



EIGRP MPLS VPN PE-CE Site of Origin の設定

- [EIGRP MPLS VPN PE-CE Site of Origin \(1 ページ\)](#)
- [EIGRP MPLS VPN PE-CE Site of Origin について \(2 ページ\)](#)
- [EIGRP MPLS VPN PE-CE Site of Origin サポートの設定方法 \(4 ページ\)](#)
- [EIGRP MPLS VPN PE-CE SoO の設定例 \(7 ページ\)](#)
- [EIGRP MPLS VPN PE-CE Site of Origin の機能履歴 \(9 ページ\)](#)

EIGRP MPLS VPN PE-CE Site of Origin

EIGRP MPLS VPN PE-CE Site of Origin 機能によって、マルチプロトコル ラベル スwitチング (MPLS) バーチャルプライベート ネットワーク (VPN) トラフィックを、Enhanced Interior Gateway Routing Protocol (EIGRP) ネットワークに対してサイト単位でフィルタリングする機能が追加されます。Site of Origin (SoO) フィルタリングは、インターフェイス レベルで設定され、これを使用して MPLS VPN トラフィックを管理し、複雑で複合的なネットワーク トポロジにおいて過渡的なルーティンググループが発生しないようにします。この機能は、プロバイダーエッジ (PE) とカスタマーエッジ (CE) 間の EIGRP に対する MPLS VPN Support 機能をサポートするために設計されています。EIGRP MPLS VPN をサポートしている PE ルータ上にインストールされている場合、この機能によってバックドアリンクに対するサポートが提供されます。

EIGRP MPLS VPN PE-CE Site of Origin の前提条件

このドキュメントでは、ネットワーク コア (またはサービス プロバイダー バックボーン) にボーダー ゲートウェイ プロトコル (BGP) が設定されていることを前提にしています。この機能を設定する前に、次のタスクも完了している必要があります。

- この機能は、PE と CE 間の EIGRP に対する MPLS VPN Support 機能をサポートするために導入されており、この機能は、EIGRP MPLS VPN の作成後に設定する必要があります。
- EIGRP MPLS VPN 対応に設定されているすべての PE ルータは、SoO の拡張コミュニティをサポートする Cisco IOS XE Gibraltar 16.11.1 以降のリリースを実行している必要があります。

EIGRP MPLS VPN PE-CE Site of Origin の制約事項

- VPN サイトがパーティション化されていて、バックドア ルータ インターフェイスで SoO 拡張コミュニティ属性が設定されている場合は、このバックドアリンクを、同じサイトの他のパーティションを起点とするプレフィックスへの代替パスとして使用することはできません。
- VPN サイトごとに、一意の SoO 値を設定する必要があります。同じ VPN サイトをサポートしているすべてのプロバイダー エッジ、およびカスタマー エッジ インターフェイスには (SoO が CE ルータ上に設定されている場合)、同じ値を設定する必要があります。
- `ip unnumbered` コマンドは MPLS 設定ではサポートされていません。

EIGRP MPLS VPN PE-CE Site of Origin について

ここでは、EIGRP MPLS VPN PE-CE Site of Origin について説明します。

EIGRP MPLS VPN PE-CE Site of Origin サポートの概要

EIGRP MPLS VPN PE-CE Site of Origin 機能によって、EIGRP から BGP へ、および BGP から EIGRP への再配布に対するサポートが追加されます。SoO 拡張コミュニティは BGP 拡張コミュニティ属性の1つで、これを使用して、あるサイトから生じたルートを特定し、そのプレフィックスが送信元サイトへ再アドバタイズメントされないようにします。SoO 拡張コミュニティは、PE ルータがルートを学習したサイトを一意に識別します。SoO サポートには、EIGRP サイト単位で MPLS VPN トラフィックをフィルタリングする機能があります。SoO のフィルタリングはインターフェイス レベルで設定されており、これを使用して MPLS VPN トラフィックを管理し、(VPN とバックドアリンクの両方が含まれている EIGRP VPN サイトなどの) 複雑で複合的なネットワーク ポロジにおいてルーティンググループが発生しないようにします。

SoO 拡張コミュニティの設定によって、サイト単位で MPLS VPN トラフィックをフィルタリングできます。SoO 拡張コミュニティは、PE ルータ上の着信 BGP ルートマップで設定され、インターフェイスに適用されます。SoO 拡張コミュニティは、より細かくフィルタリングするために、カスタマー サイトのすべての exit ポイントに適用することができますが、VPN サービスを提供する PE ルータから CE ルータへのすべてのインターフェイスに設定する必要があります。

