# IPsec VPN ハイアベイラビリティ拡張機能

IPsec VPN ハイ アベイラビリティ拡張機能：逆ルート注入（RRI）およびホットスタンバイ ルータ プロトコル（HSRP）と IPsec。これらの 2 つの機能を一緒に使用すると、VPN におけるネットワーク設計を簡素化できるほか、ゲートウェイ リストを定義する場合にリモート ピアの設定の複雑さを低減することができます。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイトペーパーを参照してください。



# IPsec VPN ハイ アベイラビリティ拡張機能に関する情報

## 逆ルート注入

逆ルート注入（RRI）は、冗長性やロードバランシングが求められるバーチャルプライベート ネットワーク（VPN）のネットワーク設計を簡素化します。RRI は、ダイナミック クリプト マップとスタティック クリプト マップのどちらを使用する場合でも適用できます。

RRI には次の利点があります。

- 複数の（冗長な）VPN ヘッドエンド デバイスがある環境で、IPsec トラフィックを特定の VPN ヘッドエンド デバイスにルーティングできます。
- 特に、リモート デバイスのルート フラッピングが多く発生する環境で IKE キープアライブを使用するとき、ヘッドエンド デバイス間のリモート セッションの予測可能なフェー

ルオーバー時間を保証します（ルート収束の効果は考慮されません。これは、使用されるルーティング プロトコルとネットワークの規模によって異なるためです）。

- ルートが動的にアップストリーム デバイスで学習されるので、アップストリーム デバイス上でスタティック ルートを管理する必要はありません。

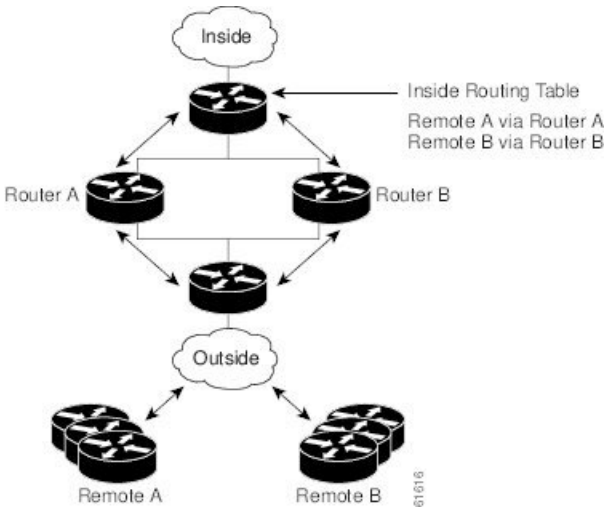
ダイナミック クリプト マップと連動する場合、リモート ピアが RRI 対応のルータとの IPsec セキュリティ アソシエーション（SA）を確立すると、スタティック ルートが、そのリモート ピアによって保護されたサブネットまたはホストごとに作成されます。スタティック クリプト マップの場合、スタティック ルートが拡張アクセス リスト ルールの各宛先に対して作成されます。アクセス コントロール リスト（ACL）を持つスタティック クリプト マップで RRI を使用すると、IPsec SA のネゴシエーションがなくても、ルートは常に存在します。

（注） RRI を使用する ACL では、any キーワードを使用できません。

作成されたルートは任意のダイナミック ルーティング プロトコルに注入され、周囲のデバイスに配布されます。このトラフィック フローでは、IPsec を正しい SA 全体に転送するために適切な RRI ルータに誘導し、IPsec ポリシーの不一致およびパケット喪失を回避する必要があります。

次の図は、RRI設定機能のトポロジを示します。リモートAにルータAがサービスを提供し、リモートBはルータBに接続します。このようにして、セントラル サイトにある VPN ゲートウェイ全体にロードバランシングを提供します。セントラルサイトのデバイスのRRIにより、ネットワーク内部の他のルータは、正しい転送判断を自動的に実行できるようになります。また、RRI により、内部ルータのスタティック ルートを管理する必要がなくなります。

**図 *1:* 逆ルート注入設定機能を示すトポロジ**



# ホットスタンバイ ルータ プロトコルおよび IPsec

ホットスタンバイ ルータ プロトコル（HSRP）は、1 つのルータのアベイラビリティに頼らなくても、イーサネットネットワークのホストから IP トラフィックをルーティングすることで、ネットワークのハイ アベイラビリティを実現します。HSRP は、ICMP Router Discovery Protocol（IRDP）などのルータ ディスカバリ プロトコルをサポートしないホスト、および選択したルータがリロードしたときまたはオフになったときに新しいルータに切り替える機能を備えていないホストには特に便利です。この機能がないと、ルータ障害が原因でデフォルト ゲートウェイを失うルータはネットワークと通信できません。

