設定

セキュリティ アプライアンスをマルチキャスト グループのメンバーとして設定できます。マルチキャスト グループに加入するようにセキュリティ アプライアンスを設定すると、アップストリーム ルータはそのグループのマルチキャスト ルーティング テーブル情報を維持して、このグループをアクティブにするパスを保持します。

セキュリティ アプライアンス をマルチキャスト グループに参加させるには、次のコマンドを入力します。

```
hostname(config-if)# igmp join-group group-address
```

静的に加入するグループの設定

グループ メンバーがグループのメンバーシップをレポートできなかったり、ネットワーク セグメントにグループのメンバーが存在しない場合でも、そのグループのマルチキャスト トラフィックをそのネットワーク セグメントに送信しなければならないことがあります。このような場合、次のいずれかの方法で、そのグループのマルチキャスト トラフィックをセグメントに送信できます。

- **igmp join-group** コマンドを使用（「グループ メンバーシップの設定」（P.11-15）を参照）。セキュリティ アプライアンス はマルチキャスト パケットを受信して転送することができます。
- **igmp static-group** コマンドを使用。セキュリティ アプライアンスは、マルチキャスト パケットを受け入れずに、指定したインターフェイスに転送します。

静的に加入するマルチキャスト グループをインターフェイス上で設定するには、次のコマンドを入力します。

```
hostname(config-if)# igmp static-group group-address
```

マルチキャスト グループへのアクセスの制御

セキュリティ アプライアンスインターフェイス上のホストが加入可能なマルチキャスト グループを制御するには、次の手順を実行します。

ステップ 1　マルチキャスト トラフィックのアクセス リストを作成します。1 つのアクセス リストに複数のエントリを作成することができます。拡張アクセス リストまたは標準アクセス リストを使用できます。

- 標準アクセス リストを作成するには、次のコマンドを入力します。

  ```
  hostname(config)# access-list name standard [permit | deny] ip_addr mask
  ```

  ip_addr 引数は、許可または拒否されるマルチキャスト グループの IP アドレスです。

- 拡張アクセス リストを作成するには、次のコマンドを入力します。

  ```
  hostname(config)# access-list name extended [permit | deny] protocol src_ip_addr
  src_mask dst_ip_addr dst_mask
  ```

  dst_ip_addr 引数は、許可または拒否されるマルチキャスト グループの IP アドレスです。

ステップ 2　次のコマンドを入力して、アクセス リストをインターフェイスに適用します。

```
hostname(config-if)# igmp access-group acl
```

acl 引数は、標準 IP アクセス リストまたは拡張 IP アクセス リストの名前です。

インターフェイスにおける IGMP 状態の数の制限

IGMP メンバーシップ報告の結果の IGMP 状態の数は、インターフェイスごとに制限することができます。設定された上限を超過したメンバーシップ報告は IGMP キャッシュに入力されず、超過した分のメンバーシップ報告のトラフィックは転送されません。

インターフェイスでの IGMP 状態の数を制限するには、次のコマンドを入力します。

```
hostname(config-if)# igmp limit number
```

有効値の範囲は 0 ～ 500 で、デフォルト値は 500 です。この値を 0 に設定すると、学習したグループが追加されなくなりますが、（**igmp join-group** コマンドおよび **igmp static-group** コマンドを使用して）手動で定義したメンバーシップは引き続き許可されます。このコマンドの **no** 形式を使用すると、デフォルト値に戻ります。

クエリー間隔とクエリー タイムアウトの変更

セキュリティ アプライアンスは、クエリー メッセージを送信して、インターフェイスに接続されているネットワークにメンバを持つマルチキャスト グループを検出します。メンバは、IGMP 報告メッセージで応答して、特定のグループに対するマルチキャスト パケットの受信を希望していることを示します。クエリー メッセージは、アドレスが 224.0.0.1 で存続可能時間値が 1 の全システム マルチキャスト グループ宛に送信されます。

これらのメッセージが定期的に送信されることにより、セキュリティ アプライアンスに保存されているメンバーシップ情報はリフレッシュされます。セキュリティ アプライアンスで、ローカル メンバーがいなくなったマルチキャスト グループがまだインターフェイスに接続されていることがわかると、そのグループへのマルチキャスト パケットを接続されているネットワークに転送するのを停止し、そのパケットの送信元にプルーニング メッセージを戻します。

デフォルトでは、サブネット上の PIM 指定ルータがクエリー メッセージの送信を担当します。このメッセージは、デフォルトでは 125 秒間に 1 回送信されます。この間隔を変更するには、次のコマンドを入力します。

```
hostname(config-if)# igmp query-interval seconds
```

