CHAPTER 9

IP ルーティングの設定

この章では、セキュリティ アプライアンスの IP ルーティングの設定方法について説明します。この章は、次の項で構成されています。

ASA セキュリティ アプライアンス内のルーティングのしくみ

ASA セキュリティ アプライアンスは、ルーティングの決定にルーティング テーブルと XLATE テーブルの両方を使用します。宛先 IP 変換済みトラフィック、つまり変換されていないトラフィックを扱うために、ASA は既存の XLATE またスタティック トランスレーションを検索して、出力インターフェイスを選択します。選択プロセスは次のとおりです。

出力インターフェイスの選択プロセス

1. 宛先 IP を変換する XLATE がすでに存在する場合は、パケットの出力インターフェイスは、ルーティング テーブルではなく XLATE テーブルから決定されます。
2. 宛先 IP を変換する XLATE が存在せず、一致するスタティック変換が存在する場合は、出力インターフェイスはスタティック ルートから決定されて XLATE が作成され、ルーティング テーブルは使用されません。
3. 宛先 IP を変換する XLATE が存在せず、一致するスタティック変換も存在しない場合は、パケットの宛先 IP 変換は実行されません。セキュリティ アプライアンスは、ルートをルックアップして出力インターフェイスを選択することでこのパケットを処理し、次に発信元 IP 変換が（必要に応じて）実行されます。

通常のダイナミック発信 NAT では、最初の発信パケットは、ルート テーブルを使用し、XLATE を作成することでルーティングされます。着信返送パケットは、既存の XLATE だけを使用して転送されます。スタティック NAT では、宛先変換された着信パケットは、常に既存の XLATE またはスタティック変換ルールを使用して転送されます。

ネクスト ホップの選択プロセス

前述のいずれかの方法を使用して出力インターフェイスを選択した後、さらにルート ルックアップが実行され、これまでに選択した出力インターフェイスに属する適切なネクスト ホップが検出されます。選択されたインターフェイスに明示的に属するルートがルーティング テーブルに存在しない場合、パケットは廃棄され、レベル 6 のエラー メッセージ 110001（「no route to host」）が生成されます。これは、所定の宛先ネットワーク用として、他の出力インターフェイスに属する別のルートが存在する場合でも同様です。選択した出力インターフェイスに属するルートが見つかると、パケットは対応するネクスト ホップに転送されます。

セキュリティ アプライアンスでのロード シェアリングは、1 つの出力インターフェイスを使用して複数のネクストホップが使用できる場合に限り可能です。ロード シェアリングでは、複数の出力インターフェイスの共有はできません。

ダイナミック ルーティングがセキュリティ アプライアンスで使用されており、XLATE の作成後にルート テーブルが変更された場合も（ルート フラップなど）、宛先変換トラフィックは、XLATE がタイムアウトするまでは、ルート テーブルではなく古い XLATE を使用して転送されます。古いルートが古いインターフェイスから削除され、ルーティング プロセスによって別のインターフェイスに接続された場合、トラフィックは不適切なインターフェイスに転送されるか、または廃棄されてメッセージ 110001（「no route to host」）が生成される可能性があります。

セキュリティ アプライアンス自体でルート フラップが発生していないにもかかわらず、その周りで一部のルーティング プロセスがフラッピングし、発信元変換された、同じフローに属するパケットを、別のインターフェイスを使用してセキュリティ アプライアンス経由で送信する場合は、同様の問題が発生することがあります。宛先変換された返送パケットは、間違った出力インターフェイスを使用して戻されることがあります。

この問題は、フローの最初のパケットの方向に応じて、実質的にすべてのトラフィックを発信元変換または宛先変換できる同じセキュリティ トラフィック構成では、高い確率で発生します。ルート フラップ後にこの問題が発生した場合、**clear xlate** コマンドを使用して手動で解決するか、XLATE タイムアウトによって自動的に解決できます。XLATE のタイムアウトは、必要に応じて小さくできます。この問題がほとんど発生しないようにするには、セキュリティ アプライアンスやその周りでルート フラップが発生しないようにします。つまり、同じフローに属する宛先変換されたパケットが、セキュリティ アプライアンスを通じて常に同じ方法で転送されるようにします。

スタティック ルートおよびデフォルト ルートの設定

この項では、セキュリティ アプライアンスにスタティック ルートとデフォルト ルートを設定する方法について説明します。

マルチ コンテキスト モードではダイナミック ルーティングがサポートされていないため、ネットワークとセキュリティ アプライアンスとの間にルータが入っている場合など、セキュリティ アプライアンスに直接接続されていないネットワークでは、すべてスタティック ルートを使用する必要があります。

次の場合は、シングル コンテキスト モードでスタティック ルートを使用します。

- ネットワークで RIP または OSPF 以外の Router Discovery Protocol を使用する場合
- ネットワークが小規模でスタティック ルートを容易に管理できる。

- ルーティング プロトコルが関係するトラフィックまたは CPU のオーバーヘッドをなくす必要がある。

最も単純なオプションは、すべてのトラフィックをアップストリーム ルータに送信するようにデフォルト ルートを設定して、トラフィックのルーティングをルータに任せることです。しかし、デフォルトのゲートウェイでは宛先ネットワークに到達できない場合があるため、スタティック ルートをさらに詳しく設定する必要があります。たとえば、デフォルトのゲートウェイが外部の場合、デフォルト ルートは、セキュリティ アプライアンス に直接接続されていない内部ネットワークにはまったくトラフィックを転送できません。

トランスペアレント ファイアウォール モードでは、セキュリティ アプライアンスから直接接続されていないネットワークに宛てたトラフィック用にデフォルト ルートまたはスタティック ルートを設定して、セキュリティ アプライアンスがトラフィックの送信先インターフェイスを認識できるようにする必要があります。セキュリティ アプライアンスから発信されるトラフィックには、syslog サーバ、Websense サーバまたは N2H2 サーバ、あるいは AAA サーバとの通信もあります。1 つのデフォルト ルートで到達できないサーバがある場合、スタティック ルートを設定する必要があります。

セキュリティ アプライアンス では、ロード バランシングのために、1 つのインターフェイスあたり最大 3 つの等コスト ルートをサポートします。

この項では、次のトピックについて取り上げます。

- 「スタティック ルートの設定」（P.9-3）
- 「デフォルト ルートの設定」（P.9-4）
- 「スタティック ルート トラッキングの設定」（P.9-5）

IPv6 スタティック / デフォルト ルートの設定の詳細については、「IPv6 デフォルト ルートおよびスタティック ルートの設定」（P.12-5）を参照してください。

スタティック ルートの設定

スタティック ルートを追加するには、次のコマンドを入力します。

```
hostname(config)# route if_name dest_ip mask gateway_ip [distance]
```

dest_ip および *mask* は宛先ネットワークの IP アドレスで、*gateway_ip* はネクストホップ ルータです。スタティック ルートに指定するアドレスは、セキュリティ アプライアンスに到達して NAT を実行する前のパケットにあるアドレスです。

distance は、ルートのアドミニストレーティブ ディスタンスです。値を指定しない場合、デフォルトは 1 です。アドミニストレーティブ ディスタンスは、複数のルーティング プロトコル間でルートを比較するのに使用されるパラメータです。スタティック ルートのデフォルトのアドミニストレーティブ ディスタンスは 1 で、ダイナミック ルーティング プロトコルで検出されるルートより優先されますが、直接には接続されていないルートです。OSPF で検出されるルートのデフォルトのアドミニストレーティブ ディスタンスは 110 です。スタティック ルートとダイナミック ルートのアドミニストレーティブ ディスタンスが同じ場合、スタティック ルートが優先されます。接続されているルートは常に、スタティック ルートおよびダイナミックに検出されたルートのどちらよりも優先されます。

スタティック ルートは、指定されたゲートウェイが利用できなくなってもルーティング テーブルに保持されています。指定されたゲートウェイが利用できなくなった場合は、スタティック ルートをルーティング テーブルから手動で削除する必要があります。しかし、スタティック ルートは、指定されたインターフェイスがダウンした場合はルーティング テーブルから削除されます。インターフェイスが元に戻ると、スタティック ルートは復旧します。

（注） セキュリティ アプライアンス で動作中のルーティング プロトコルのアドミニストレーティブ ディスタンスよりも長いアドミニストレーティブ ディスタンスを指定してスタティック ルートを作成すると、ルーティング プロトコルで検出される指定の宛先へのルートがスタティック ルートより優先されます。スタティック ルートは、ダイナミックに検出されたルートがルーティング テーブルから削除された場合に限り使用されます。