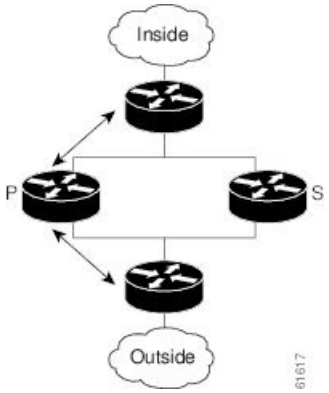
HSRP は、スタンバイ コマンドライン インターフェイス（CLI）コマンドを使用して LAN インターフェイス上に設定できます。インターフェイスから、ローカル IPsec ID またはローカル トンネル エンドポイントとしてスタンバイ IP アドレスを使用できます。

スタンバイ IP アドレスをトンネル エンドポイントとして使用すると、HSRP を使用してフェールオーバーを VPN ルータに適用できます。リモート VPN ゲートウェイは、HSRP グループ内のアクティブ デバイスに所属するスタンバイ アドレスを使用してローカル VPN ルータに接続します。フェールオーバーの際、スタンバイ デバイスはスタンバイ IP アドレスの所有権を引き継いで、リモート VPN ゲートウェイへのサービスを開始します。

フェールオーバーは、HSRP を使用して VPN ルータに適用できます。リモート VPN ゲートウェイは、HSRP グループ内のアクティブ デバイスに所属するスタンバイ アドレスを使用してローカル VPN ルータに接続します。この機能では、定義の必要があるのは HSRP スタンバイ アドレスだけなので、ゲートウェイ リストの定義に関してリモート ピア上での設定の複雑さが軽減されます。

次の図は、拡張 HSRP 機能のトポロジを示します。トラフィックは、スタンバイ グループのアクティブ装置である、アクティブ ルータ P でサービスが提供されています。フェールオーバーが発生した場合、トラフィックは、元のスタンバイ装置であるルータ S に迂回されます。ルータ S は新しいアクティブ ルータの役割を想定し、スタンバイ IP アドレスの所有権を引き継ぎます。

**図 *2:* ホットスタンバイ ルータ プロトコル機能を示すトポロジ**



（注） フェールオーバーの場合、HSRP は、VPN ルータ間の IPsec 状態情報の転送を促進しません。つまり、この状態の転送が行われない場合、リモートに対する SA が削除され、インターネット キー交換（IKE）および IPsec SA を再確立する必要があります。IPsec フェールオーバーをさらに効率的に行うために、IKE キープアライブをすべてのルータ上でイネーブルにすることを推奨します。

# IPsec VPN ハイ アベイラビリティ拡張機能の設定方法

## ダイナミック クリプト マップでの逆ルート注入の設定

標準スタティック クリプト マップ エントリのようなダイナミック クリプト マップ エントリは各セットにグループ化されます。セットは、すべて同じダイナミック マップ名を持つダイナミック クリプト マップ エントリのグループですが、ダイナミック シーケンス番号はそれぞれ異なります。セットの各メンバーは、RRI に設定できます。

ダイナミック クリプト マップ エントリを作成し、RRI をイネーブルにするには、この項の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **crypto dynamic-map** *map-name seq-num*
4. **set transform-set**
5. **reverse-route**

### 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**<br>例：<br>`Router> enable` | 特権 EXEC モードを有効にします。<br>• 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**<br>例：<br>`Router# 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。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | **crypto dynamic-map** *map-name seq-num*<br>例：<br>`Router(config)# crypto dynamic-map mymap` | ダイナミック クリプト マップ エントリを作成し、クリプト マップ コンフィギュレーション モードを開始します。 |
| ステップ 4 | **set transform-set**<br>例：<br>`Router(config-crypto-m)#set transform-set` | このクリプト マップ エントリで許可するトランスフォーム セットを指定します。複数のトランスフォームセットをプライオリティの順に表示します（最もプライオリティの高いものを先頭に表示）。<br>このエントリは、ダイナミック クリプト マップ エントリで必要とされる唯一の設定文です。 |
| ステップ 5 | **reverse-route**<br>例：<br>`Router(config-crypto-m)#reverse-route` | 送信元プロキシの情報を作成します。 |

