管理プレーン保護の実装

Cisco IOS XR ソフトウェア の管理プレーン保護（MPP）機能では、ネットワーク管理パケットのデバイスへの着信を許可するインターフェイスを制限できます。 ネットワーク オペレータは MPP 機能を使用して、1 つ以上のルータ インターフェイスを管理インターフェイスとして指定できます。

デバイス管理トラフィックは、これらの管理インターフェイスを通じてのみ着信が許可されます。 MPP をイネーブルにすると、指定された管理インターフェイス以外のインターフェイスでは、そのデバイス宛のネットワーク管理トラフィックは許可されません。 指定されたインターフェイスに管理パケットを制限することで、デバイスの管理方法をより詳細に制御できるため、デバイスのセキュリティが向上します。

このモジュールでは、Cisco ASR 9000 Series Routers での管理プレーン保護の実装方法について説明します。

MPP コマンドの詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Security Command Reference*』の「*Management Plane Protection Commands on* Cisco ASR 9000 シリーズ ルータ」モジュールを参照してください。

管理プレーン保護の実装の機能履歴

リリース	変更点
リリース 3.7.2	この機能を追加しました。

管理プレーン保護の実装に関する前提条件

適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 このコマンド リファレンスには、各コマンドに必要なタスク ID が含まれます。ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。

管理プレーン保護の実装に関する制約事項

管理プレーン保護（MPP）の実装には次の制約事項があります。

- 現在、MPP は拒否またはドロップされたプロトコル要求を追跡していません。
- MPP 設定では、プロトコル サービスをイネーブルにはできません。 MPP はさまざまなインターフェイスでサービスを利用可能にする役割のみを果たします。プロトコルは明示的にイネーブル化されます。
- インバンドインターフェイスで受信する管理要求は、その場で必ずしも認知されるわけではありません。
- ルータ プロセッサ（RP）と分散ルート プロセッサ（DRP）のイーサネット インターフェイスは、デフォルトでアウトオブバンド インターフェイスとなり、MPP で設定できます。
- MPP設定に加えた変更は、その変更よりも前に確立されているアクティブなセッションには影響を与えません。
- 現在、MPP は、TFTP、Telnet、簡易ネットワーク管理プロトコル（SNMP）、セキュア シェル（SSH）、HTTP などのプロトコルに対して着信する管理要求のみを制御します。
- MIB はサポートされていません。

管理プレーン保護の実装について

管理プレーン保護機能をイネーブルにする前に、次の概念について理解しておく必要があります。

インバンド管理インターフェイス

インバンド管理インターフェイスは、データ転送パケットだけでなく管理パケットも処理する、Cisco IOS XR ソフトウェア の物理インターフェイスまたは論理インターフェイスです。 インバンド管理インターフェイスは、共有管理インターフェイスとも呼ばれています。

アウトオブバンド管理インターフェイス

アウトオブバンドは、管理プロトコル トラフィックの転送または処理だけを許可するインターフェイスを意味します。アウトオブバンド管理インターフェイスは、ネットワーク管理トラフィックだけを受信するようネットワーク オペレータによって定義されます。 これには、転送（またはカスタマー）トラフィックによってルータの管理が妨害されないという利点があります。これにより、サービス拒否攻撃を受ける可能性は大幅に低下します。

アウトオブバンドインターフェイスは、アウトオブバンドインターフェイス間のトラフィックのみを転送するか、ルータ宛の管理パケットを終端します。また、アウトオブバンドインターフェイスをダイナミック ルーティング プロトコルに加えることができます。 サービス プロバイダーはルータのアウトオブバンド インターフェイスに接続し、ルータが提供可能なすべてのルーティング ツールおよびポリシー ツールを使用して、独立したオーバーレイ管理ネットワークを構築します。