バックドア リンクに対する Site of Origin のサポート

EIGRP MPLS VPN PE-CE Site of Origin (SoO) 機能によって、バックドア リンクに対するサポートが追加されます。バックドア リンクまたはルートは、リモートサイトとメインサイトの間の VPN の外部に設定される接続で、たとえば、リモートサイトを企業ネットワークへ接続する WAN 専用線などがあります。バックドア リンクは通常、VPN リンクが停止した、または使用できなくなった場合に EIGRP のサイト間でバックアップルートとして使用されます。

VPN リンクの障害がない場合はバックドア ルータを介したルートが選択されないように、メトリックはバックドア リンク上に設定されます。

SoO 拡張コミュニティは、バックドア ルータのインターフェイス上に定義されます。これはローカル サイト ID を特定するもので、同じサイトをサポートしている PE ルータで使用される値と一致している必要があります。バックドア ルータが、バックドア リンクを介してネイバーから EIGRP アップデート（またはリプライ）を受信すると、ルータは、SoO 値のアップデートを調べます。EIGRP アップデート内の SoO 値がローカルなバックドア インターフェイスの SoO 値と一致している場合、そのルートは拒否され、EIGRP トポロジテーブルには追加されません。このシナリオは通常、受信した EIGRP アップデート内で値が設定されたローカル SoO を備えたルートが他の VPN サイトで学習され、他の VPN サイト内のバックドア ルータによって、バックドア リンクを介してアドバタイズされたときに発生します。バックドア リンクにおける SoO フィルタリングでは、ローカル サイト ID を伝送するルートが含まれている EIGRP アップデートをフィルタリングすることによって、過渡的なルーティンググループが発生しないようにします。

PE ルータ、およびカスタマーサイトのバックドア ルータでこの機能が有効になっており、PE ルータとバックドア ルータの両方で SoO 値が定義されている場合は、PE ルータおよびバックドア ルータは VPN サイト間の統合をサポートします。カスタマーサイトの他のルータでは、ルートがネイバーへ転送されるため、ルートによって伝送される SoO 値を伝搬するだけですみます。これらのルータは、通常の拡散更新アルゴリズム（DUAL）計算以上は統合に影響を与えず、サポートもしません。

Site of Origin 拡張コミュニティとルータとの相互運用

SoO 拡張コミュニティを設定すると、EIGRP MPLS VPN PE-CE Site of Origin 機能をサポートしているルータが、各ルートの起点となるサイトを識別できます。この機能が有効になっていると、PE または CE ルータ上の EIGRP ルーティング プロセスは、受信したそれぞれのルートを SoO 拡張コミュニティに対してチェックし、次の条件に基づいてフィルタリングします。

- BGP または CE ルータから受信したルートには、受信側インターフェイス上の SoO 値と一致する SoO 値が含まれている場合：受信側インターフェイス上に設定されている SoO 値と一致する関連 SoO 値とともにルートを受信した場合、そのルートは別の PE ルータまたはバックドアリンクから学習したルートであるため、フィルタリングされます。この動作は、ルーティンググループを回避するために設計されています。
- CE ルータから受信したルートが一致しない SoO 値で設定されている場合：あるルートが、関連付けられている SoO 値とともに受信され、その値が、受信インターフェイス上で設定されている SoO 値と一致しない場合、そのルートは、BGP へ再配布されるように EIGRP トポロジテーブルに追加されます。ルートがすでに EIGRP トポロジテーブルにインストールされているが、別の SoO 値と関連付けられている場合は、そのルートが BGP へ再配布されるときに、トポロジテーブルの SoO 値が使用されます。
- CE ルータから受信したルートに SoO 値が含まれていない場合：受信したルートに SoO 値がない場合、そのルートは EIGRP トポロジテーブルに受け入れられます。ルートが BGP へ再配布される前に、ネクストホップ CE ルータに到達するために使用されるインターフェイスの SoO 値がそのルートに付加されます。

SoO 拡張コミュニティをサポートする BGP および EIGRP ピアがこれらのルートを受信する場合には、関連付けられている SoO 値も受信します。次に、これらの値を、SoO 拡張コミュニティをサポートしている他の BGP および EIGRP ピアへ渡します。このフィルタリングは、過渡的なルートが発信元サイトから再学習されないように、つまり過渡的なルーティンググループが発生しないようにする目的で設計されています。