# スタティック クリプト マップでの逆ルート注入の設定

スタティック クリプト マップに RRI を設定する前に、次の内容に注意してください。

- 逆ルートが mymap 2 でイネーブルになっていない場合、ルートはアクセス リスト 102 に基づいて作成されません。RRIは、デフォルトでイネーブルになっておらず、ルータ設定に表示されません。
- アップストリーム デバイスに VPN ルートを配布するには、ルーティング プロトコルをイネーブルにしてください。
- RRI 用に設定された VPN ルータ上でシスコ エクスプレス フォワーディング（CEF）が実行されている場合は、ネクスト ホップ デバイスを使用して、RRI 注入されたネットワークごとに隣接を設定する必要があります。これらのルートに対してネクストホップがルーティング テーブルで明示的に定義されていないので、プロキシ ARP をネクスト ホップ ルータ上でイネーブルにする必要があります（このルータによりそのデバイスのレイヤ 2 アドレスを使用して CEF 隣接関係を設定できます）。RRI 注入ルートが多い場合、RRI ルートが表す各サブネットからエントリがデバイスごとに作成されるので、隣接関係テーブルが非常に大きくなることがあります。

スタティック クリプト マップ セットに RRI を追加するには、この項の手順を実行します。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* **ipsec-isakmp**
4. **set peer** *ip-address*

5. **reverse-route**
6. **match address**
7. **set transform-set** *transform-set-name*

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**<br>例：<br>`Router> enable` | 特権 EXEC モードを有効にします。<br>• 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**<br>例：<br>`Router# 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 | **crypto map** *map-name seq-num* **ipsec-isakmp**<br>例：<br>`Router(config)#crypto map mymap 3 ipsec-isakmp` | ダイナミック クリプト マップ セットをスタティック クリプト マップ セットに追加し、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 4 | **set peer** *ip-address*<br>例：<br>`Router(config-if)#set peer 209.165.200.248` | クリプト マップ エントリに対して IPsec ピアの IP アドレスを指定します。 |
| ステップ 5 | **reverse-route**<br>例：<br>`Router (config-if)#reverse-route` | スタティック ルートをクリプト アクセス コントロール リスト（ACL）に基づいて動的に作成します。 |
| ステップ 6 | **match address**<br>例：<br>`Router(config-if)# match address` | クリプト マップ エントリの拡張アクセス リストを指定します。 |
| ステップ 7 | **set transform-set** *transform-set-name*<br>例：<br>`Router (config-if)# set transform-set my_t_set1` | このクリプト マップ エントリで許可するトランスフォーム セットを指定します。複数のトランスフォームセットをプライオリティ順（最高のプライオリティのものが最初）に列挙します。 |

# IPsec を使用した HSRP の設定

IPsec を使用して HSRP を設定する場合、次の条件を満たさなければならないことがあります。

- スタンバイ IP アドレスまたはスタンバイ名をインターフェイス上で変更した場合、HSRP をインターフェイス上のクリプト マップに適用するときに、クリプト マップを再度適用する必要があります。
- HSRP がインターフェイス上のクリプトマップに適用され、そのインターフェイスからスタンバイ IP アドレスまたはスタンバイ名を削除した場合、暗号トンネル エンドポイントは、そのインターフェイスの実際の IP アドレスに再初期化されます。
- IPsec フェールオーバーの要件があるインターフェイスにスタンバイ IP アドレスおよびスタンバイ名を追加する場合、適切な冗長情報を使用してクリプトマップを再度適用する必要があります。
- スタンバイ プライオリティは、アクティブ ルータとスタンバイ ルータ上で等しくなる必要があります。等しくない場合、プライオリティが高いルータがアクティブ ルータを引き継ぎます。以前アクティブだったルータが再度アップ状態になり、ただちにアクティブ ロールを引き継いたためスタンバイの報告がされず同期化しない場合、接続は廃棄されます。
- HSRP 追跡されるインターフェイスの、スタンバイ ルータおよびアクティブ ルータ上の IP アドレスは、他方のルータより低く、あるいは高くする必要があります。プライオリティが等しい（HA 要件）場合、HSRP はアクティブ状態に基づいた IP アドレスを割り当てます。ルータ A のパブリック IP アドレスはルータ B のパブリック IP アドレスよりも低いが、プライベートインターフェイスに関してはその逆になるようなアドレッシング方式が存在する場合、アクティブ/スタンバイとスタンバイ/アクティブのように分裂した状況が発生し、接続が切断される可能性があります。