次に、10.1.1.0/24 宛てのすべてのトラフィックを、内部インターフェイスに接続されたルータ（10.1.2.45）に送信するスタティック ルートを作成する例を示します。

```
hostname(config)# route inside 10.1.1.0 255.255.255.0 10.1.2.45 1
```

インターフェイスごとに同じ宛先でコストの等しいルートを 3 つまで定義できます。ECMP は複数のインターフェイス間ではサポートされていません。ECMP では、トラフィックは必ずしもルート間で均等に分割されるわけではありません。トラフィックは、送信元 IP アドレスおよび宛先 IP アドレスをハッシュするアルゴリズムに基づいて、指定したゲートウェイ間に分配されます。

次に、外部インターフェイス上の 3 台のゲートウェイにトラフィックを転送する、コストの等しいスタティック ルートの例を示します。セキュリティ アプライアンスは、指定された複数のゲートウェイ間にトラフィックを分散します。

```
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.2
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.3
```

デフォルト ルートの設定

デフォルト ルートは、既知のルートもスタティック ルートも指定されていない IP パケットすべてを、セキュリティ アプライアンスが送信するゲートウェイの IP アドレスを特定するルートです。デフォルト ルートは、宛先 IP アドレスが 0.0.0.0/0 のスタティック ルートです。特定の宛先が特定されたルートはデフォルト ルートより優先されます。

（注） ASA ソフトウェア バージョン 7.0 以降で、異なるメトリックを持つ個別のインターフェイス上で 2 つのデフォルト ルートが設定されている場合は、それよりも大きいメトリックを持つインターフェイスから ASA ファイアウォールへの接続は失敗しますが、小さいメトリックを持つインターフェイスからの ASA ファイアウォールへの接続は予期したとおりに成功します。PIX ソフトウェア バージョン 6.3 では、高位および低位メトリック インターフェイスからの接続をサポートしています。

デバイスあたり最大 3 つの等コスト デフォルト ルート エントリを定義することができます。複数の等コスト デフォルト ルート エントリを定義すると、デフォルト ルートに送信されるトラフィックは、指定されたゲートウェイの間に分散されます。複数のデフォルト ルートを定義する場合は、各エントリに同じインターフェイスを指定する必要があります。

コストの等しいデフォルト ルート エントリを 3 つより多く定義しようとすると、または定義済みのデフォルト ルートとは異なるインターフェイスでデフォルト ルートを定義しようとすると、「ERROR: Cannot add route entry, possible conflict with existing routes.」というメッセージが表示されます。

トンネル トラフィックには、標準のデフォルト ルートの他に別のデフォルト ルートを 1 つ定義することができます。**tunneled** オプションを使用してデフォルト ルートを作成すると、セキュリティ アプライアンスで終端するトンネルからのすべてのトラフィックは、学習したルートまたはスタティック

ルートを使用してルーティングできない場合、このルートに送信されます。トンネルから出るトラフィックの場合、このルートは、その他の設定または学習されたデフォルト ルートをすべて上書きします。

tunneled オプションを使用したデフォルト ルートには、次の制約事項が適用されます。

- トンネル ルートの出力インターフェイスで、ユニキャスト RPF（**ip verify reverse-path**）をイネーブルにしないでください。トンネル ルートの出力インターフェイスで uRPF をイネーブルにすると、セッションに障害が発生します。
- トンネル ルートの出力インターフェイスで、TCP 代行受信をイネーブルにしないでください。イネーブルにすると、セッションでエラーが発生します。
- VoIP インスペクション エンジン（CTIQBE、H.323、GTP、MGCP、RTSP、SIP、SKINNY）、DNS インスペクション エンジン、または DCE RPC インスペクション エンジンは、トンネル ルートでは使用しないでください。これらのインスペクション エンジンは、トンネル ルートを無視します。

[tunneled] オプションを使用して複数のデフォルト ルートは定義できません。トンネル トラフィックの ECMP はサポートされていません。

デフォルト ルートを定義するには、次のコマンドを入力します。

```
hostname(config)# route if_name 0.0.0.0 0.0.0.0 gateway_ip [distance | tunneled]
```

ヒント　宛先ネットワーク アドレスおよびマスクとして、0.0.0.0 0.0.0.0 の代わりに 0 0 と入力することができます。たとえば、次のように入力します。`hostname(config)# route outside 0 0 192.168.1 1`

次の例は、セキュリティ アプライアンスに 3 つの等コスト デフォルト ルートとトンネル トラフィック用のデフォルト ルート 1 つを設定しています。セキュリティ アプライアンスで受信した非暗号化トラフィックは、スタティック ルートも既知のルートも指定されていない場合、IP アドレスが 192.168.2.1、192.168.2.2、192.168.2.3 のゲートウェイの間に分散されます。セキュリティ アプライアンスで受信した暗号化されたトラフィックは、スタティック ルートも既知のルートも指定されていない場合、IP アドレス 192.168.2.4 のゲートウェイに転送されます。

```
hostname(config)# route outside 0 0 192.168.2.1
hostname(config)# route outside 0 0 192.168.2.2
hostname(config)# route outside 0 0 192.168.2.3
hostname(config)# route outside 0 0 192.168.2.4 tunneled
```

スタティック ルート トラッキングの設定

スタティック ルートの問題の 1 つは、ルートがアップ状態なのかダウン状態なのかを判定する固有のメカニズムがないことです。スタティック ルートは、ネクスト ホップ ゲートウェイが使用できなくなった場合でも、ルーティング テーブルに保持されています。スタティック ルートは、セキュリティ アプライアンス 上の関連付けられたインターフェイスがダウンした場合に限りルーティング テーブルから削除されます。

スタティック ルート トラッキング機能には、スタティック ルートの使用可能状況を追跡し、プライマリ ルートがダウンした場合のバックアップ ルートをインストールするための方式が用意されています。これを利用すると、たとえば、ISP ゲートウェイへのデフォルト ルートを定義し、プライマリ ISP が使用できなくなった場合に備えて、セカンダリ ISP へのバックアップ用のデフォルト ルートを定義することができます。

セキュリティ アプライアンスでは、定義されたモニタリング対象にスタティック ルートを関連付けることで、この機能を実行します。対象のモニタリングは、ICMP エコー要求を使用して行います。指定された時間内にエコー応答がない場合は、そのオブジェクトはダウンしていると見なされ、関連付けられたルートはルーティング テーブルから削除されます。削除されたルートに代わって、すでに定義されているバックアップ ルートが使用されます。

モニタリング対象の選択時には、その対象が ICPM エコー要求に応答できることを確認してください。対象には任意のネットワーク オブジェクトを選択できますが、次のものを使用することを検討する必要があります。

- ISP ゲートウェイ アドレス（デュアル ISP サポート用）
- ネクスト ホップ ゲートウェイ アドレス（ゲートウェイの使用可能状況に懸念がある場合）
- セキュリティ アプライアンスが通信を行う必要のある対象ネットワーク上のサーバ（AAA サーバなど）
- 宛先ネットワーク上の永続的なネットワーク オブジェクト（夜間にシャットダウンするデスクトップ PC やノートブック PC は適しません）

スタティック ルート トラッキングは、スタティックに定義されたルートや、DHCP または PPPoE を通じて取得したデフォルト ルートに対して設定することができます。ルート トラッキングでは、複数のインターフェイス上の PPPoE クライアントだけをイネーブルにすることができます。

スタティック ルート トラッキングを設定するには、次の手順を実行します。

ステップ 1　追跡対象オブジェクトのモニタリング パラメータを設定します。

a. モニタリング プロセスを次のように定義します。

```
hostname(config)# sla monitor sla_id
```

新しいモニタリング プロセスを設定する場合は、SLA モニタ コンフィギュレーション モードになります。タイプが定義済みでスケジュールが未設定のモニタリング プロセスのモニタリング パラメータを変更する場合は、直接、SLA プロトコル コンフィギュレーション モードになります。

b. モニタリング プロトコルを指定します。タイプが定義済みでスケジュールが未設定のモニタリング プロセスのモニタリング パラメータを変更する場合は、直接、SLA プロトコル コンフィギュレーション モードになり、この設定は変更できません。

```
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho target_ip interface
if_name
```

target_ip は、トラッキング プロセスによって使用可能かどうかをモニタされるネットワーク オブジェクトの IP アドレスです。このオブジェクトが使用可能な場合、トラッキング プロセス ルートがルーティング テーブルにインストールされます。このオブジェクトが使用できない場合、トラッキング プロセスがルートを削除し、代わりにバックアップ ルートが使用されます。

c. モニタリング プロセスのスケジュールを設定します。

```
hostname(config)# sla monitor schedule sla_id [life {forever | seconds}] [start-time
{hh:mm[:ss] [month day | day month] | pending | now | after hh:mm:ss}] [ageout
seconds] [recurring]
```