Site of Origin を EIGRP に伝送する BGP VPN ルートの再配布

PE ルータ上の EIGRP ルーティングプロセスが、BGP VPN ルートを EIGRP トポロジテーブルへ再配布する場合、EIGRP は、付加された BGP 拡張コミュニティ属性から (SoO 値があれば) SoO 値を抽出し、EIGRP トポロジテーブルへ追加する前に、その SoO 値をルートへ付加します。アップデートを CE ルータへ送信する前に、EIGRP は各ルートについて SoO 値をテストします。インターフェイス上で設定されている SoO 値と一致する SoO 値に関連付けられているルートは、CE ルータに渡される前にフィルタリングされます。EIGRP ルーティングプロセスが、異なる SoO 値に関連付けられているルートを受信すると、その SoO 値は CE ルータに渡され、CE サイトを介して伝送されます。

EIGRP MPLS VPN PE-CE Site of Origin サポート機能の利点

EIGRP MPLS VPN PE-CE Site of Origin サポート機能の設定によって、サイト単位の VPN フィルタリングが導入されます。これにより、バックドアリンクを備えた MPLS VPN、複数の PE ルータに対してデュアルホーム接続になっている CE ルータ、同じ virtual routing and forwarding (VRF) インスタンス内のさまざまなサイトから CE ルータをサポートしている PE ルータなどの複雑なトポロジに対するサポートが改善されます。

EIGRP MPLS VPN PE-CE Site of Origin サポートの設定方法

ここでは、EIGRP MPLS VPN PE-CE Site of Origin サポートの設定方法について説明します。

Site of Origin 拡張コミュニティの設定

SoO 拡張コミュニティの設定によって、サイト単位で MPLS VPN トラフィックをフィルタリングできます。SoO 拡張コミュニティは、PE ルータ上の着信 BGP ルートマップで設定され、インターフェイスに適用されます。SoO 拡張コミュニティは、より細かくフィルタリングするために、カスタマーサイトのすべての exit ポイントに適用することができますが、VPN サービスを提供する PE ルータから CE ルータへのすべてのインターフェイスに設定する必要があります。

始める前に

- ネットワークコア (またはサービスプロバイダーバックボーン) にボーダーゲートウェイプロトコル (BGP) が設定されていることを確認する。
- この機能を設定する前に、EIGRP MPLS VPN を設定する。

- EIGRP MPLS VPN をサポートするよう設定されているすべての PE ルータは、SoO 拡張コミュニティをサポートしていること。
- 各 VPN サイトに対して一意の SoO 値を設定すること。各 VPN サイトでは、CE ルータに接続する PE ルータのインターフェイス上で同じ値を使用する必要があります。

手順

	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。 <ul style="list-style-type: none"> • 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	route-map map-name {permit deny} [sequence-number] 例： Device (config)# route-map Site-of-Origin permit 10	ルートマップコンフィギュレーションモードを開始して、ルートマップを作成します。 <ul style="list-style-type: none"> • この手順でルートマップが作成され、SoO 拡張コミュニティが適用されるようになります。
ステップ 4	set extcommunity sooextended-community-value 例： Device (config-route-map)# set extcommunity soo 100:1	BGP 拡張コミュニティ属性を設定します。 <ul style="list-style-type: none"> • soo キーワードには、Site of Origin 拡張コミュニティ属性を指定します。 • extended-community-value 引数には、設定する値を指定します。この値では、次のいずれかの形式を使用できます。 <ul style="list-style-type: none"> • 自律システム番号: ネットワーク番号 • IP アドレス: ネットワーク番号 自律システム番号とネットワーク番号、または IP アドレスとネットワーク

	コマンドまたはアクション	目的
		番号の区切りにはコロンを使用します。
ステップ 5	exit 例： Device(config-route-map)# exit	ルートマップコンフィギュレーションモードを終了し、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 6	interface type number 例： Device(config)# interface GigabitEthernet 1/0/1	特定のインターフェイスを設定するため、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 7	no switchport 例： Device(config-if)# no switchport	インターフェイスをレイヤ 2 ポートとして動作することを停止し、シスコルーテッド (レイヤ 3) ポートにします。
ステップ 8	vrf forwarding vrf-name 例： Device(config-if)# vrf forwarding VRF1	VRF をインターフェイスまたはサブインターフェイスに関連付けます。 <ul style="list-style-type: none">この手順で設定された VRF 名は、プロバイダーエッジとカスタマーエッジ間の EIGRP に対する MPLS VPN Support 機能を備えた EIGRP MPLS VPN に対して作成された VRF 名と一致している必要があります。
ステップ 9	ip vrf sitemap route-map-name 例： Device(config-if)# ip vrf sitemap Site-of-Origin	VRF をインターフェイスまたはサブインターフェイスに関連付けます。 <ul style="list-style-type: none">この手順で設定されたルートマップ名は、手順 3 で、SoO 拡張コミュニティを適用するために作成されたルートマップ名と一致している必要があります。
ステップ 10	ip address ip-address subnet-mask 例： Device(config-if)# ip address 10.0.0.1 255.255.255.255	インターフェイスの IP アドレスを設定します。 <ul style="list-style-type: none">IP アドレスは、VRF フォワーディングをイネーブルにした後で再設定する必要があります。