（注） IPsec を使用せずに HSRP を設定するには、『*IP Application Services Configuration Guide*』の「Configuring IP Services」モジュールを参照してください。

インターフェイスにクリプト マップ セットを適用するには、この項の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *port*
4. **standby name** *group-name*
5. **standby ip** *ip-address*
6. **crypto map** *map-name* **redundancy** [*standby-name*]

### 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**<br>例： | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Router>enable` | |
| ステップ 2 | **configure terminal**<br>例：<br>`Router#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** *type slot / port*<br>例：<br>`Router(config)#interface GigabitEthernet 0/0` | インターフェイスを指定し、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 4 | **standby name** *group-name*<br>例：<br>`Router(config-if)#standby name mygroup` | スタンバイのグループ名を指定します。 |
| ステップ 5 | **standby ip** *ip-address*<br>例：<br>`Router(config-if)#standby ip 209.165.200.249` | スタンバイ グループの IP アドレスを指定します。<br>• グループ内のデバイスごとにこのコマンドが必要です。 |
| ステップ 6 | **crypto map** *map-name* **redundancy** [*standby-name*]<br>例：<br>`Router (config-if)#crypto map mymap redundancy` | IPsec のトンネル エンドポイントとして IP 冗長アドレスを指定します。 |

# VPN IPsec 暗号設定の確認

手順の概要

1. **enable**
2. **show crypto ipsec transform-set**
3. **show crypto map** [**interface** *interface* | **tag** *map-name*]
4. **show crypto ipsec sa** [**map** *map-name* | **address** | **identity**] [**detail**]
5. **show crypto dynamic-map** [**tag** *map-name*]

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**<br>例： | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Router> enable` | |
| ステップ 2 | **show crypto ipsec transform-set**<br>例：<br>`Router#show crypto ipsec transform-set` | トランスフォーム セットの設定を表示します。 |
| ステップ 3 | **show crypto map** [**interface** *interface* \| **tag** *map-name*]<br>例：<br>`Router#show crypto map tag mycryptomap` | クリプト マップ コンフィギュレーションを表示します。 |
| ステップ 4 | **show crypto ipsec sa** [**map** *map-name* \| **address** \| **identity**] [**detail**]<br>例：<br>`Router#show crypto ipsec sa address detail` | IPsec SA に関する情報を表示します。 |
| ステップ 5 | **show crypto dynamic-map** [**tag** *map-name*]<br>例：<br>`Router#show crypto dynamic-map tag mymap` | ダイナミック クリプト マップに関する情報を表示します。 |

# IPsec VPN ハイ アベイラビリティ拡張機能の設定例

## 例：ダイナミック クリプト マップでの逆ルート注入の設定

次の例では、ダイナミック クリプト マップ テンプレートの定義で **reverse-route** コマンドを使用することにより、接続しているリモート IPsec ピアによって保護されている、すべてのリモートプロキシ（サブネットまたはホスト）に対してルートが確実に作成されるようにします。

```
crypto dynamic mydynmap 1
 set transform-set my-transform-set
 reverse-route
```

このテンプレートは、「親」クリプトマップ文に関連付けられてから、インターフェイスに適用されます。

```
crypto map mymap 3 ipsec-isakmp dynamic mydynmap
 interface FastEthernet 0/0
 crypto map mymap
```

# 例：スタティック クリプト マップでの逆ルート注入の設定

RRI は、暗号化されたトラフィックを VPN ルータに転送し、他のトラフィックをすべて別のルータに転送する必要があるトポロジに適したソリューションです。このようなシナリオでは、RRI により、デバイスにスタティック ルートを手動で定義する必要はなくなります。

単一の VPN ルータが使用され、すべてのトラフィックがそのルータのネットワークのパスに出入りするときに VPN ルータを通過する場合、RRI は不要です。

リモート プロキシの VPN ルータに手動でスタティック ルートを定義し、これらのルートを永続的にルーティング テーブルにインストールする場合には、同じリモート プロキシをカバーするクリプト マップ インスタンスで RRI をイネーブルにしないでください。この場合、ユーザ定義のスタティック ルートが RRI によって削除されません。

