



IP マルチキャストの最適化：マルチキャスト向け SSM チャンネルベース フィルタリング

- 機能情報の確認 (1 ページ)
- マルチキャスト境界向け SSM チャンネルベース フィルタリングの前提条件 (2 ページ)
- マルチキャスト境界向け SSM チャンネルベース フィルタリング機能について (2 ページ)
- マルチキャスト境界向け SSM チャンネルベース フィルタリングの設定方法 (3 ページ)
- マルチキャスト境界向け SSM チャンネルベース フィルタリングの設定例 (4 ページ)
- その他の参考資料 (6 ページ)
- マルチキャスト境界向け SSM チャンネルベース フィルタリングの機能履歴と情報 (7 ページ)

機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの **Bug Search Tool** およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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** には、<http://www.cisco.com/go/cfn> からアクセスします。**Cisco.com** のアカウントは必要ありません。

マルチキャスト境界向け SSM チャンネル ベース フィルタリングの前提条件

IP マルチキャストをデバイスで有効にするには、『*IP Multicast: PIM Configuration Guide*』の「Configuring Basic IP Multicast」モジュールに記載されているタスクを使用します。

マルチキャスト境界向け SSM チャンネル ベース フィルタリング機能について

マルチキャスト境界のルール

マルチキャスト境界のための SSM チャンネルベースフィルタリング機能は、**ip multicast boundary** コマンドを拡張して、コントロールプレーンフィルタリングをサポートします。複数の **ip multicast boundary** コマンドをインターフェイスに適用できます。

次のルールで、**ipmulticastboundary** コマンドは制御されます。

- 1 つのインターフェイスに設定できるのは、**in** および **out** キーワードの一方のインスタンスです。
- **in** および **out** キーワードは、標準アクセス リストまたは拡張アクセス リストに使用できます。
- **filter-autorp** キーワードまたは **no** キーワードを使用する場合、標準のアクセス リストだけが許可されます。
- コマンドの最大 3 つのインスタンスが 1 つのインターフェイスで許可されます。**in** の 1 つのインスタンス、**out** の 1 つのインスタンス、および **filter-autorp** または **no** キーワードの 1 つのインスタンスです。
- コマンドの複数のインスタンスを使用すると、フィルタリングは累積的になります。キーワードなしの境界ステートメントが、**in** キーワードが含まれる境界ステートメントと存在する場合、両方のアクセス リストが **in** 方向に適用され、どちらか一方での一致で十分です。
- コマンドのすべてのインスタンスは、制御トラフィックおよびデータプレーントラフィックの両方に適用されます。
- 拡張アクセス リストのプロトコル情報は解析され、一貫性の再利用とフィルタリングが許可されます。アクセス リストがすべてのプロトコルの (S,G) トラフィックをフィルタリングする場合、(S,G) オペレーションは、キーワードについて記述されたすべての条件で拡張アクセス リストによってフィルタリングされます。

関連トピック

[マルチキャスト境界の設定 \(3 ページ\)](#)[トラフィックを許可および拒否するマルチキャスト境界の設定例 \(4 ページ\)](#)[トラフィックを許可するマルチキャスト境界の設定例 \(5 ページ\)](#)[トラフィックを拒否するマルチキャスト境界の設定例 \(5 ページ\)](#)

マルチキャスト境界向け SSM チャンネル ベース フィルタリングの利点

- この機能によって、送信元インターフェイスでの入力が可能になります。
- アクセス制御機能は、SSM および Any Source Multicast (ASM) の場合と同じです。

マルチキャスト境界向け SSM チャンネル ベース フィルタリングの設定方法

マルチキャスト境界の設定

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 モードをイネーブルにします。
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	ipaccess-list {standard extended} access-list-name 例： Device(config)# ip access-list 101	標準または拡張のアクセス リストを設定します。
ステップ 4	permit protocol host address host address 例： Device(config-ext-nacl)# permit ip host 181.1.2.201 host 232.1.1.11	指定された ip ホスト トラフィックを許可します。