インターフェイス上のピア フィルタリング

ピア フィルタリング オプションでは、特定のピアまたはピア範囲からの管理トラフィックの設定を許可します。

コントロール プレーン保護の概要

コントロール プレーンは、ルート プロセッサ上でプロセス レベルで動作し、Cisco IOS XR ソフトウェアのほとんどの機能に対して高レベルの制御を一括提供するプロセスの集合です。直接または間接的にルータが宛先となるすべてのトラフィックは、コントロール プレーンによって処理されます。 管理プレーン保護はコントロール プレーン インフラストラクチャ内で動作します。

管理プレーン

管理プレーンは、ルーティング プラットフォームの管理に関連するすべてのトラフィックの論理パスです。 レイヤおよびプレーン内で構造化されている通信アーキテクチャの 3 つのプレーンのうちの 1 つである管理プレーンは、ネットワークの管理機能を実行し、すべてのプレーン（管理プレーン、コントロール プレーン、データ プレーン）の機能を調整します。 また、管理プレーンはネットワークとの接続を通じてデバイスの管理に使用されます。

管理プレーンで処理されるプロトコルには、簡易ネットワーク管理プロトコル（SNMP）、Telnet、HTTP、セキュア HTTP（HTTPS）、SSH などがあります。 これらの管理プロトコルは、モニタリングやコマンドライン インターフェイス（CLI）のアクセスに使用されます。 デバイスへのアクセスを内部ソース（信頼ネットワーク）に制限することが重要です。

管理プレーン保護機能

MPP 保護機能は、MPP 配下のすべての管理プロトコルと同様、デフォルトではディセーブルになっています。 インターフェイスをアウトオブバンドまたはインバンドとして設定すると、インターフェイスは自動的に MPP をイネーブルにします。 これにより、MPP 配下のすべてのプロトコルもイネーブルになります。

MPP がディセーブルでプロトコルがアクティブな場合、トラフィックはすべてのインターフェイスを通過できます。

アクティブなプロトコルが存在する状態でMPPがイネーブルになると、管理トラフィックを許可するデフォルトの管理インターフェイスはルート プロセッサ（RP）およびスタンバイ ルート プロセッサ（SRP）のイーサネットインターフェイスのみになります。 MPP をイネーブルにする他のすべてのインターフェイスについては、次に説明する MPP CLI を使用して、手動で管理インターフェイスとして設定する必要があります。 以後は、デフォルト管理インターフェイスと事前にMPPインターフェイスとして設定したインターフェイスのみがデバイス宛のネットワーク管理パケットを受け付けます。 他のすべてのインターフェイスは、デバイス宛のネットワーク管理パケットをドロップします。

（注） 論理インターフェイス（またはデータ プレーンに存在しない他のすべてのインターフェイス）は、入力物理インターフェイスに基づいてパケットをフィルタリングします。

設定後に、管理インターフェイスを変更または削除できます。

MPP機能がサポートしている管理プロトコルは、次のとおりです。 これらの管理プロトコルは、MPP がイネーブルになった際に影響を受ける唯一のプロトコルでもあります。

- SSH v1 と v2
- SNMP のすべてのバージョン
- Telnet
- TFTP
- HTTP
- HTTPS

管理プレーン保護機能のメリット

MPP 機能の実装には次の利点があります。

- デバイスの管理における、すべてのインターフェイスで管理プロトコルを許可するよりも優れたアクセス制御の実現。
- 管理インターフェイスでないインターフェイスでのデータ パケットのパフォーマンスの向上。

- ネットワークの拡張性のサポート。
- デバイスへの管理アクセスを制限する、インターフェイス別のアクセス コントロール リスト（ACL）を使用する作業のシンプル化。
- デバイスへのアクセス制限に必要な ACL 数の低減。
- スイッチングインターフェイスおよびルーティングインターフェイスのパケット フラッディングによる CPU への影響を防止。

管理プレーン保護のデバイスの設定方法

ここでは、次の作業について説明します。

インバンド インターフェイスの管理プレーン保護のデバイスの設定

ネットワークに追加した直後のデバイスや、ネットワークですでに動作しているデバイスを設定するには、この作業を実行します。 この作業では、特定のインターフェイスを通じてのみ Telnet のルータへのアクセスが許可されるインバンドインターフェイスとして、MPP を設定する方法について説明します。