指定されたタイムアウト値（デフォルトは 255 秒）の間にインターフェイス上でクエリー メッセージがセキュリティ アプライアンスによって検出されないと、セキュリティ アプライアンスが指定ルータになり、クエリー メッセージの送信を開始します。このタイムアウト値を変更するには、次のコマンドを入力します。

```
hostname(config-if)# igmp query-timeout seconds
```

（注）　**igmp query-timeout** コマンドおよび **igmp query-interval** コマンドを実行するには、IGMP バージョン 2 が必要です。

クエリー応答時間の変更

デフォルトでは、IGMP クエリーでアドバタイズされる最大クエリー応答時間は 10 秒です。セキュリティ アプライアンスがこの時間内にホスト クエリーの応答を受信しなかった場合、グループを削除します。

最大クエリー応答時間を変更するには、次のコマンドを入力します。

```
hostname(config-if)# igmp query-max-response-time seconds
```

IGMP バージョンの変更

デフォルトでは、セキュリティ アプライアンス は IGMP Version 2 を実行します。このプロトコルにより、**igmp query-timeout** コマンドや **igmp query-interval** コマンドなど複数の追加機能がイネーブルになります。

サブネットのマルチキャスト ルータはすべて、同じ IGMP バージョンをサポートしている必要があります。セキュリティ アプライアンスは、バージョン 1 ルータを自動的に検出してバージョン 1 に切り替えることはありません。しかし、サブネットに IGMP のバージョン 1 のホストとバージョン 2 のホストが混在しても問題はありません。IGMP バージョン 2 を実行しているセキュリティ アプライアンスは、IGMP バージョン 1 のホストが存在しても正常に動作します。

インターフェイスで動作中の IGMP のバージョンを制御するには、次のコマンドを入力します。

```
hostname(config-if)# igmp version {1 | 2}
```

スタブ マルチキャスト ルーティングの設定

スタブ エリアへのゲートウェイとして動作しているセキュリティ アプライアンスは、PIM に参加する必要はありません。その代わりに、そのセキュリティ アプライアンスを IGMP プロキシ エージェントとして設定すると、あるインターフェイスに接続されているホストから、別のインターフェイスのアップストリーム マルチキャスト ルータに IGMP メッセージを転送することができます。セキュリティ アプライアンスを IGMP プロキシ エージェントとして設定するには、ホスト加入（join）メッセージおよびホスト脱退（leave）メッセージをスタブ エリアからアップストリーム インターフェイスに転送します。

ホスト加入メッセージおよびホスト脱退メッセージを転送するには、スタブ エリアに接続されているインターフェイスから次のコマンドを入力します。

```
hostname(config-if)# igmp forward interface if_name
```

（注） スタブ マルチキャスト ルーティングと PIM は同時にはサポートされません。

UDP と非 UDP の両方のトランスポートがマルチキャスト ルーティングに対してサポートされます。ただし、非 UDP トランスポートでは FastPath 最適化は行われません。

スタティック マルチキャスト ルートの設定

PIM を使用する場合、セキュリティ アプライアンスは、ユニキャスト パケットを発信元に返送するときと同じインターフェイスでパケットを受信することを想定しています。マルチキャスト ルーティングをサポートしていないルートをバイパスする場合などは、ユニキャスト パケットで 1 つのパスを使用し、マルチキャスト パケットで別の 1 つのパスを使用することもあります。

スタティック マルチキャスト ルートはアドバタイズも再配布もされません。

PIM 用のスタティック マルチキャスト ルートを設定するには、次のコマンドを入力します。

```
hostname(config)# mroute src_ip src_mask {input_if_name | rpf_addr) [distance]
```

スタブ エリア用のスタティック マルチキャスト ルートを設定するには、次のコマンドを入力します。

```
hostname(config)# mroute src_ip src_mask input_if_name [dense output_if_name] [distance]
```

（注） **dense** *output_if_name* キーワードと引数のペアは、スタブ マルチキャスト ルーティングだけでサポートされます。

PIM 機能の設定

ルータは、PIM を使用してマルチキャスト ダイアグラムを転送する転送テーブルを維持します。セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにすると、PIM および IGMP がすべてのインターフェイスで自動的にイネーブルになります。

（注） PIM は、PAT ではサポートされません。PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルに対してのみ動作します。

