RIP の設定

この章では、Routing Information Protocol（RIP）を使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように ASA を設定する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。

RIP に関する情報

この項は、次の内容で構成されています。

RIP と呼ばれることが多い Routing Information Protocol は、すべてのルーティング プロトコルの中で最も堅牢なものの 1 つです。RIP には、ルーティング アップデート プロセス、RIP ルーティング メトリック、ルーティング安定性、ルーティング タイマーの 4 つの基本的なコンポーネントがあります。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、ホップ カウントをメトリックとして使用するディスタンスベクトル ルーティング プロトコルです。RIP がインターフェイス上でイネーブルの場合、そのインターフェイスは、ネイバー デバイスと RIP ブロードキャストを交換して、ルートの動的な学習およびアドバタイズを行います。

ASA は、RIP バージョン 1 と RIP バージョン 2 の両方をサポートしています。RIP バージョン 1 では、ルーティング アップデートでサブネット マスクは送信されません。RIP バージョン 2 では、ルーティング アップデートでサブネット マスクが送信され、可変長サブネット マスクがサポートされています。さらに、RIP バージョン 2 では、ルーティング アップデートを交換するときのネイバー認証がサポートされています。この認証により、信頼できるソースからの信頼性のあるルーティング情報が ASA で受信されることが保証されます。

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。

ルーティング アップデート プロセス

RIP は、ルーティングアップデート メッセージを定期的に、またネットワーク トポロジが変更されたときに送信します。ルータは、エントリの変更が含まれるルーティング アップデートを受け取ると、新しいルートを反映するようにそのルーティング テーブルを更新します。パスのメトリック値は 1 ずつ大きくなり、送信者はネクスト ホップとして示されます。RIP ルータは、宛先に対する最適なルート（メトリック値が最も小さいルート）だけを保持します。ルータは、そのルーティング テーブルを更新した後、他のネットワーク ルータに変更を通知するために、ルーティング アップデートの送信をただちに開始します。これらのアップデートは、RIP ルータが送信する定期的にスケジュールされたアップデートとは独立して送信されます。

RIP のルーティング メトリック

RIP は、1 つのルーティング メトリック（ホップ カウント）を使用して発信元と宛先ネットワークとの距離を測定します。発信元から宛先までのパスの各ホップにはホップ カウント値（通常は 1）が割り当てられます。ルータが、新しいまたは変更された宛先ネットワーク エントリが含まれるルーティング アップデートを受け取ると、アップデートで示されたメトリック値に 1 を加算し、そのネットワークをルーティング テーブルに入れます。送信者の IP アドレスがネクスト ホップとして使用されます。

RIP 安定性機能

RIP は、送信元から宛先へのパスで許可されるホップ数に制限を導入することにより、ルーティング ループが無限に続くことを防止しています。パス内のホップの最大数は 15 です。新しいまたは変更されたエントリが含まれるルーティング アップデートをルータが受信し、メトリック値に 1 を加えた結果、メトリックが無限（つまり 16）になる場合は、ネットワークの宛先は到達不能と見なされます。この安定性機能の欠点は、この機能によって RIP ネットワークの直径の最大値が 16 ホップ未満に制限されることです。

RIP には、その他にも、多くのルーティング プロトコルに共通の安定性機能がいくつか含まれます。ネットワーク トポロジは急激に変化する可能性がありますが、これらの機能は、安定性を提供するように設計されています。たとえば、RIP では、スプリット ホライズンとホールドダウン メカニズムを実装して、間違ったルーティング情報が伝搬されることを防止しています。

RIP タイマー

RIP では、多数のタイマーを使用してそのパフォーマンスを調整しています。これらのタイマーには、ルーティングアップデート タイマー、ルートタイムアウト タイマー、ルートフラッシュ タイマーがあります。ルーティングアップデート タイマーは、定期的なルーティング アップデートの間隔を測りま

す。通常は 30 秒に設定されており、タイマーがリセットされたときにはランダムな時間がわずかに追加されます。これは、すべてのルータがそのネイバーを同時にアップデートしようとした結果発生する輻輳を防ぐためです。ルーティング テーブルの各エントリには、ルートタイムアウト タイマーが関連付けられています。ルートタイムアウト タイマーが期限切れになると、ルートには無効のマークが付きますが、ルートフラッシュ タイマーが期限切れになるまではテーブル内に保持されます。