デフォルトでない VRF でインバンド MPP インターフェイスを設定するには、次の作業を追加で実行します。

- デフォルトでないインバンド VRF のインターフェイスを設定します。
- グローバル インバンド VRF を設定します。
- Telnet の場合は、インバンド VRF に対して Telnet VRF サーバを設定します。

手順の概要

1. **configure**
2. control-plane
3. management-plane
4. inband
5. **interface** {*type instance* | **all**}
6. **allow** {*protocol* | **all**} [**peer**]
7. **address ipv4** {*peer-ip-address* | *peer ip-address/length*}
8. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**
9. **show mgmt-plane** [**inband** | **out-of-band**] [**interface** {*type instance*}]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	control-plane
	例：
	`RP/0/RSP0/CPU0:router(config)# control-plane`
	`RP/0/RSP0/CPU0:router(config-ctrl)#`
		コントロールプレーン 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	management-plane
	例：
	`RP/0/RSP0/CPU0:router(config-ctrl)# management-plane`
	`RP/0/RSP0/CPU0:router(config-mpp)#`
		管理プレーン保護を設定してプロトコルを許可および拒否し、管理プレーン保護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	inband
	例：
	`RP/0/RSP0/CPU0:router(config-mpp)# inband`
	`RP/0/RSP0/CPU0:router(config-mpp-inband)#`
		インバンドインターフェイスを設定し、管理プレーン保護インバンドコンフィギュレーション モードを開始します。

ステップ 5	**interface** {*type instance* | **all**}
	例：
	`RP/0/RSP0/CPU0:router(config-mpp-inband)# interface GigabitEthernet 0/6/0/1`
	`RP/0/RSP0/CPU0:router(config-mpp-inband-Gi0_6_0_1)#`
		特定のインバンドインターフェイスを設定するか、すべてのインバンド インターフェイスを設定します。管理プレーン保護インバンドインターフェイス コンフィギュレーション モードを開始するには、**interface** コマンドを使用します。
		• **all** キーワードを使用して、すべてのインターフェイスを設定します。

ステップ 6	**allow** {*protocol* | **all**} [**peer**]
	例：
	`RP/0/RSP0/CPU0:router(config-mpp-inband-Gi0_6_0_1)# allow Telnet peer`
	`RP/0/RSP0/CPU0:router(config-telnet-peer)#`
		指定されたプロトコルまたはすべてのプロトコルに対するインバンド インターフェイスとして、インターフェイスを設定します。
		• *protocol* 引数を使用して、指定管理インターフェイスで管理プロトコルを許可します。
		◦ HTTP または HTTPS
		◦ SNMP（バージョンも）

	コマンドまたはアクション	目的
		◦セキュア シェル（v1 および v2） ◦TFTP ◦Telnet • **all** キーワードを使用して、プロトコルのリストで指定されるすべての管理トラフィックを許可するようにインターフェイスを設定します。 •（任意）**peer** キーワードを使用して、インターフェイスでピア アドレスを設定します。
ステップ **7**	**address ipv4** {*peer-ip-address* | *peer ip-address/length*} 例： `RP/0/RSP0/CPU0:router(config-telnet-peer)# address ipv4 10.1.0.0/16`	このインターフェイス上で管理トラフィックが許可されるピア IPv4 アドレスを設定します。 • *peer-ip-address* 引数を使用して、このインターフェイス上で管理トラフィックが許可されるピア IPv4 アドレスを設定します。 • *peer ip-address/length* 引数を使用して、ピア IPv4 アドレスのプレフィックスを設定します。