一般的に、モニタリング スケジュールには **sla monitor schedule** *sla_id* **life forever start-time now** を使用し、モニタリング コンフィギュレーションがテスト頻度を判別できるようにします。ただし、このモニタリング プロセスを将来開始するようにしたり、指定した時刻だけに実行されるようにスケジュールを設定したりできます。

ステップ 2　次のコマンドを入力して、追跡されるスタティック ルートを SLA モニタリング プロセスに関連付けます。

```
hostname(config)# track track_id rtr sla_id reachability
```

track_id は、このコマンドで割り当てるトラッキング番号です。*sla_id* は、ステップ 1 で定義した SLA プロセスの ID 番号です。

ステップ 3　次のいずれかのオプションを指定して、追跡されるオブジェクトが到達可能な場合にルーティング テーブルにインストールするスタティック ルートを定義します。

- スタティック ルートを追跡するには、次のコマンドを入力します。

```
hostname(config)# route if_name dest_ip mask gateway_ip [admin_distance] track
track_id
```

スタティック ルート トラッキングでは、**route** コマンドに **tunneled** オプションを使用できません。

- DHCP から取得したデフォルト ルートを追跡するには、次のコマンドを入力します。

```
hostname(config)# interface phy_if
hostname(config-if)# dhcp client route track track_id
hostname(config-if)# ip addresss dhcp setroute
hostname(config-if)# exit
```

（注） DHCP を使用してデフォルト ルートを取得するには、**ip address dhcp** コマンドで **setroute** 引数を使用する必要があります。

- PPPoE から取得したデフォルト ルートを追跡するには、次のコマンドを入力します。

```
hostname(config)# interface phy_if
hostname(config-if)# pppoe client route track track_id
hostname(config-if)# ip addresss pppoe setroute
hostname(config-if)# exit
```

（注） PPPoE を使用してデフォルト ルートを取得するには、**ip address pppoe** コマンドで **setroute** 引数を使用する必要があります。

ステップ 4　次のいずれかのオプションを指定して、追跡されるオブジェクトが使用できないときに使用するバックアップ ルートを定義します。バックアップ ルートのアドミニストレーティブ ディスタンスは、追跡されるルートのアドミニストレーティブ ディスタンスよりも大きくなければなりません。大きくない場合は、追跡されるルートではなくバックアップ ルートがルーティング テーブルにインストールされます。

- スタティック ルートを使用するには、次のコマンドを入力します。

```
hostname(config)# route if_name dest_ip mask gateway_ip [admin_distance]
```

スタティック ルートの宛先とマスクは、追跡されるルートと同じものでなければなりません。DHCP または PPPoE から取得したデフォルト ルートを追跡する場合、アドレスとマスクは 0.0.0.0 0.0.0.0 です。

- DHCP から取得したデフォルト ルートを使用するには、次のコマンドを入力します。

```
hostname(config)# interface phy_if
hostname(config-if)# dhcp client route track track_id
hostname(config-if)# dhcp client route distance admin_distance
hostname(config-if)# ip addresss dhcp setroute
hostname(config-if)# exit
```

DHCP を使用してデフォルト ルートを取得するには、**ip address dhcp** コマンドで **setroute** 引数を使用する必要があります。アドミニストレーティブ ディスタンスが、追跡されるルートのアドミニストレーティブ ディスタンスより大きいことを確認します。

- PPPoE から取得したデフォルト ルートを使用するには、次のコマンドを入力します。

```
hostname(config)# interface phy_if
hostname(config-if)# pppoe client route track track_id
hostname(config-if)# pppoe client route distance admin_distance
hostname(config-if)# ip addresss pppoe setroute
hostname(config-if)# exit
```

PPPoE を使用してデフォルト ルートを取得するには、**ip address pppoe** コマンドで **setroute** 引数を使用する必要があります。アドミニストレーティブ ディスタンスが、追跡されるルートのアドミニストレーティブ ディスタンスより大きいことを確認します。

ルート マップの定義

ルート マップは、ルートを OSPF または RIP ルーティング プロセスに再配布するときに使用します。また、デフォルト ルートを OSPF ルーティング プロセスに生成するときにも使用します。ルート マップは、指定されたルーティング プロトコルのどのルートを対象ルーティング プロセスに再配布できるのかを定義します。

ルート マップを定義するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、ルート マップ エントリを作成します。

```
hostname(config)# route-map name {permit | deny} [sequence_number]
```

ルート マップのエントリは順番に読み取られます。この順序は、*sequence_number* オプションを使用して指定できます。このオプションで指定しなければ、エントリを追加した順序がセキュリティ アプライアンスで使用されます。

ステップ 2　1 つまたは複数の **match** コマンドを入力します。

- 標準の ACL に一致する宛先ネットワークを持つ任意のルートを照合するには、次のコマンドを入力します。

```
hostname(config-route-map)# match ip address acl_id [acl_id] [...]
```

複数の ACL を指定する場合、ルートは任意の ACL を照合できます。

- メトリックが指定されたルートを照合する場合は、次のコマンドを入力します。

```
hostname(config-route-map)# match metric metric_value
```

metric_value には、0 ～ 4294967295 が指定できます。

- 標準の ACL に一致するネクスト ホップ ルータ アドレスを持つ任意のルートを照合するには、次のコマンドを入力します。

```
hostname(config-route-map)# match ip next-hop acl_id [acl_id] [...]
```

複数の ACL を指定する場合、ルートは任意の ACL を照合できます。

- ネクスト ホップ インターフェイスが指定されているルートを照合する場合は、次のコマンドを入力します。

```
hostname(config-route-map)# match interface if_name
```

2 つ以上のインターフェイスを指定する場合、ルートはいずれかのインターフェイスと一致します。

- 標準の ACL と一致するルータによってアドバタイズされている任意のルートを照合するには、次のコマンドを入力します。

```
hostname(config-route-map)# match ip route-source acl_id [acl_id] [...]
```

複数の ACL を指定する場合、ルートは任意の ACL を照合できます。

- ルート タイプを照合する場合は、次のコマンドを入力します。

```
hostname(config-route-map)# match route-type {internal | external [type-1 | type-2]}
```

ステップ 3　1 つまたは複数の **set** コマンドを入力します。

ルートが **match** コマンドで一致する場合は、次の **set** コマンドによって、ルートを再配布する前にルートで実行するアクションが決まります。

- メトリックを設定する場合は、次のコマンドを入力します。

```
hostname(config-route-map)# set metric metric_value
```

metric_value には 0 ～ 294,967,295 の任意の値を指定できます。

- メトリック タイプを設定する場合は、次のコマンドを入力します。

```
hostname(config-route-map)# set metric-type {type-1 | type-2}
```

次の例は、ホップ カウント 1 でルートを OSPF に再配布する方法を示しています。セキュリティ アプライアンスは、これらのルートをメトリック 5、メトリック タイプ 1 で外部 LSA として再配布します。

```
hostname(config)# route-map 1-to-2 permit
hostname(config-route-map)# match metric 1
hostname(config-route-map)# set metric 5
hostname(config-route-map)# set metric-type type-1
```

OSPF の設定

ここでは、OSPF 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。

OSPF の概要

OSPF は、リンクステート アルゴリズムを使用して、すべての既知の宛先までの最短パスを構築および計算します。OSPF エリア内の各ルータには、ルータが使用可能なインターフェイスと到達可能なネイバーそれぞれのリストである同一のリンクステート データベースが置かれています。

RIP に比べると OSPF は次の点で有利です。

- OSPF のリンクステート データベースのアップデート送信は RIP ほど頻繁ではありません。また、古くなった情報のタイムアウトで徐々にアップデートされるのではなく、リンクステート データベースは瞬時にアップデートされます。
- ルーティング決定はコストに基づいて行われます。これは、特定のインターフェイスを介してパケットを送信するためにオーバーヘッドが必要であることを示しています。セキュリティ アプライアンスは、インターフェイスのコストをリンク帯域幅に基づいて計算し、宛先までのホップ数は使用しません。コストは優先パスを指定するために設定できます。

最短パス優先アルゴリズムの欠点は、CPU サイクルとメモリが大量に必要になることです。

セキュリティ アプライアンスは、OSPF プロトコルのプロセス 2 つを異なるインターフェイス セット上で同時に実行できます。同じ IP アドレスを使用する複数のインターフェイス（NAT ではこのようなインターフェイスは共存可能ですが、OSPF ではアドレスの重複は許しません）があるときに、2 つのプロセスを実行する場合があります。あるいは、一方のプロセスを内部で実行しながら別のプロセスを外部で実行し、ルートのサブセットをこの 2 つのプロセス間で再配布する場合もあります。同様に、プライベート アドレスをパブリック アドレスから分離する必要がある場合もあります。