	コマンドまたはアクション	目的
ステップ 11	end 例 : Device (config-if) # end	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

次のタスク

- バックドアルトが含まれている、複合的な EIGRP MPLS VPN ネットワークトポロジの場合は、次に、バックドアルトに対して「準最適パス」コストコミュニティを設定します。

SoO 拡張コミュニティの設定の確認

手順

	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。 <ul style="list-style-type: none"> 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 bgp vpnv4 {all rd route-distinguisher vrf vrf-name} [ip-prefixlength] 例 : Device# ip bgp vpnv4 vrf SOO-1 20.2.1.1/32	VPN アドレス情報を BGP テーブルから表示します。 <ul style="list-style-type: none"> show ip bgp vpnv4 コマンドと all キーワードを使用して、指定したルートが、SoO 拡張コミュニティ属性で設定されていることを検証します。

EIGRP MPLS VPN PE-CE SoO の設定例

ここでは、EIGRP MPLS VPN PE-CE SoO の設定例を紹介します。

Site of Origin 拡張コミュニティの設定例

次に、グローバル コンフィギュレーション モードで開始し、インターフェイス上で SoO 拡張コミュニティを設定する例を示します。

```
route-map Site-of-Origin permit 10
set extcommunity soo 100:1
exit
```

```
GigabitEthernet1/0/1
vrf forwarding RED
ip vrf sitemap Site-of-Origin
ip address 10.0.0.1 255.255.255.255
end
```

Site of Origin 拡張コミュニティの確認の例

次の例では、BGP テーブルの VPN アドレス情報を表示し、SoO 拡張コミュニティの設定を確認します。

```
Device# show ip bgp vpnv4 all 10.0.0.1
  BGP routing table entry for 100:1:10.0.0.1/32, version 6
  Paths: (1 available, best #1, no table)
  Advertised to update-groups:
  1
 100 300
192.168.0.2 from 192.168.0.2 (172.16.13.13)
Origin incomplete, localpref 100, valid, external, best
Extended Community: SOO:100:1
```

カスタマー エッジ デバイス show コマンド

```
Device# show ip eigrp topo 20.2.1.1/32
EIGRP-IPv4 Topology Entry for AS(30)/ID(30.0.0.1) for 20.2.1.1/32
  State is Passive, Query origin flag is 1, 2 Successor(s), FD is 131072
  Descriptor Blocks:
 31.1.1.2 (GigabitEthernet1/0/13), from 31.1.1.2, Send flag is 0x0
  Composite metric is (131072/130816), route is External
  Vector metric:
    Minimum bandwidth is 1000000 Kbit
    Total delay is 5020 microseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
    Hop count is 2
    Originating router is 30.0.0.2
  Extended Community: SoO:100:1
  External data:
    AS number of route is 0
    External protocol is Connected, external metric is 0
    Administrator tag is 0 (0x00000000)
```

プロバイダー エッジ デバイス show コマンド

```
Device# show ip eigrp vrf SOO-1 topology 31.1.1.0/24
EIGRP-IPv4 VR(L3VPN) Topology Entry for AS(30)/ID(2.2.2.22)
  Topology(base) TID(0) VRF(SOO-1)
EIGRP-IPv4(30): Topology base(0) entry for 31.1.1.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 1310720
  Descriptor Blocks:
 1.1.1.1, from VPNv4 Sourced, Send flag is 0x0
  Composite metric is (1310720/0), route is Internal (VPNv4 Sourced)
  Vector metric:
    Minimum bandwidth is 1000000 Kbit
    Total delay is 10000000 picoseconds
    Reliability is 255/255
```



```

Load is 1/255
Minimum MTU is 1500
Hop count is 0
Originating router is 1.1.1.11
Extended Community: SoO:100:1

```

EIGRP MPLS VPN PE-CE Site of Origin の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.6.1	EIGRP MPLS VPN PE-CE Site of Origin	EIGRP MPLS VPN PE-CE Site of Origin 機能によって、マルチプロトコルラベルスイッチング (MPLS) バーチャルプライベート ネットワーク (VPN) トラフィックを、Enhanced Interior Gateway Routing Protocol (EIGRP) ネットワークに対してサイト単位でフィルタリングする機能が追加されます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。

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。