ステップ **8**	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。

	コマンドまたはアクション	目的
		• 実行コンフィギュレーションファイルに設定変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。
ステップ 9	**show mgmt-plane** [**inband** | **out-of-band**] [**interface** {*type instance*}] 例： `RP/0/RSP0/CPU0:router# show mgmt-plane inband interface GigabitEthernet 0/6/0/1`	インターフェイスのタイプやインターフェイスでイネーブルにされるプロトコルなど、管理プレーンに関する情報を表示します。 • （任意）**inband** キーワードを使用して、管理パケットおよびデータ転送パケットを処理するインターフェイスであるインバンド管理インターフェイスの設定を表示します。 • （任意）**out-of-band** キーワードを使用して、アウトオブバンドインターフェイス設定を表示します。 • （任意）**interface** キーワードを使用して、特定のインターフェイスの詳細を表示します。

アウトオブバンドインターフェイスの管理プレーン保護のデバイスの設定

アウトオブバンド MPP インターフェイスを設定するには、次の作業を実行します。

- アウトオブバンド VRF のインターフェイスを設定します。
- グローバル アウトオブバンド VRF を設定します。
- Telnet の場合は、アウトオブバンド VRF に対して Telnet VRF サーバを設定します。

手順の概要

1. **configure**
2. control-plane
3. management-plane
4. out-of-band
5. **vrf** *vrf-name*
6. **interface** {*type instance* | **all**}
7. **allow** {*protocol* | **all**} [**peer**]
8. **address ipv6** {*peer-ip-address* | *peer ip-address/length*}
9. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**
10. **show mgmt-plane** [**inband** | **out-of-band**] [**interface** {*type instance*} | **vrf**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	control-plane
	例：
	`RP/0/RSP0/CPU0:router(config)# control-plane`
	`RP/0/RSP0/CPU0:router(config-ctrl)#`
		コントロール プレーン 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	management-plane
	例：
	`RP/0/RSP0/CPU0:router(config-ctrl)# management-plane`
	`RP/0/RSP0/CPU0:router(config-mpp)#`
		管理プレーン保護を設定してプロトコルを許可および拒否し、管理プレーン保護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	out-of-band 例： `RP/0/RSP0/CPU0:router(config-mpp)# out-of-band`	帯域外インターフェイスまたはプロトコルを設定し、管理プレーン保護帯域外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
	`RP/0/RSP0/CPU0:router(config-mpp-outband)#`	
ステップ 5	**vrf** *vrf-name* 例： `RP/0/RSP0/CPU0:router(config-mpp-outband)# vrf target`	帯域外インターフェイスのバーチャル プライベート ネットワーク（VPN）Routing and Forwarding（VRF; VPN ルーティングおよび転送）リファレンスを設定します。 • *vrf-name* 引数を使用して、VRF に名前を割り当てます。

ステップ 6	**interface** {*type instance* | **all**}
	
	例：
	
	`RP/0/RSP0/CPU0:router(config-mpp-outband)# interface GigabitEthernet 0/6/0/2`
	`RP/0/RSP0/CPU0:router(config-mpp-outband-Gi0_6_0_2)#`
		特定のアウトオブバンド インターフェイス、またはすべてのアウトオブバンド インターフェイスをアウトオブバンド インターフェイスとして設定します。管理プレーン保護アウトオブバンドコンフィギュレーション モードを開始するには、**interface** コマンドを使用します。
		• **all** キーワードを使用して、すべてのインターフェイスを設定します。

ステップ 7	**allow** {*protocol* | **all**} [**peer**]
	
	例：
	
	`RP/0/RSP0/CPU0:router(config-mpp-outband-Gi0_6_0_2)# allow TFTP peer`
	`RP/0/RSP0/CPU0:router(config-tftp-peer)#`
		指定されたプロトコルまたはすべてのプロトコルに対するアウトオブバンドインターフェイスとして、インターフェイスを設定します。
		• *protocol* 引数を使用して、指定管理インターフェイスで管理プロトコルを許可します。
		◦ HTTP または HTTPS
		◦ SNMP（バージョンも）
		◦ セキュア シェル（v1 および v2）
		◦ TFTP
		◦ Telnet
		• **all** キーワードを使用して、プロトコルのリストで指定されるすべての管理トラフィックを許可するようにインターフェイスを設定します。
		• （任意）**peer** キーワードを使用して、インターフェイスでピア アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 8	**address ipv6** {*peer-ip-address* | *peer ip-address/length*} 例： `RP/0/RSP0/CPU0:router(config-tftp-peer)# address ipv6 33::33`	このインターフェイス上で管理トラフィックが許可されるピア IPv6 アドレスを設定します。 • *peer-ip-address* 引数を使用して、このインターフェイス上で管理トラフィックが許可されるピア IPv6 アドレスを設定します。 • *peer ip-address/length* 引数を使用して、ピア IPv6アドレスのプレフィックスを設定します。