OSPF ルーティング プロセスには、別の OSPF ルーティング プロセスや RIP ルーティング プロセスから、または OSPF 対応インターフェイスに設定されているスタティック ルートおよび接続されているルートから、ルートを再配布できます。

セキュリティ アプライアンスでは、次の OSPF の機能がサポートされています。

- エリア内ルート、エリア間ルート、および外部ルート（タイプ I とタイプ II）のサポート
- 仮想リンクのサポート
- OSPF の LSA フラッディング
- OSPF パケットの認証（パスワード認証と MD5 認証の両方）
- セキュリティ アプライアンスの指定ルータまたは指定バックアップ ルータとしての設定のサポート。セキュリティ アプライアンスは、ABR としてもセットアップできます。しかし、セキュリティ アプライアンスを ASBR として設定するための機能は、デフォルト情報に限定されています（デフォルト ルートの挿入など）。
- スタブ エリアと not so stubby エリア（NSSA）のサポート
- ABR タイプ 3 LSA フィルタリング
- スタティック アドレス変換およびグローバル アドレス変換のアドバタイズ

OSPF のイネーブル化

OSPF をイネーブルにするには、OSPF ルーティング プロセスを作成し、このルーティング プロセスに関連付ける IP アドレスの範囲を指定し、さらにその IP アドレスの範囲にエリア ID を割り当てる必要があります。

OSPF をイネーブルにするには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、OSPF ルーティング プロセスを作成します。

```
hostname(config)# router ospf process_id
```

このコマンドによって、この OSPF プロセスに対応するルータ コンフィギュレーション モードが開始されます。

process_id は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2　次のコマンドを入力して、OSPF を実行する IP アドレスを定義し、さらにそのインターフェイスのエリア ID を定義します。

```
hostname(config-router)# network ip_address mask area area_id
```

次に、OSPF をイネーブルに設定する例を示します。

```
hostname(config)# router ospf 2
hostname(config-router)# network 10.0.0.0 255.0.0.0 area 0
```

OSPF へのルートの再配布

セキュリティ アプライアンスは、OSPF ルーティング プロセス間のルート再配布を制御できます。セキュリティ アプライアンス は、**redistribute** コマンドの設定値に従って、またはルート マップを使用することによって、ルートを照合して変更します。ルート マップのその他の用途については、「デフォルト ルートの生成」（P.9-18）も参照してください。

スタティック ルート、接続されているルート、RIP ルート、または OSPF ルートを OSPF プロセスに再配布するには、次の手順を実行します。

ステップ 1　（任意）ルートマップを作成して、指定されたルーティング プロトコルのどのルートを OSPF ルーティング プロセスに再配布するのかを詳細に定義します。「ルート マップの定義」（P.9-8）を参照してください。

ステップ 2　次のコマンドを入力して、再分配先の OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

ステップ 3　次のコマンドを入力して、再分配するルートを指定します。

```
hostname(config-router)# redistribute {ospf process_id
[match {internal | external 1 | external 2}] | static | connected | rip}
[metric metric-value] [metric-type {type-1 | type-2}] [tag tag_value] [subnets] [route-map
map_name]
```

ospf *process_id*、**static**、**connected**、および **rip** キーワードでは、どの場所からルートを再分配するかを指定します。

このコマンドのオプションを使用して、ルート プロパティを照合したり設定したりできます。またはルート マップを使用することもできます。**tag** オプションおよび **subnets** オプションに相当するオプションは、**route-map** コマンドにはありません。ルート マップと **redistribute** コマンドのオプションを両方とも使用する場合は、両方を一致させる必要があります。

次に、メトリックが 1 のルートと照合することによって、OSPF プロセス 1 から OSPF プロセス 2 にルートを再分配する例を示します。セキュリティ アプライアンス は、メトリックが 5、メトリック タイプが Type 1、タグが 1 の外部 LSA として、これらのルートを再分配します。

```
hostname(config)# route-map 1-to-2 permit
hostname(config-route-map)# match metric 1
hostname(config-route-map)# set metric 5
hostname(config-route-map)# set metric-type type-1
hostname(config-route-map)# set tag 1
hostname(config-route-map)# router ospf 2
hostname(config-router)# redistribute ospf 1 route-map 1-to-2
```

次に、指定した OSPF プロセスのルートが OSPF プロセス 109 に再分配される例を示します。OSPF メトリックは 100 に再マッピングされます。

```
hostname(config)# router ospf 109
hostname(config-router)# redistribute ospf 108 metric 100 subnets
```

次に、リンク ステート コストが 5、メトリック タイプが外部に設定されたルート再分配の例を示します。この場合、内部メトリックよりプライオリティが下がります。

```
hostname(config)# router ospf 1
hostname(config-router)# redistribute ospf 2 metric 5 metric-type external
```

OSPF インターフェイスのパラメータの設定

インターフェイス固有の OSPF パラメータは、必要に応じて変更できます。これらのパラメータは、特に変更する必要はありませんが、一部のインターフェイス パラメータについては、接続先ネットワーク上のすべてのルータで一致している必要があります。該当するパラメータは、**ospf hello-interval**、**ospf dead-interval**、および **ospf authentication-key** です。これらのパラメータのいずれかを設定する場合は、ネットワーク上のすべてのルータのコンフィギュレーションに適合する値にするようにしてください。

OSPF インターフェイス パラメータを設定するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、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。

```
hostname(config)# interface interface_name
```

ステップ 2　次のコマンドを任意で入力します。

- インターフェイスの認証タイプを指定する場合は、次のコマンドを入力します。

  ```
  hostname(config-interface)# ospf authentication [message-digest | null]
  ```

- OSPF 簡易パスワード認証を使用中のネットワーク セグメントに存在する隣接 OSPF ルータで使用するパスワードを割り当てるには、次のコマンドを入力します。

  ```
  hostname(config-interface)# ospf authentication-key key
  ```

key には、最大 8 バイトの連続する文字列が指定できます。

このコマンドで作成するパスワードはキーとして使用され、このキーはセキュリティ アプライアンスのソフトウェアによるルーティング プロトコル パケットの発信時に OSPF ヘッダーに直接挿入されます。各ネットワークにはインターフェイスごとに個別のパスワードを割り当てることができます。OSPF 情報を交換するには、同じネットワーク上のすべての隣接ルータが同じパスワードを持っている必要があります。

- OSPF インターフェイス上でのパケット送信コストを明示的に指定する場合は、次のコマンドを入力します。

```
hostname(config-interface)# ospf cost cost
```

cost は、1 ～ 65535 の整数です。

- hello パケットの最後の受信から、デバイスで近接する OSPF ルータのダウンを宣言するまでの待機時間（秒）を設定する場合は、次のコマンドを入力します。

```
hostname(config-interface)# ospf dead-interval seconds
```

この値はネットワーク上のすべてのノードで同じにする必要があります。

- セキュリティ アプライアンス が OSPF インターフェイス上で送信する hello パケットの時間間隔を指定する場合は、次のコマンドを入力します。

```
hostname(config-interface)# ospf hello-interval seconds
```

この値は、ネットワーク上のすべてのノードで一致させる必要があります。

- OSPF MD5 認証をイネーブルにする場合は、次のコマンドを入力します。

```
hostname(config-interface)# ospf message-digest-key key_id md5 key
```

次の値を設定します。

  - *key_id*：範囲 1 ～ 255 の識別子
  - *key*：最大 16 バイトの英数字によるパスワード

通常は、インターフェイスあたり 1 つのキーを使用して、パケット送信時に認証情報を生成するとともに着信パケットを認証します。隣接ルータの同一キー識別子は、キー値を同一にする必要があります。

1 インターフェイスで 2 つ以上のキーを保持しないことをお勧めします。新しいキーを追加したらその都度古いキーを削除して、ローカル システムが古いキー情報を持つ悪意のあるシステムと通信を続けることのないようにしてください。古いキーを削除すると、ロールオーバー中のオーバーヘッドを減らすことにもなります。

- ネットワーク用の OSPF 指定ルータを決定するときに役立つプライオリティを設定する場合は、次のコマンドを入力します。

```
hostname(config-interface)# ospf priority number_value
```

number_value は、0 ～ 255 です。

- OSPF インターフェイスに属している隣接ノードへの LSA 再送信間隔（秒）を指定する場合は、次のコマンドを入力します。

```
hostname(config-interface)# ospf retransmit-interval seconds
```

seconds は、接続ネットワーク上の 2 つのルータ間で予期される往復遅延より大きくする必要があります。範囲は 1 ～ 65535 秒です。デフォルトは 5 秒です。