クラスタリングの使用

RIP でクラスタリングを使用する方法については、「ダイナミック ルーティングおよびクラスタリング」（P.24-10）を参照してください。

RIP のライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードでだけサポートされます。

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 モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 はサポートされません。

その他のガイドライン

次の情報は、RIP バージョン 2 だけに適用されます。

- ネイバー認証を使用する場合、認証キーとキー ID は、RIP バージョン 2 アップデートをそのインターフェイスに提供するすべてのネイバー デバイス上で同じにする必要があります。
- RIP バージョン 2 の場合、ASA は、マルチキャスト アドレス 224.0.0.9 を使用してデフォルト ルート アップデートを送受信します。パッシブ モードでは、そのアドレスでルート アップデートが受信されます。
- RIP バージョン 2 がインターフェイス上で設定されると、マルチキャスト アドレス 224.0.0.9 がそのインターフェイス上で登録されます。RIP バージョン 2 設定がインターフェイスから削除されると、そのマルチキャスト アドレスの登録は解除されます。

制限事項

RIP には、次の制限事項があります。

- RIP アップデートは、ASA のインターフェイス間を通過できません。
- RIP バージョン 1 では、可変長サブネット マスクがサポートされていません。
- RIP の最大ホップ カウントは 15 です。ホップ カウントが 15 を超えるルートは、到達不能と見なされます。
- RIP の収束は、他のルーティング プロトコルと比べて時間がかかります。
- ASA では、RIP プロセスを 1 つだけイネーブルにできます。

RIP の設定

この項では、ASA で RIP プロセスをイネーブルにし、再起動する方法について説明します。

RIP をイネーブルにした後に、ASA で RIP プロセスをカスタマイズする方法については、「RIP のカスタマイズ」（P.28-4）を参照してください。

（注）　指定されたルーティング プロトコルから、ターゲット ルーティング プロセスに再配布できるルートを定義することでルートを再配布する場合は、デフォルト ルートを最初に生成する必要があります。詳細については、「デフォルト スタティック ルートの設定」（P.25-4）を参照してください。その後、ルート マップを定義します。詳細については、「ルート マップの定義」（P.26-4）を参照してください。

RIP のイネーブル化

ASA 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、ASA 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するには、次のコマンドを入力します。

コマンド	目的
router rip **例：** `hostname(config)# router rip`	RIP ルーティング プロセスを開始し、ルータ コンフィギュレーション モードに入ります。 イネーブルにした RIP 設定全体を削除するには、**no router rip** コマンドを使用します。設定を削除すると、**router rip** コマンドを使用して RIP を再度設定する必要があります。

RIP のカスタマイズ

この項では、RIP を設定する方法について説明します。次の項目を取り上げます。

- 「RIP バージョンの設定」（P.28-5）
- 「RIP のインターフェイスの設定」（P.28-6）
- 「インターフェイス上の RIP 送受信バージョンの設定」（P.28-6）

RIP バージョンの設定

ASA で使用される RIP のバージョンを指定するには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**router rip** **例：** `hostname(config)# router rip`	RIP ルーティング プロセスを開始し、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	**network** *network_address* **例：** `hostname(config)# router rip` `hostname(config-router)# network 10.0.0.0`	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。 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	RIP ルーティングに参加するようにインターフェイスをカスタマイズするには、次のいずれかの番号を入力します。	
	version [1 | 2] **例：** `hostname(config-router):# version [1]`	ASA が使用する RIP のバージョンを指定します。 この設定はインターフェイスごとに上書きできます。 この例では、バージョン 1 が入力されます。

RIP のインターフェイスの設定

RIP ルーティングに参加させないインターフェイスがアドバタイズするネットワークに接続されている場合は、そのインターフェイスが接続されているネットワークが含まれるネットワークを（**network** コマンドを使用して）設定し、パッシブ インターフェイスを（**passive-interface** コマンドを使用して）設定して、そのインターフェイスによる RIP の使用を防止できます。さらに、ASA がアップデートのために使用する RIP のバージョンを指定することもできます。

RIP についてインターフェイスを設定するには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**router rip** **例：** `hostname(config)# router rip`	RIP ルーティング プロセスを開始し、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	**network** *network_address* **例：** `hostname(config)# router rip` `hostname(config-router)# network 10.0.0.0`	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。 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	**passive-interface** [**default** | *if_name*] **例：** `hostname(config-router)# passive-interface [default]`	パッシブ モードで動作するインターフェイスを指定します。 **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 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。