ステップ 9	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーションセッションが終了して、ルータがEXECモードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		
		• 実行コンフィギュレーション ファイルに設定変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ステップ 10	**show mgmt-plane** [**inband** | **out-of-band**] [**interface** {*type instance*} | **vrf**] 例： `RP/0/RSP0/CPU0:router# show mgmt-plane out-of-band interface GigabitEthernet 0/6/0/2`	インターフェイスのタイプやインターフェイスでイネーブルにされるプロトコルなど、管理プレーンに関する情報を表示します。 • （任意）**inband** キーワードを使用して、管理パケットおよびデータ転送パケットを処理するインターフェイスであるインバンド管理インターフェイスの設定を表示します。

	コマンドまたはアクション	目的
		• （任意）**out-of-band** キーワードを使用して、アウトオブバンド インターフェイス設定を表示します。 • （任意）**interface** キーワードを使用して、特定のインターフェイスの詳細を表示します。 • （任意）**vrf** キーワードを使用して、アウトオブバンド インターフェイスのバーチャル プライベート ネットワーク（VPN）ルーティングおよび転送リファレンスを表示します。

管理プレーン保護の実装の設定例

この項では、次の設定例について説明します。

管理プレーン保護の設定：例

次に、MPP 配下の特定の IP アドレスにインバンドおよびアウトオブバンド インターフェイスを設定する例を示します。

```
configure
 control-plane
  management-plane
   inband
    interface all
     allow SSH
     !
    interface GigabitEthernet 0/6/0/0
     allow all
     allow SSH
     allow Telnet peer
      address ipv4 10.1.0.0/16
     !
    !
    interface GigabitEthernet 0/6/0/1
     allow Telnet peer
      address ipv4 10.1.0.0/16
     !
    !
   !
   out-of-band
    vrf my_out_of_band
    interface GigabitEthernet 0/6/0/2
     allow TFTP peer
      address ipv6 33::33
     !
    !
   !
```

```
  !
 !

show mgmt-plane

Management Plane Protection

inband interfaces
----------------------

interface - GigabitEthernet0_6_0_0
        ssh configured -
                All peers allowed
        telnet configured -
                peer v4 allowed - 10.1.0.0/16
        all configured -
                All peers allowed
interface - GigabitEthernet0_6_0_1
        telnet configured -
                peer v4 allowed - 10.1.0.0/16

interface - all
        all configured -
                All peers allowed

outband interfaces
----------------------
interface - POS0_6_0_2
        tftp configured -
                peer v6 allowed - 33::33

show mgmt-plane out-of-band vrf

Management Plane Protection -
        out-of-band VRF - my_out_of_band
```

参考資料

ここでは、管理プレーン保護の実装に関する関連資料について説明します。

関連資料

関連項目	ドキュメント名
MPP コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco ASR 9000 Series Aggregation Services Router System Monitoring Command Reference*』の管理プレーン保護コマンド

標準

標準	タイトル
この機能でサポートが追加または変更された標準はありません。また、この機能で変更された既存の標準のサポートはありません。	—

MIB

MIB	MIB リンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検出およびダウンロードするには、URL（http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml）にある Cisco MIB Locator を使用して、[Cisco Access Products] メニューでプラットフォームを選択します。

RFC

RFC	タイトル
この機能でサポートが追加または変更された RFC はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカルサポート Web サイトには、数千ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。 Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html