- OSPF インターフェイス上でリンク ステート アップデート パケットを送信するときに必要な推定秒数を設定する場合は、次のコマンドを入力します。

```
hostname(config-interface)# ospf transmit-delay seconds
```

seconds は 1 ～ 65,535 秒です。デフォルト値は 1 秒です。

次に、OSPF インターフェイスを設定する例を示します。

```
hostname(config)# router ospf 2
hostname(config-router)# network 2.0.0.0 255.0.0.0 area 0
hostname(config-router)# interface inside
hostname(config-interface)# ospf cost 20
hostname(config-interface)# ospf retransmit-interval 15
hostname(config-interface)# ospf transmit-delay 10
hostname(config-interface)# ospf priority 20
hostname(config-interface)# ospf hello-interval 10
hostname(config-interface)# ospf dead-interval 40
hostname(config-interface)# ospf authentication-key cisco
hostname(config-interface)# ospf message-digest-key 1 md5 cisco
hostname(config-interface)# ospf authentication message-digest
```

次に、**show ospf** コマンドの出力例を示します。

```
hostname(config)# show ospf

Routing Process "ospf 2" with ID 20.1.89.2 and Domain ID 0.0.0.2
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 5. Checksum Sum 0x 26da6
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm executed 2 times
        Area ranges are
        Number of LSA 5. Checksum Sum 0x 209a3
        Number of opaque link LSA 0. Checksum Sum 0x     0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

OSPF エリア パラメータの設定

複数のエリア パラメータを設定できます。これらのエリア パラメータ（次の作業手順を参照）には、認証の設定、スタブ エリアの定義、およびデフォルトの集約ルートへの特定コストの割り当てが含まれます。認証では、エリアへの不正アクセスに対してパスワードベースで保護します。

スタブ エリアに外部ルートに関する情報は送信されません 代わりに、自律システムの外部の宛先のスタブ エリア内には、ARB によって生成されるデフォルトの外部ルートがあります。OSPF スタブ エリアのサポートを活用するには、デフォルトのルーティングをスタブ エリアで使用する必要があります。スタブ エリアに送信される LSA 数を減らすには、ABR に **area stub** コマンドの **no-summary** キーワードを設定して、ABR からスタブ エリアへの集約リンク アドバタイズ（LSA タイプ 3）の送信を阻止できます。

ネットワークにエリア パラメータを指定するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、設定する OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

ステップ 2　次のコマンドを任意で入力します。

- OSPF エリアの認証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-router)# area area-id authentication
  ```

- OSPF エリアの MD5 認証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-router)# area area-id authentication message-digest
  ```

- エリアをスタブ エリアとして定義するには、次のコマンドを入力します。

  ```
  hostname(config-router)# area area-id stub [no-summary]
  ```

- スタブ エリアで使用するデフォルトの集約ルートに、特定のコストを割り当てるには、次のコマンドを入力します。

  ```
  hostname(config-router)# area area-id default-cost cost
  ```

  cost は、1 ～ 65535 の整数です。デフォルトは 1 です。

次に、OSPF エリア パラメータを設定する例を示します。

```
hostname(config)# router ospf 2
hostname(config-router)# area 0 authentication
hostname(config-router)# area 0 authentication message-digest
hostname(config-router)# area 17 stub
hostname(config-router)# area 17 default-cost 20
```

OSPF NSSA の設定

Not-So-Stubby Area（NSSA）の OSPF への実装は、OSPF のスタブ エリアに似ています。NSSA では、コアからエリアへのタイプ 5 外部 LSA のフラッディングは実行されませんが、限定された方法で、自律システムの外部ルートをエリア内にインポートできます。

NSSA では、再分配により、NSSA エリア内にタイプ 7 自律システム外部ルートをインポートします。これらのタイプ 7 LSA は、NSSA の ABR によってタイプ 5 LSA に変換され、ルーティング ドメイン全体へフラッディングされます。変換中は集約とフィルタリングがサポートされます。

OSPF を使用する中央サイトから異なるルーティング プロトコルを使用するリモート サイトに接続しなければならない ISP またはネットワーク管理者は、NSSA を使用することによって管理を簡略化できます。

NSSA が実装される前は、企業サイトの境界ルータとリモート ルータ間の接続では、OSPF スタブ エリアとしては実行されませんでした。これは、リモート サイト向けのルートは、スタブ エリアに再配布することができず、2 種類のルーティング プロトコルを維持する必要があったためです。RIP のようなシンプルなプロトコルを実行して再配布を処理する方法が一般的でした。NSSA が実装されたことで、企業ルータとリモート ルータ間のエリアを NSSA として定義することにより、NSSA で OSPF を拡張してリモート接続をカバーできます。

OSPF NSSA を設定するために必要なエリア パラメータをネットワークに指定するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、設定する OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

ステップ 2　次のコマンドを任意で入力します。

- NSSA エリアを定義するには、次のコマンドを入力します。

  ```
  hostname(config-router)# area area-id nssa [no-redistribution]
  [default-information-originate]
  ```

- アドレス グループを集約するには、次のコマンドを入力します。

  ```
  hostname(config-router)# summary address ip_address mask [not-advertise] [tag tag]
  ```

  このコマンドは、ルーティング テーブルの容量縮小に有効です。OSPF でこのコマンドを使用すると、このアドレスでカバーされる再配布ルートすべての集約として、1 つの外部ルートが OSPF ASBR からアドバタイズされます。

  OSPF は **summary-address 0.0.0.0 0.0.0.0** をサポートしません。

  次の例では、集約アドレス 10.1.0.0 にアドレス 10.1.1.0、10.1.2.0、10.1.3.0 などが含まれています。外部 LSA では、アドレス 10.1.0.0 だけがアドバタイズされます。

  ```
  hostname(config-router)# summary-address 10.1.1.0 255.255.0.0
  ```

  この機能を使用する前に、次のガイドラインを参考にしてください。

  - 外部の宛先に到達するためのタイプ 7 デフォルト ルートを設定できます。この設定により、ルータは NSSA または NSSA の ABR が使用するタイプ 7 デフォルト ルートを生成します。
  - 同じエリア内のすべてのルータは、そのエリアが NSSA であることに合意している必要があります。合意していないと、ルータ間の通信ができません。

OSPF エリア間のルート集約の設定

ルート集約は、アドバタイズされるアドレスを統合することです。この機能を実行すると、1 つのサマリー ルートがエリア境界ルータを通して他のエリアにアドバタイズされます。OSPF のエリア境界ルータは、ネットワークをある 1 つのエリアから別のエリアへとアドバタイズしていきます。あるエリアにおいて連続する複数のネットワーク番号が割り当てられている場合、指定された範囲に含まれるエリア内の個別のネットワークをすべてカバーするサマリー ルートをアドバタイズするようにエリア境界ルータを設定することができます。

ルート集約のアドレス範囲を定義するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、設定する OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

ステップ 2　次のコマンドを入力して、アドレス範囲を設定します。

```
hostname(config-router)# area area-id range ip-address mask [advertise | not-advertise]
```

次に、OSPF エリア間のルート集約を設定する例を示します。

```
hostname(config)# router ospf 1
hostname(config-router)# area 17 range 12.1.0.0 255.255.0.0
```

OSPF へのルート再配布時のルート集約の設定

他のプロトコルからのルートを OSPF に再配布する場合、各ルートは外部 LSA で個別にアドバタイズされます。その一方で、指定したネットワーク アドレスとマスクでカバーされる再配布ルートすべてに対して 1 つのルートをアドバタイズするようにセキュリティ アプライアンスを設定することができます。この設定によって OSPF リンクステート データベースのサイズが小さくなります。

ネットワーク アドレスとマスクでカバーされる再配布ルートすべてに対して 1 つのサマリー ルートをアドバタイズするようにソフトウェアを設定するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、設定する OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

ステップ 2　次のコマンドを入力して、集約アドレスを設定します。

```
hostname(config-router)# summary-address ip_address mask [not-advertise] [tag tag]
```

（注）　OSPF は **summary-address 0.0.0.0 0.0.0.0** をサポートしません。

次に、ルート集約を設定する例を示します。集約アドレス 10.1.0.0 にアドレス 10.1.1.0、10.1.2.0、10.1.3.0 などが含まれています。外部 LSA では、アドレス 10.1.0.0 だけがアドバタイズされます。