インターフェイス上の RIP 送受信バージョンの設定

ASA 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。

アップデートを送受信するための RIP バージョンを設定するには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**interface** *phy_if* **例：** `hostname(config)# interface phy_if`	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 モードを開始します。
ステップ 2	次のいずれかの手順を実行し、インターフェイスごとに RIP アップデートを送受信します。	
	rip send version {[**1**] [**2**]} **例：** `hostname(config-if)# rip send version 1`	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。 この例では、バージョン 1 が選択されます。
	rip receive version {[**1**] [**2**]} **例：** `hostname(config-if)# rip receive version 2`	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します。 この例では、バージョン 2 が選択されます。 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。

ルート集約の設定

（注） RIP バージョン 1 では、常に自動ルート集約を使用します。RIP バージョン 1 ではこの機能をディセーブルにできません。RIP バージョン 2 では、デフォルトで自動ルート集約を使用します。

RIP ルーティング プロセスは、ネットワーク番号の境界で集約を行います。このため、ネットワークが連続していない場合、ルーティングの問題を引き起こすことがあります。

たとえば、ネットワーク 192.168.1.0、192.168.2.0、192.168.3.0 が接続されているルータがあり、それらのネットワークがすべて RIP に参加しているとすると、RIP ルーティング プロセスはそれらのルートに対しサマリー アドレス 192.168.0.0 を作成します。さらにネットワーク 192.168.10.0 と 192.168.11.0 が接続されているルータがこのネットワークに追加され、それらのネットワークが RIP に参加すると、これらもまた 192.168.0.0 として集約されます。トラフィックが誤った場所にルーティングされる可能性をなくすために、競合するサマリー アドレスを作成しているルータでの自動ルート集約をディセーブルにする必要があります。

RIP バージョン 1 では常に自動ルート集約が使用され、RIP バージョン 2 ではデフォルトのときに常に自動ルート集約が使用されるため、ルート集約を設定する場合は、ルート集約をディセーブルにすることだけが必要です。

自動ルート集約をディセーブルにするには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**router rip** **例：** `hostname(config)# router rip`	RIP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 2	**no auto-summarize** **例：** `hostname(config-router):# no auto-summarize`	自動ルート集約をディセーブルにします。

RIP でのネットワークのフィルタリング

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。

（注） 開始する前に、標準 ACL 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 プロセスが破棄するネットワークを拒否するように設定する必要があります。

手順の詳細

	コマンド	目的
ステップ 1	**router rip** **例：** `hostname(config)# router rip`	RIP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 2	**distribute-list** *acl* **in** [**interface** *if_name*] **distribute-list** *acl* **out** [**connected** | **eigrp** | **interface** *if_name* | **ospf** | **rip** | **static**] **例：** `hostname(config-router)# distribute-list acl2 in [interface interface1]` `hostname(config-router)# distribute-list acl3 out [connected]`	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。フィルタを適用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。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、EIGRP 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。

（注）　この手順を開始する前に、ルート マップを作成し、指定されたルーティング プロトコルのうち RIP ルーティング プロセスに再配布されるルートを詳細に定義する必要があります。ルート マップの作成の詳細については、第 26 章「ルート マップの定義」を参照してください。

ルートを RIP ルーティング プロセスに再配布するには、次のいずれかのコマンドを入力します。

コマンド	目的
redistribute connected [**metric** *metric-value* | **transparent**] [**route-map** *route-map-name*] **例：** hostname(config-router): # redistribute connected [metric metric-value | transparent] [route-map route-map-name]	接続されているルートを RIP ルーティング プロセスに再配布します。 RIP ルータ コンフィギュレーション内に **default-metric** コマンドが含まれていない場合、**redistribute** コマンドに RIP メトリック値を指定する必要があります。
redistribute static [**metric** {*metric_value* | **transparent**}] [**route-map** *map_name*] **例：** hostname(config-router):# redistribute static [metric {metric_value | transparent}] [route-map map_name]	スタティック ルートを EIGRP ルーティング プロセスに再配布します。
redistribute ospf *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}] [**metric** {*metric_value* | **transparent**}] [**route-map** *map_name*] **例：** hostname(config-router):# redistribute ospf pid [match {internal | external [1 | 2] | nssa-external [1 | 2]}] [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 プロセスに再配布します。
redistribute eigrp *as-num* [**metric** {*metric_value* | **transparent**}] [**route-map** *map_name*] **例：** hostname(config-router):# redistribute eigrp as-num [metric {metric_value | transparent}] [route-map map_name]	ルートを EIGRP ルーティング プロセスから RIP ルーティング プロセスに再配布します。