ここでは、任意の PIM 設定を行う方法について説明します。この項では、次のトピックについて取り上げます。

インターフェイス上での PIM のディセーブル化

特定のインターフェイスで PIM をディセーブルにできます。インターフェイス上で PIM をディセーブルにするには、次のコマンドを入力します。

```
hostname(config-if)# no pim
```

インターフェイス上で PIM を再びイネーブルにするには、次のコマンドを入力します。

```
hostname(config-if)# pim
```

（注）　インターフェイス コンフィギュレーションには、**no pim** コマンドだけが表示されます。

スタティック ランデブー ポイント アドレスの設定

共通の PIM スパース モードまたは双方向ドメイン内のルータはすべて、PIM RP アドレスを認識している必要があります。このアドレスは、**pim rp-address** コマンドを使用してスタティックに設定されます。

（注）　セキュリティ アプライアンス は Auto-RP や PIM BSR をサポートしていないため、ユーザは **pimrp-address** コマンドを使用して RP アドレスを指定する必要があります。

セキュリティ アプライアンスを複数のグループの RP として機能するように設定することができます。アクセス リストに指定されているグループ範囲によって、PIM RP のグループ マッピングが決まります。アクセス リストが指定されていない場合は、マルチキャスト グループ全体の範囲（224.0.0.0/4）にグループの RP が適用されます。

PIM PR のアドレスを設定するには、次のコマンドを入力します。

```
hostname(config)# pim rp-address ip_address [acl] [bidir]
```

ip_address 引数は、PIM RP となるルータのユニキャスト IP アドレスです。*acl* 引数は、RP とともに使用する必要があるマルチキャスト グループを定義している標準アクセス リストの名前または番号です。このコマンドではホスト ACL を使用しないでください。**bidir** キーワードを除外すると、グループは PIM スパース モードで動作するようになります。

（注）　セキュリティ アプライアンスは、実際の双方向コンフィギュレーションとは関係なく、常に双方向機能を PIM hello メッセージ内でアドバタイズします。

指定ルータのプライオリティの設定

Designated Router（DR; 代表ルータ）は、PIM 登録メッセージ、PIM 加入メッセージ、およびプルーニング メッセージの RP への送信を担当します。ネットワーク セグメントに 2 つ以上のマルチキャスト ルータがある場合、DR のプライオリティに基づいて DR を選定するプロセスがあります。複数のデバイスの DR プライオリティが等しい場合、最上位の IP アドレスを持つデバイスが DR になります。

デフォルトでは、セキュリティ アプライアンスの DR プライオリティは 1 です。次のコマンドを入力して、この値を変更できます。

```
hostname(config-if)# pim dr-priority num
```

num は 1 ～ 4294967294 の任意の数字にできます。

PIM 登録メッセージのフィルタリング

PIM 登録メッセージをフィルタリングするように セキュリティ アプライアンス を設定できます。PIM 登録メッセージをフィルタリングするには、次のコマンドを入力します。

```
hostname(config)# pim accept-register {list acl | route-map map-name}
```

PIM メッセージ間隔の設定

ルータ クエリー メッセージは、PIM DR の選択に使用されます。PIM DR は、ルータ クエリー メッセージを送信します。デフォルトでは、ルータ クエリー メッセージは 30 秒間隔で送信されます。次のコマンドを入力して、この値を変更できます。

```
hostname(config-if)# pim hello-interval seconds
```

seconds 引数の有効な値は 1 ～ 3600 秒です。

セキュリティ アプライアンスは 60 秒ごとに PIM ジョイン/Prune メッセージを送信します。この値を変更するには、次のコマンドを入力します。

```
hostname(config-if)# pim join-prune-interval seconds
```

seconds 引数の有効な値は 10 ～ 600 秒です。

マルチキャスト境界の設定

アドレス スコーピングは、同じ IP アドレスを持つ RP が含まれるドメインが相互にデータを漏出させることのないように、ドメイン境界を定義します。スコーピングは、大きなドメイン内のサブネット境界や、ドメインとインターネットの間の境界で実行されます。

multicast boundary コマンドを使用して、インターフェイスでマルチキャスト グループ アドレスの管理スコープ境界を設定できます。IANA では、マルチキャスト アドレス範囲の 239.0.0.0 ～ 239.255.255.255 を管理スコープ アドレスに指定しています。この範囲のアドレスは、さまざまな組織で管理されるドメイン内で再使用されます。これらは、グローバルに一意ではなくローカルとみなされます。

マルチキャスト境界を設定するには、次のコマンドを入力します。

```
hostname(config-if)# multicast boundary acl [filter-autorp]
```