```
hostname(config)# router ospf 1
hostname(config-router)# summary-address 10.1.0.0 255.255.0.0
```

スタティック OSPF ネイバーの定義

ポイントツーポイントの非ブロードキャスト ネットワークを介して OSPF ルートをアドバタイズするには、スタティック OSPF ネイバーを定義する必要があります。これにより、OSPF アドバタイズメントを GRE トンネルにカプセル化しなくても、既存の VPN 接続でブロードキャストすることができます。

スタティック OSPF ネイバーを定義するには、次のタスクを実行します。

ステップ 1　OSPF ネイバーへのスタティック ルートを作成します。スタティック ルートを作成する方法の詳細については、「スタティック ルートおよびデフォルト ルートの設定」（P.9-2）を参照してください。

ステップ 2　次の作業を行って、OSPF ネイバーを定義します。

a. その OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します。次のコマンドを入力します。

```
hostname(config)# router ospf pid
```

b. 次のコマンドを入力して、OSPF ネイバーを定義します。

```
hostname(config-router)# neighbor addr [interface if_name]
```

addr 引数には OSPF ネイバーの IP アドレスを指定します。*if_name* は、ネイバーとの通信に使用するインターフェイスです。OSPF ネイバーが直接接続されているインターフェイスのいずれとも同じネットワーク上にない場合、**interface** を指定する必要があります。

デフォルト ルートの生成

自律システムの境界ルータによって、デフォルト ルートが OSPF ルーティング ドメインに必ず生成されるようにすることができます。ルートを OSPF ルーティング ドメインに再配布するように特に設定すると、ルータは自動的に自律システム境界ルータになります。しかし、自律システム境界ルータは、デフォルトでは OSPF ルーティング ドメインにデフォルト ルートを生成しません。

デフォルト ルートを生成する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、設定する OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

ステップ 2　自律システム境界ルータでデフォルト ルートが必ず生成されるようにするには、次のコマンドを入力します。

```
hostname(config-router)# default-information originate [always] [metric metric-value]
[metric-type {1 | 2}] [route-map map-name]
```

次に、デフォルト ルートを生成する例を示します。

```
hostname(config)# router ospf 2
hostname(config-router)# default-information originate always
```

ルート計算タイマーの設定

OSPF によるトポロジ変更受信と最短パス優先（SPF）計算開始との間の遅延時間が設定できます。最初に SPF を計算してから次に計算するまでの保持時間も設定できます。

ルート計算タイマーを設定するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、設定する OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

ステップ 2　次のコマンドを入力して、ルート計算時間を設定します。

```
hostname(config-router)# timers spf spf-delay spf-holdtime
```

spf-delay は、OSPF によるトポロジ変更受信と SPF 計算開始との間の遅延時間（秒）です。0 ～ 65535 の整数に設定できます。デフォルトの時間は 5 秒です。値の 0 は遅延がないことを意味します。つまり、SPF 計算はただちに開始されます。

spf-holdtime は、2 つの連続する SPF 計算の間の最短時間（秒）です。0 ～ 65535 の整数に設定できます。デフォルトの時間は 10 秒です。値の 0 は遅延がないことを意味します。つまり、2 回の SPF 計算がすぐに続けて行われます。

次に、ルート計算タイマーを設定する例を示します。

```
hostname(config)# router ospf 1
hostname(config-router)# timers spf 10 120
```

ネイバーがアップ状態またはダウン状態になった時点でのロギング

デフォルトでは、システムは OSPF ネイバーがアップ状態またはダウン状態になったときにシステムメッセージを送信します。

アップ状態またはダウン状態になった OSPF ネイバーについて、**debug ospf adjacency** コマンドを実行せずに確認する必要がある場合に、このコマンドを設定します。**log-adj-changes** router コンフィギュレーション コマンドでは、少ない出力によってピアの関係が高いレベルで表示されます。各ステート変更のメッセージを表示する場合には、**log-adj-changes detail** を設定します。

アップ状態またはダウン状態になったネイバーをログに記録するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、設定する OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

ステップ 2　次のコマンドを入力して、ネイバーのアップ / ダウンに関するロギングを設定します。

```
hostname(config-router)# log-adj-changes [detail]
```

（注）　ネイバーのアップまたはダウンのメッセージが送信されるには、ロギングがイネーブルになっている必要があります。

次に、ネイバーのアップ / ダウン メッセージをロギングする例を示します。

```
hostname(config)# router ospf 1
hostname(config-router)# log-adj-changes detail
```

OSPF アップデート パケット ペーシングの表示

OSPF アップデート パケットは、自動的にペーシングされるため、各パケットの送信間隔が 33 ミリ秒未満になることはありません。ペーシングを行わないと、リンクが低速の状態でアップデート パケットの一部が失われたり、ネイバーがアップデートを十分すばやく受信できなくなったり、あるいは、ルータがバッファ スペースを使い切ってしまったりすることがあります。たとえば、ペーシングを行わないと、次のいずれかのトポロジが存在する場合にパケットがドロップされる可能性があります。

- 高速ルータがポイントツーポイント リンクを介して低速のルータと接続している。
- フラッディング中に、複数のネイバーから 1 つのルータに同時にアップデートが送信される。

ペーシングは、再送信間でも、送信効率を高めて再送信パケットの損失を最小にするために利用されます。インターフェイスへの送信を待機している LSA を表示することもできます。ペーシングの利点は、OSPF アップデートおよび再送信パケットの送信の効率をよくすることです。

この機能を設定するタスクはありません。自動的に行われます。

指定したインターフェイス上でフラッディングされる待機中 LSA のリストを表示し、OSPF パケット ペーシングを確認するには、次のコマンドを入力します。

```
hostname# show ospf flood-list if_name
```

OSPF のモニタリング

IP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。提供された情報を使用して、リソース利用状況を判別したり、ネットワークの問題を解決したりできます。また、ノードの到達可能性情報を表示して、デバイス パケットがネットワークを通過するときにとるルーティング パスを見つけることもできます。

さまざまな OSPF ルーティング統計情報を表示するには、必要に応じて次のいずれかのタスクを実行します。

- OSPF ルーティング プロセスに関する一般情報を表示するには、次のコマンドを入力します。

  ```
  hostname# show ospf [process-id [area-id]]
  ```

- ABR および ASBR への内部 OSPF ルーティング テーブルのエントリを表示するには、次のコマンドを入力します。

  ```
  hostname# show ospf border-routers
  ```

- 特定のルータについて、OSPF データベース関連の情報リストを表示するには、次のコマンドを入力します。

  ```
  hostname# show ospf [process-id [area-id]] database
  ```

- （OSPF パケット ペーシングを確認するために）指定したインターフェイス上でフラッディングを待機中の LSA のリストを表示するには、次のコマンドを入力します。

  ```
  hostname# show ospf flood-list if-name
  ```

- OSPF 関連のインターフェイス情報を表示するには、次のコマンドを入力します。

  ```
  hostname# show ospf interface [if_name]
  ```

- OSPF ネイバー情報をインターフェイス単位で表示するには、次のコマンドを入力します。

  ```
  hostname# show ospf neighbor [interface-name] [neighbor-id] [detail]
  ```

- ルータが要求したすべての LSA のリストを表示するには、次のコマンドを入力します。

```
hostname# show ospf request-list neighbor if_name
```

- 再送信待ちになっているすべての LSA のリストを表示するには、次のコマンドを入力します。

```
hostname# show ospf retransmission-list neighbor if_name
```

- OSPF プロセスに基づいて設定したすべての集約アドレス再分配情報のリストを表示するには、次のコマンドを入力します。

```
hostname# show ospf [process-id] summary-address
```

- OSPF 関連の仮想リンク情報を表示するには、次のコマンドを入力します。

```
hostname# show ospf [process-id] virtual-links
```

OSPF プロセスの再起動

OSPF プロセスを再起動し、再分配またはカウンタを消去するには、次のコマンドを入力します。

```
hostname(config)# clear ospf pid {process | redistribution | counters
[neighbor [neighbor-interface] [neighbor-id]]}
```

RIP の設定

RIP をサポートしているデバイスは、ネットワークのトポロジが変更されると、ルーティングアップデート メッセージを所定の間隔で送信します。これらの RIP パケットには、デバイスが到達可能なネットワークに関する情報、さらに宛先アドレスに到達するためにパケットが通過しなければならないルータやゲートウェイの数が含まれています。RIP では、生成されるトラフィックは OSPF より多くなりますが、設定は OSPF より容易です。

RIP は、初期コンフィギュレーションが簡単で、トポロジが変更されても設定をアップデートする必要がないため、スタティック ルーティングより有利です。RIP の欠点は、ネットワーク数や処理オーバーヘッドがスタティック ルーティングより大きいことです。

セキュリティ アプライアンスは、RIP バージョン 1 および 2 をサポートしています。

ここでは、RIP 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。

- 「RIP のイネーブル化と設定」（P.9-21）
- 「RIP ルーティング プロセスへのルートの再配布」（P.9-23）
- 「インターフェイス上の RIP 送受信バージョンの設定」（P.9-23）
- 「RIP 認証のイネーブル化」（P.9-24）
- 「RIP のモニタリング」（P.9-25）

RIP のイネーブル化と設定

セキュリティ アプライアンス では、RIP ルーティング プロセスを 1 つだけイネーブルにできます。RIP ルーティング プロセスをイネーブルにした後に、**network** コマンドを使用して、そのルーティング プロセスに参加するインターフェイスを定義する必要があります。デフォルトでは、セキュリティ アプライアンス は RIP バージョン 1 アップデートを送信し、RIP バージョン 1 およびバージョン 2 アップデートを受け取ります。

RIP ルーティング プロセスをイネーブルにし設定するには、次の手順を実行します。

ステップ 1　グローバル コンフィギュレーション モードで次のコマンドを入力して、RIP ルーティング プロセスを開始します。