RIP 認証のイネーブル化

（注）　ASA 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 ルート認証では、RIP ルーティング プロトコルからのルーティング アップデートの MD5 認証を提供します。MD5 キーを使用したダイジェストが各 RIP パケットに含まれており、承認されていない送信元からの不正なルーティング メッセージや虚偽のルーティング メッセージが取り込まれないように阻止します。

RIP ルート認証は、インターフェイスごとに設定します。RIP 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 RIP 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。

（注）　RIP ルート認証をイネーブルにするには、事前に RIP をイネーブルにする必要があります。

インターフェイスでの RIP 認証をイネーブルにするには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**router rip** *as-num* **例：** `hostname(config)# router rip 2`	RIP ルーティング プロセスを作成し、この RIP 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。 *as-num* 引数は、RIP ルーティング プロセスの自律システム番号です。
ステップ 2	**interface** *phy_if* **例：** `hostname(config)# interface phy_if`	RIP メッセージ認証を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。
ステップ 3	**rip authentication mode** {**text** | **md5**} **例：** `hostname(config-if)# rip authentication mode md5`	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 認証の使用をお勧めします。
ステップ 4	**rip authentication key** *key* **key-id** *key-id* **例：** `hostname(config-if)# rip authentication key cisco key-id 200`	MD5 アルゴリズムで使用する認証キーを設定します。 *key* 引数には、最大 16 文字を指定できます。 *key-id* 引数には、0 ～ 255 の数字を指定します。

RIP プロセスの再起動

RIP 設定全体を削除するには、次のコマンドを入力します。

コマンド	目的
clear rip *pid* {**process** | **redistribution** | **counters** [**neighbor** [*neighbor-interface*] [*neighbor-id*]]} **例：** `hostname(config)# clear rip`	イネーブルにした RIP 設定全体を削除します。設定を削除すると、**router rip** コマンドを使用して RIP を再度設定する必要があります。

RIP のモニタリング

debug コマンドは、特定の問題のトラブルシューティングや、Cisco TAC とのトラブルシューティング セッションだけで使用することをお勧めします。

デバッグ出力は CPU プロセスで高い優先度が割り当てられているため、デバッグ出力を行うと ASA 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パフォーマンスに影響が生じる可能性が低くなります。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。

さまざまな RIP ルーティング統計情報をモニタまたはデバッグするには、次のいずれかのコマンドを入力します。

コマンド	目的
RIP ルーティングのモニタリング	
show rip database	RIP ルーティング データベースの内容を表示します。
show running-config router rip	RIP コマンドを表示します。
`show route cluster`	クラスタリングに関する追加ルートの同期の詳細を表示します。
RIP のデバッグ	
debug rip events	RIP 処理イベントを表示します。
debug rip database	RIP データベース イベントを表示します。
`debug route cluster`	RIB テーブルの複製のトレース メッセージをイネーブルにして、RIB がクラスタリングのスレーブ装置に正しく同期されているかどうかを確認します。

RIP の設定例

次の例に、さまざまなオプションのプロセスを使用して RIP をイネーブルにし、設定する方法を示します。

```
hostname(config)# router rip 2
hostname(config-router)# default-information originate
hostname(config-router)# version [1]
hostname(config-router)# network 225.25.25.225
```

```
hostname(config-router)# passive-interface [default]
hostname(config-router)# redistribute connected [metric bandwidth delay reliability
loading mtu] [route-map map_name]
```

RIP の機能履歴

表 28-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 28-1　RIP の機能履歴

機能名	リリース	機能情報
RIP のサポート	7.0(1)	Routing Information Protocol（RIP）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。 **route rip** コマンドが導入されました。
クラスタリング	9.0(1)	RIP の場合、バルク同期、ルートの同期およびレイヤ 2 ロード バランシングは、クラスタリング環境でサポートされます。 **show route cluster**、**debug route cluster**、**show mfib cluster**、**debug mfib cluster** の各コマンドが導入または変更されました。