ルーティング コンバージェンスの影響で、ルートのアドバタイズ（リンク状態と定期的な更新）に使用される、ルーティング プロトコルに基づくフェールオーバーの成否が左右されることがあります。ルーティング ステートの変更が検出された直後に、ルーティング アップデートが確実に送信されるようにして、コンバージェンス時間を短縮するには、OSPF などのリンク ステート ルーティング プロトコルを使用することを推奨します。

次の例では、RRI が mymap 2 に対してではなく、mymap 1 に対してイネーブルにされています。インターフェイスにクリプト マップが適用されると、ルートが次のようなアクセス リスト 101 に基づいて作成されます。

```
IP route 172.17.11.0 255.255.255.0 FastEthernet 0/0
crypto map mymap 1 ipsec-isakmp
 set peer 172.17.11.1
 reverse-route
 set transform-set my-transform-set
 match address 101
crypto map mymap 2 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set my-transform-set
 match address 102
access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.11.0 0.0.0.255
access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
interface FastEthernet 0/0
 crypto map mymap
```

# 例：IPsec を使用した HSRP の設定

次の例では、すべてのリモート VPN ゲートウェイを、192.168.0.3 を介してルータに接続する方法を示します。インターフェイス上のクリプトマップは、このスタンバイ アドレスを *mymap* のすべてのインスタンスのローカル トンネル エンドポイントとしてバインドすると同時に、group1 と呼ばれる同じスタンバイ グループに属しているアクティブ デバイスとスタンバイ デバイスの間で HSRP フェールオーバーが確実に行われるようにします。

RRI により、HSRP グループ内のアクティブ デバイスだけが、リモート プロキシへのネクストホップ VPN ゲートウェイとして、内部のデバイスにアドバタイズできることにも注意してください。フェールオーバーが発生すると、ルートは、以前アクティブだったデバイス上から削除され、新たにアクティブになったデバイス上に作成されます。

```
crypto map mymap 1 ipsec-isakmp
 set peer 10.1.1.1
 reverse-route
 set transform-set esp-aes-sha
 match address 102
Interface FastEthernet 0/0
 ip address 192.168.0.2 255.255.255.0
 standby name group1
 standby ip 192.168.0.3
 crypto map mymap redundancy group1
access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

スタンバイ名はスタンバイ グループ内のすべてのデバイスに設定する必要があり、スタンバイ アドレスはグループの少なくとも 1 つのメンバーに設定する必要があります。スタンバイ名がルータから削除されると、IPsec SA は削除されます。スタンバイ名が再度追加された場合、使用される名前が同じかどうかにかかわらず、（冗長オプションを使用して）クリプトマップをインターフェイスに再度適用する必要があります。

# その他の参考資料

### 関連資料

| 関連項目 | マニュアル タイトル |
|---|---|
| Cisco IOS コマンド | 『Cisco IOS Master Command List, All Releases』 |
| IPsec を使用しない HSRP の設定 | 『*IP Application Services Configuration Guide*』の「Configuring IP Services」モジュール |
| IP security（IPsec）用のステートフル フェールオーバーの設定 | 『*Security Configuration Guide: Secure Connectivity*』の「Stateful Failover for IPsec」モジュール |
| 推奨される暗号化アルゴリズム | 『Next Generation Encryption』 |

### MIB

| MIB | MIB のリンク |
|---|---|
| なし | 選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。<br>http://www.cisco.com/go/mibs |

### シスコのテクニカル サポート

| 説明 | リンク |
|---|---|
| 右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。 | http://www.cisco.com/cisco/web/support/index.html |

# IPsec VPN ハイ アベイラビリティ拡張機能の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

**表 *1 : IPsec VPN* ハイ アベイラビリティ拡張機能の機能情報**

| 機能名 | リリース | 機能情報 |
|---|---|---|
| IPsec VPN ハイ アベイラビリティ拡張機能 | Cisco IOS XE 3.1.0S | IPsec VPN ハイ アベイラビリティ拡張機能は次の 2 つの機能から構成されます。逆ルート注入（RRI）およびホット スタンバイ ルータ プロトコル（HSRP）と IPsec。これらの 2 つの機能を一緒に使用すると、VPN におけるネットワーク設計を簡素化できるほか、ゲートウェイ リストを定義する場合にリモート ピアの設定の複雑さを低減することができます。<br><br>次のコマンドが導入または変更されました。**crypto map**（インターフェイス IPsec）、**reverse-route**。 |

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。