標準 ACL では、影響を受けるアドレスの範囲を定義します。境界が設定されると、マルチキャスト データ パケットは境界を越えて出入りできなくなります。境界を定めることで、同じマルチキャスト グループ アドレスをさまざまな管理ドメイン内で使用できます。

filter-autorp キーワードを設定して、管理用スコープの境界で Auto-RP 検出と通知メッセージを検査し、フィルタできます。境界のアクセス コントロール リスト（ACL）に拒否された Auto-RP パケットからの Auto-RP グループ範囲通知は削除されます。Auto-RP グループ範囲通知は、Auto-RP グループ範囲のすべてのアドレスが境界 ACL によって許可される場合に限り境界を通過できます。許可されないアドレスがある場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージが転送される前に Auto-RP メッセージから削除されます。

PIM ネイバーのフィルタリング

PIM ネイバーにできるルータは、**pim neighbor-filter** コマンドで定義できます。PIM ネイバーにできるルータをフィルタリングすると、次の制御を行うことができます。

- 許可されていないルータが PIM ネイバーにならないようにする。
- 添付されたスタブ ルータが PIM に参加できないようにする。

PIM ネイバーとして設定可能なネイバーを定義するには、次の手順を実行します。

ステップ 1　**access-list** コマンドを使用して、PIM への参加を許可するルータを定義した標準アクセス リストを定義します。

たとえば、**pim neighbor-filter** コマンドと一緒に次のアクセス リストを使用すると、10.1.1.1 ルータを PIM ネイバーとして設定できなくなります。

```
hostname(config)# access-list pim_nbr deny 10.1.1.1 255.255.255.255
```

ステップ 2　**pim neighbor-filter** コマンドをインターフェイスで使用して、隣接ルータをフィルタリングします。

たとえば、次のコマンドを使用すると、GigabitEthernet0/3 インターフェイスで 10.1.1.1 ルータを PIM ネイバーとして設定できません。

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pim neighbor-filter pim_nbr
```

混合双方向およびスパース モード PIM ネットワークのサポート

双方向 PIM では、マルチキャスト ルータで保持するステート情報を減らすことができます。1 つのセグメント内のマルチキャスト ルータすべては、双方向で DF を選定できるようにするため、双方向でイネーブルになっている必要があります。

pim bidir-neighbor-filter コマンドを使用すると、スパース モード専用ネットワークから双方向ネットワークへの移行が可能になります。この場合、すべてのルータのスパース モード ドメインへの参加を許可しながら、DF 選出へ参加しなければならないルータを指定します。双方向にイネーブルにされたルータは、セグメントに非双方向ルータがある場合でも、それらのルータの中から DF を選定できます。非双方向ルータ上のマルチキャスト境界により、双方向グループから PIM メッセージやデータが双方向サブセット クラウドに出入りできないようにします。

pim bidir-neighbor-filter コマンドがイネーブルの場合、ACL で許可されているルータは双方向対応であると見なされます。したがって、次のようにします。

- 許可されたネイバーが双方向対応でない場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向対応である場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向をサポートしない場合、DF 選定が実行されます。

DF 選定に参加できるネイバーを制御するには、次の手順を実行します。

ステップ 1　**access-list** コマンドを使用して、標準アクセス リストを定義します。このアクセス リストは、DF 選定に参加させるルータを許可し、その他をすべて拒否します。

たとえば、次のアクセス リストでは、10.1.1.1 および 10.2.2.2 のルータが DF 選定に参加するのを許可し、その他をすべて拒否します。

```
hostname(config)# access-list pim_bidir permit 10.1.1.1 255.255.255.255
hostname(config)# access-list pim_bidir permit 10.1.1.2 255.255.255.255
hostname(config)# access-list pim_bidir deny any
```

ステップ 2　インターフェイスで **pim bidir-neighbor-filter** コマンドをイネーブルにします。

次の例では、前のステップで作成されたアクセス リストを GigabitEthernet0/3 インターフェイスに適用しています。

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pim bidir-neighbor-filter pim_bidir
```

マルチキャスト ルーティングの参考資料

次の Internet Engineering Task Force（IETF）による RFC には、SMR 機能を実装するための、IGMP 規格およびマルチキャスト ルーティング規格に関する技術的な詳細が示されています。

- RFC 2236 IGMPv2
- RFC 2362 PIM-SM
- RFC 2588 IP マルチキャストとファイアウォール
- RFC 2113 IP ルータ アラート オプション
- IETF draft-ietf-idmr-igmp-proxy-01.txt