```
hostname(config): router rip
```

RIP ルーティング プロセスのルータ コンフィギュレーション モードに入ります。

ステップ 2　RIP ルーティング プロセスに参加するインターフェイスを指定します。RIP ルーティング プロセスに参加するインターフェイスごとに、次のコマンドを入力します。

```
hostname(config-router): network network_address
```

インターフェイスがこのコマンドで定義されるネットワークに属していれば、そのインターフェイスは RIP ルーティング プロセスに参加します。インターフェイスがこのコマンドで定義されるネットワークに属していなければ、そのインターフェイスは RIP アップデートを送受信しません。

ステップ 3　（任意）次のコマンドを入力して、セキュリティ アプライアンスで使用する RIP のバージョンを指定します。

```
hostname(config-router): version [1 | 2]
```

この設定はインターフェイスごとに上書きできます。

ステップ 4　（任意）デフォルト ルートを RIP に生成するには、次のコマンドを入力します。

```
hostname(config-router): default-information originate
```

ステップ 5　（任意）インターフェイスがパッシブ モードで動作するように指定するには、次のコマンドを入力します。

```
hostname(config-router): passive-interface [default | if_name]
```

default キーワードを使用すると、すべてのインターフェイスがパッシブ モードで動作するようになります。1 つのインターフェイス名を指定すると、そのインターフェイスだけがパッシブ RIP モードに設定されます。パッシブ モードでは、RIP ルーティング アップデートは、指定されたインターフェイスにより受信されますが、そこから送信されることはありません。パッシブ モードに設定するインターフェイスごとに、このコマンドを入力できます。

ステップ 6　（任意）次のコマンドを入力して、自動ルート集約をディセーブルにします。

```
hostname(config-router): no auto-summarize
```

RIP バージョン 1 では、常に自動ルート集約を使用するのでディセーブルにはできません。RIP バージョン 2 ではデフォルトでルート集約を使用するため、このコマンドを使用してディセーブルにできます。

ステップ 7　（任意）アップデートで受信されるネットワークをフィルタリングするには、次の手順を実行します。

a. 標準アクセス リストを作成し、ルーティング テーブルの中で RIP プロセスが許可しているネットワークを許可し、RIP プロセスが廃棄するネットワークを拒否するように設定します。

b. 次のコマンドを入力して、フィルタを適用します。インターフェイスを指定して、そのインターフェイスが受信するアップデートだけにフィルタを適用することができます。

```
hostname(config-router): distribute-list acl in [interface if_name]
```

このコマンドは、フィルタを適用するインターフェイスごとに入力できます。インターフェイス名を指定しない場合、フィルタは RIP アップデートに適用されます。

ステップ 8　（任意）アップデートで送信されるネットワークをフィルタリングするには、次の手順を実行します。

a. 標準アクセス リストを作成し、RIP プロセスがアドバタイズするネットワークを許可し、アドバタイズしないネットワークを拒否するように設定します。

b. 次のコマンドを入力して、フィルタを適用します。インターフェイスを指定して、そのインターフェイスが送信するアップデートだけにフィルタを適用できます。

```
hostname(config-router): distribute-list acl out [interface if_name]
```

このコマンドは、フィルタを適用するインターフェイスごとに入力できます。インターフェイス名を指定しない場合、フィルタは RIP アップデートに適用されます。

RIP ルーティング プロセスへのルートの再配布

OSPF ルーティング プロセス、スタティック ルーティング プロセス、および接続されているルーティング プロセスからルートを RIP ルーティング プロセスに再配布できます。

ルートを RIP ルーティング プロセスに再配布するには、次の手順を実行します。

ステップ 1　（任意）ルート マップを作成して、指定されたルーティング プロトコルのどのルートを RIP ルーティング プロセスに再分配するのかを詳細に定義します。ルート マップを作成する方法の詳細については、「ルート マップの定義」（P.9-8）を参照してください。

ステップ 2　選択したルート タイプを RIP ルーティング プロセスに再配布するには、次のいずれかのオプションを選択します。

- 接続されているルートを RIP ルーティング プロセスに再配布するには、次のコマンドを入力します。

  ```
  hostname(config-router): redistribute connected [metric {metric_value | transparent}]
  [route-map map_name]
  ```

- スタティック ルートを RIP ルーティング プロセスに再配布するには、次のコマンドを入力します。

  ```
  hostname(config-router): redistribute static [metric {metric_value | transparent}]
  [route-map map_name]
  ```

- ルートを OSPF ルーティング プロセスから RIP ルーティング プロセスに再配布するには、次のコマンドを入力します。

  ```
  hostname(config-router): redistribute ospf pid [match {internal | external [1 | 2] |
  nssa-external [1 | 2]}] [metric {metric_value | transparent}] [route-map map_name]
  ```

インターフェイス上の RIP 送受信バージョンの設定

セキュリティ アプライアンスが RIP アップデートの送受信に使用する RIP のグローバルに設定されたバージョンを、インターフェイスごとに上書きできます。

RIP 送受信の設定

ステップ 1　（任意）インターフェイスから送信される RIP アドバタイズメントのバージョンを指定するには、次の手順を実行します。

a. 次のコマンドを入力して、設定するインターフェイスのインターフェイス コンフィギュレーション モードに入ります。

```
hostname(config)# interface phy_if
```

b. 次のコマンドを入力して、RIP アップデートをインターフェイスから送信するときに使用する RIP のバージョンを指定します。

```
hostname(config-if)# rip send version {[1] [2]}
```

ステップ 2　（任意）インターフェイスによる受信が許可される RIP アドバタイズメントのバージョンを指定するには、次の手順を実行します。

a. 次のコマンドを入力して、設定するインターフェイスのインターフェイス コンフィギュレーション モードに入ります。

```
hostname(config)# interface phy_if
```

b. 次のコマンドを入力して、RIP アップデートをインターフェイスで受信するときに許可される RIP のバージョンを指定します。

```
hostname(config-if)# rip receive version {[1] [2]}
```

インターフェイスで受信された RIP アップデートは、許可されているバージョンと一致しなければドロップされます。

RIP 認証のイネーブル化

セキュリティ アプライアンス は、RIP バージョン 2 メッセージ用に RIP メッセージ認証をサポートしています。

RIP メッセージ認証をイネーブルにするには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、設定するインターフェイスのインターフェイス コンフィギュレーション モードに入ります。

```
hostname(config)# interface phy_if
```

ステップ 2　（任意）次のコマンドを入力して、認証モードを設定します。デフォルトでは、テキスト認証が使用されます。MD5 認証をお勧めします。

```
hostname(config-if)# rip authentication mode {text | md5}
```

ステップ 3　次のコマンドを入力して、認証をイネーブルにし、認証キーを設定します。

```
hostname(config-if)# rip authentication key key key_id key-id
```

RIP のモニタリング

さまざまな RIP ルーティング統計情報を表示するには、必要に応じて次のいずれかのタスクを実行します。

- RIP ルーティング データベースの内容を表示するには、次のコマンドを入力します。

  ```
  hostname# show rip database
  ```

- 実行コンフィギュレーション内の RIP コマンドを表示するには、次のコマンドを入力します。

  ```
  hostname# show running-config router rip
  ```

次の **debug** コマンドは、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り使用してください。デバッグ出力は CPU プロセスで高いプライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムのパフォーマンスに影響が生じる可能性が低くなります。

- RIP 処理イベントを表示するには、次のコマンドを入力します。

  ```
  hostname# debug rip events
  ```

- RIP データベース イベントを表示するには、次のコマンドを入力します。

  ```
  hostname# debug rip database
  ```

ルーティング テーブル

ここでは、次の内容について説明します。

ルーティング テーブルの表示

ルーティング テーブルのエントリを表示するには、次のコマンドを入力します。