	コマンドまたはアクション	目的
ステップ 5	deny protocol host address host address 例： Device(config-acl-nacl)# deny ip host 181.1.2.203 host 232.1.1.1	指定されたマルチキャスト ip グループ および送信元トラフィックを拒否しま す。
ステップ 6	必要に応じて、ステップ4またはステッ プ5を繰り返します。	指定されたホストおよび送信元トラ フィックを許可および拒否します。
ステップ 7	interface type interface-number port-number 例： Device(config)# interface gigabitethernet 2/3/0	インターフェイスコンフィギュレーショ ンモードをイネーブルにします。
ステップ 8	ipmulticastboundary access-list-name [in out filter-autorp] 例： Device(config-if)# ip multicast boundary acc_grpl out	マルチキャスト境界を設定します。 (注) filter-autorp キーワードは、拡 張アクセスリストをサポート していません。

関連トピック

[マルチキャスト境界のルール \(2 ページ\)](#)

[トラフィックを許可および拒否するマルチキャスト境界の設定例 \(4 ページ\)](#)

[トラフィックを許可するマルチキャスト境界の設定例 \(5 ページ\)](#)

[トラフィックを拒否するマルチキャスト境界の設定例 \(5 ページ\)](#)

マルチキャスト境界向け SSM チャンネル ベース フィルタリングの設定例

トラフィックを許可および拒否するマルチキャスト境界の設定例

次の例では、(181.1.2.201, 232.1.1.1) および (181.1.2.202, 232.1.1.1) への発信トラフィックを許可し、他のすべての (S,G) を拒否します。

```
configure terminal
ip access-list extended acc_grpl
permit ip host 0.0.0.0 232.1.1.1 0.0.0.255
permit ip host 181.1.2.201 host 232.1.1.1
permit udp host 181.1.2.202 host 232.1.1.1
permit ip host 181.1.2.202 host 232.1.1.1
```

```
deny igmp host 181.2.3.303 host 232.1.1.1
interface gigabitethernet 2/3/0
ip multicast boundary acc_grp1 out
```

関連トピック

[マルチキャスト境界の設定 \(3 ページ\)](#)

[マルチキャスト境界のルール \(2 ページ\)](#)

トラフィックを許可するマルチキャスト境界の設定例

次の例では、(192.168.2.201, 232.1.1.5) および (192.168.2.202, 232.1.1.5) への発信トラフィックを許可します。

```
configure terminal
ip access-list extended acc_grp6
permit ip host 0.0.0.0 232.1.1.1 5.0.0.255
deny udp host 192.168.2.201 host 232.1.1.5
permit ip host 192.168.2.201 host 232.1.1.5
deny pim host 192.168.2.201 host 232.1.1.5
permit ip host 192.168.2.202 host 232.1.1.5
deny igmp host 192.2.3.303 host 232.1.1.1
interface gigabitethernet 2/3/0
ip multicast boundary acc_grp6 out
```

関連トピック

[マルチキャスト境界の設定 \(3 ページ\)](#)

[マルチキャスト境界のルール \(2 ページ\)](#)

トラフィックを拒否するマルチキャスト境界の設定例

次に、候補 RP でアナウンスされるグループ範囲を拒否する例を示します。グループ範囲が拒否されるため、pim auto-rp マッピングは作成されません。

```
configure terminal
ip access-list standard acc_grp10
deny 225.0.0.0 0.255.255.255
permit any
access-list extended acc_grp12
permit pim host 181.1.2.201 host 232.1.1.8
deny udp host 181.1.2.201 host 232.1.1.8
permit pim host 181.1.2.203 0.0.0.255 host 227.7.7.7
permit ip host 0.0.0.0 host 227.7.7.7
permit ip 181.1.2.203 0.0.0.255 host 227.7.7.7
permit ip host 181.1.2.201 host 232.1.1.7
ip access-list extended acc_grp13
deny ip host 181.1.2.201 host 232.1.1.8
permit ip any any
interface gigabitethernet 2/3/0
ip multicast boundary acc_grp10 filter-autorp
ip multicast boundary acc_grp12 out
ip multicast boundary acc_grp13 in
```

関連トピック

[マルチキャスト境界の設定 \(3 ページ\)](#)

マルチキャスト境界のルール (2 ページ)

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 Commands List, All Releases』
Cisco IOS IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』

MIB

MIB	MIB のリンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存規格のサポートはありません。	選択したプラットフォーム、Cisco IOS XE Release、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には、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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

マルチキャスト境界向け SSM チャンネル ベース フィルタリングの機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