```
hostname# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

S    10.1.1.0 255.255.255.0 [3/0] via 10.86.194.1, outside
C    10.86.194.0 255.255.254.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.86.194.1, outside
```

ASA 5505 適応型セキュリティ アプライアンスでは、次のルートも表示されます。これは、内部ループバック インターフェイスであり、VPN ハードウェア クライアント機能によって個々のユーザ認証に使用されます。

```
C 127.1.0.0 255.255.0.0 is directly connected, _internal_loopback
```

ルーティング テーブルへの入力方法

セキュリティ アプライアンスのルーティング テーブルには、スタティックに定義されたルート、直接接続されているルート、および RIP、OSPF の各ルーティング プロトコルで検出されたルートを入力できます。セキュリティ アプライアンスは、ルーティング テーブルに含まれるスタティック ルートと接続されているルートに加えて、複数のルーティング プロトコルを実行できるため、同じルートが複数の方法で検出または入力される可能性があります。同じ宛先への 2 つのルートがルーティング テーブルに追加されると、ルーティング テーブルに残るルートは次のように決定されます。

- 2 つのルートのネットワーク プレフィックス長（ネットワーク マスク）が異なる場合、どちらのルートも固有と見なされ、ルーティング テーブルに入力されます。入力された後は、パケット転送ロジックが 2 つのうちどちらを使用するかを決定します。

  たとえば、RIP プロセスと OSPF プロセスが次のルートを検出したとします。

  - RIP：192.168.32.0/24
  - OSPF：192.168.32.0/19

  OSPF ルートのアドミニストレーティブ ディスタンスの方が適切であるにもかかわらず、これらのルートのプレフィックス長（サブネット マスク）はそれぞれ異なるため、両方のルートがルーティング テーブルにインストールされます。これらは異なる宛先と見なされ、パケット転送ロジックが使用するルートを決定します。

- セキュリティ アプライアンスが、1 つのルーティング プロトコル（RIP など）から同じ宛先に複数のパスがあることを検知すると、（ルーティング プロトコルが判定した）メトリックがよい方のルートがルーティング テーブルに入力されます。

  メトリックは特定のルートに関連付けられた値で、ルートを最も優先されるものから順にランク付けします。メトリックスの判定に使用されるパラメータは、ルーティング プロトコルによって異なります。メトリックが最も小さいパスは最適パスとして選択され、ルーティング テーブルにインストールされます。同じ宛先への複数のパスのメトリックが等しい場合は、これらの等コストパスに対してロード バランシングが行われます。

- セキュリティ アプライアンスが、ある宛先へのルーティング プロトコルが複数あることを検知すると、ルートのアドミニストレーティブ ディスタンスが比較され、アドミニストレーティブ ディスタンスが最も小さいルートがルーティング テーブルに入力されます。

アドミニストレーティブ ディスタンスは、2 つの異なるルーティング プロトコルから同じ宛先に 2 つ以上の異なるルートがある場合に、セキュリティ アプライアンスが最適なパスの選択に使用するルート パラメータです。ルーティング プロトコルには、他のプロトコルとは異なるアルゴリズムに基づくメトリックがあるため、異なるルーティング プロトコルによって生成された、同じ宛先への 2 つのルートについて常に「最適パス」を判定できるわけではありません。

各ルーティング プロトコルには、アドミニストレーティブ ディスタンス値を使用して優先順位が付けられています。表 9-1 に、セキュリティ アプライアンスがサポートするルーティング プロトコルのデフォルトのアドミニストレーティブ ディスタンス値を示します。

表 9-1　サポートされるルーティング プロトコルのデフォルトのアドミニストレーティブ ディスタンス

ルートの送信元	デフォルトのアドミニストレーティブ ディスタンス
接続されているインターフェイス	0
スタティック ルート	1
OSPF	110
RIP	120

アドミニストレーティブ ディスタンス値が小さいほど、プロトコルの優先順位が高くなります。たとえば、OSPF ルーティング プロセス（デフォルト アドミニストレーティブ ディスタンス：110）と RIP ルーティング プロセス（デフォルト アドミニストレーティブ ディスタンス：100）の両方からセキュリティ アプライアンスが特定のネットワークへの 1 つのルートを受け取ると、OSPF の方がプリファレンスが高いため、セキュリティ アプライアンスは OSPF ルートを選択します。つまり、ルータは OSPF バージョンのルートをルーティング テーブルに追加します。

上の例では、OSPF 導出ルートの送信元が（電源遮断などで）失われると、セキュリティ アプライアンスは、OSPF 導出ルートが再度現れるまで、RIP 導出ルートを使用します。

アドミニストレーティブ ディスタンスはローカルの設定値です。たとえば、OSPF を通して取得したルートのアドミニストレーティブ ディスタンスを変更するために **distance-ospf** コマンドを使用する場合、その変更は、コマンドが入力されたセキュリティ アプライアンスのルーティング テーブルにだけ影響します。アドミニストレーティブ ディスタンスがルーティング アップデートでアドバタイズされることはありません。

アドミニストレーティブ ディスタンスは、ルーティング プロセスに影響を与えません。OSPF および RIP ルーティング プロセスは、ルーティング プロセスで検出されたか、ルーティング プロセスに再配布されたルートだけをアドバタイズします。たとえば、RIP ルーティング プロセスは、セキュリティ アプライアンスのルーティング テーブルで OSPF ルーティング プロセスによって検出されたルートが使用されていても、RIP ルートをアドバタイズします。

バックアップ ルート

ルートを最初にルーティング テーブルにインストールしようとしたとき、他のルートがインストールされてしまい、インストールできなかった場合に、そのルートはバックアップ ルートとして登録されます。ルーティング テーブルにインストールされたルートに障害が発生すると、ルーティング テーブル メンテナンス プロセスが、登録されたバックアップ ルートを持つ各ルーティング プロトコル プロセスを呼び出し、ルーティング テーブルにルートを再インストールするように要求します。障害が発生したルートに対して、登録されたバックアップ ルートを持つプロトコルが複数ある場合、アドミニストレーティブ ディスタンスに基づいて優先順位の高いルートが選択されます。

このプロセスのため、ダイナミック ルーティング プロトコルによって検出されたルートに障害が発生したときにルーティング テーブルにインストールされる「フローティング」スタティック ルートを作成できます。フローティング スタティック ルートとは、単に、セキュリティ アプライアンスで動作しているダイナミック ルーティング プロトコルよりも大きなアドミニストレーティブ ディスタンスが設定されているスタティック ルートです。ダイナミック ルーティング プロセスで検出された対応するルートに障害が発生すると、このスタティック ルートがルーティング テーブルにインストールされます。

転送の決定方法

転送は次のように決定されます。

- 宛先が、ルーティング テーブル内のエントリと一致しない場合、パケットはデフォルト ルートに指定されているインターフェイスを通して転送されます。デフォルト ルートが設定されていない場合、パケットは破棄されます。
- 宛先が、ルーティング テーブル内の 1 つのエントリと一致した場合、パケットはそのルートに関連付けられているインターフェイスを通して転送されます。
- 宛先が、ルーティング テーブル内の複数のエントリと一致し、そのエントリのネットワーク プレフィックス長がすべて同じ場合、その宛先へのパケットはそのルートに関連付けられているインターフェイスに配布されます。
- 宛先が、ルーティング テーブル内の複数のエントリと一致し、そのエントリのネットワーク プレフィックス長が異なる場合、パケットはネットワーク プレフィックス長がより長いルートに関連付けられているインターフェイスから転送されます。

たとえば、192.168.32.1 宛てのパケットが、ルーティング テーブルの次のルートを使用してセキュリティ アプライアンスのインターフェイスに到着したとします。

```
hostname# show route
        ....
        R   192.168.32.0/24 [120/4] via 10.1.1.2
        O   192.168.32.0/19 [110/229840] via 10.1.1.3
        ....
```

この場合、192.168.32.1 は 192.168.32.0/24 ネットワークに含まれるため、192.168.32.1 宛てのパケットは 10.1.1.2 宛てに送信されます。このアドレスはまた、ルーティング テーブルの他のルートにも含まれますが、ルーティング テーブル内では 192.168.32.0/24 の方が長いプレフィックスを持ちます（24 ビットと 19 ビット）。パケットを転送する場合、プレフィックスが長い方が常に短いものより優先されます。

ダイナミック ルーティングとフェールオーバー

ダイナミック ルートは、フェールオーバー コンフィギュレーションのスタンバイ装置またはフェールオーバー グループには複製されません。したがって、フェールオーバーの発生直後、セキュリティ アプライアンスが受信したパケットの一部は、設定されているダイナミック ルーティング プロトコルがルーティング テーブルに再入力される間、ルーティング情報がないためにドロップされるか、デフォルト スタティック ルートにルーティングされることがあります。