合法的傍受の実装

合法的傍受は司法命令や行政命令によって認可され、司法当局が回線通信およびパケットモード通信に対して電子機器を用いた情報収集を実施するプロセスです。 世界中のサービス プロバイダーは、司法当局の回線交換およびパケットモード ネットワークにおける電子機器を用いた情報収集の実施をサポートすることが法的に求められます。

認可されたサービス プロバイダーの担当者のみが、法的に認可された傍受命令を処理および設定することを許可されています。 ネットワーク管理者および技術者は、法的に認可された傍受命令、または進行中の傍受に関する知識を得ることを禁止されています。 ルータにインストールされている傍受に関するエラー メッセージまたはプログラム メッセージは、コンソールには表示されません。

合法的傍受の実装の機能履歴

リリース	変更点
リリース 4.1.0	この機能を追加しました。
リリース 4.2.0	合法的傍受のハイ アベイラビリティ サポートが追加されました。 IPv6 の合法的傍受のサポートが追加されました。

• 参考資料，16 ページ

合法的傍受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。

合法的傍受の実装には、次の前提条件も満たす必要があります。

- Cisco ASR 9000 シリーズ アグリゲーション サービス ルータは、合法的傍受の運用においてコンテンツの傍受アクセス ポイント（IAP）ルータとして使用されます。
- **プロビジョニングされたルータ**：ルータはプロビジョニング済みである必要があります。詳細については、『*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*』を参照してください。

ヒント 合法的傍受のタップには、ループバック インターフェイスをプロビジョニングすると、他のインターフェイス タイプに比べて利点があります。

- **Cisco IOS XR ソフトウェアの SNMP Server コマンドの理解**：合法的傍受を実現する基盤となる簡易ネットワーク管理プロトコル バージョン 3（SNMP v3）は、『*Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference*』の「*SNMP Server Commands*」モジュールに説明されているコマンドを使用して設定されます。 合法的傍受を実装するには、SNMP サーバの機能を理解する必要があります。 このため、『*Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide*』の「*Implementing SNMP*」モジュールに説明されている情報をよく確認してください。
- **合法的傍受が明示的にディセーブルになっていること**：プロビジョニングされたルータでは、合法的傍受は自動的にイネーブルになっています。ただし、進行中のアクティブなタップがある場合、タップは削除されるため、LI をディセーブルにしないでください。
- **管理プレーンで SNMPv3 がイネーブルに設定されていること**：コマンドがルータのインターフェイス（できればループバック）に送信されるよう、管理プレーンが SNMP コマンドを受け付けられるようにします。 これにより、メディエーション デバイス（MD）が物理インターフェイスと通信できるようになります。
- **VACM ビューが SNMP サーバ向けにイネーブルになっていること**：ビューベース アクセス制御モデル（VACM）ビューは、ルータでイネーブルになっている必要があります。
- **プロビジョニングされた MD**：詳細については、ご使用の MD に関するベンダーのマニュアルを参照してください。 シスコが推奨する MD 機器サプライヤのリストについては、http://www.cisco.com/en/US/tech/tk583/tk799/tsd_technology_support_protocol_home.html を参照してください。
- **VoIP 監視固有の要件**

- **合法的傍受がイネーブルになっているコール エージェント**：合法的傍受がイネーブルになっているコール エージェントでは、監視ターゲットが MD にシグナリング情報を提供できるように、MD との通信用インターフェイスをサポートしている必要があります。 MD は、監視ターゲットのセッション記述プロトコル（SDP）のシグナリング情報から、送信元 IP アドレス、宛先 IP アドレス、Real-Time Protocol（RTP）のポート番号を抽出します。 これらの情報を使用して SNMPv3 SET を作成します。SNMPv3 SET はコンテンツ IAP として動作しているルータに送信され、監視ターゲットの傍受を実現します。

  MD は CISCO-TAP2-MIB を使用して、コンテンツ IAP として動作しているルータと MD との間の通信をセットアップします。

  MD は CISCO-IP-TAP-MIB を使用して、SDP から傍受および取得する IP アドレスとポート番号のフィルタをセットアップします。

- ターゲット番号によるコールで使用されるルータは、この目的のために MD を通じてプロビジョニングされる必要があります。

- 傍受するターゲット番号がプロビジョニングされている MD。

• データ セッション監視固有の要件

- データ ターゲットによって使用される、この目的のために MD を通じてプロビジョニングされているルータ。

- **ユーザ ログイン ID、ユーザの CPE デバイスの MAC アドレス、または DSLAM の物理位置 ID がプロビジョニングされている MD**：IP アドレスは、ネットワーク内のターゲットの特定に非常に頻繁に使用されるバインディングになります。 ただし、一部のネットワーク アーキテクチャでは、ネットワーク内のターゲットを独自に特定する別の情報形式が使用されている場合があります。 このような情報形式には、MAC アドレスと acct-session-id が含まれています。

• MD はネットワーク内の任意の場所に配置できますが、ターゲットの傍受に使用されているコンテンツ IAP ルータから到達可能である必要があります。 MD はグローバル ルーティング テーブルからのみ到達可能で、VRF ルーティング テーブルからは到達不可である必要があります。

合法的傍受の実装に関する制約事項

合法的傍受は、Cisco ASR 9000 Series Router では次の機能をサポートしていません。

• IPv6 マルチキャスト タッピング

• IPv4 マルチキャスト タッピング

• タップ別ドロップ カウンタ

• ギガビット イーサネット LC における IPv6 の傍受

• IPv6 MD カプセル化

- インターフェイス別タッピング
- 1 つのタップの複数 MD への複製
- タグ パケットのタッピング
- L2 フローのタッピング
- RTP のカプセル化
- 複製デバイスの暗号化および整合性チェック

（注） タップ別ドロップ カウンタのサポートは、ASR9000-SIP-700 ラインカードのみで利用できます。イーサネット ラインカードでは利用できません。

合法的傍受の実装について

シスコの合法的傍受は、サービス非依存傍受（SII）アーキテクチャと、SNMPv3 プロビジョニング アーキテクチャに基づいています。 SNMPv3 は、データの送信元を認証し、ルータから MD への接続がセキュアであることを保証する要件に対応します。 これにより、認可されていないパーティが傍受のターゲットを偽造できないようにします。

合法的傍受は、次の機能を提供します。

- SNMPv3 を使用した、MD からの Voice-over IP（VoIP）およびデータ セッション傍受のプロビジョニング
- 傍受された VoIP およびデータ セッション データの MD への配信
- SNMPv3 合法的傍受プロビジョニング インターフェイス
- 合法的傍受 MIB：CISCO-TAP2-MIB バージョン 2
- CISCO-IP-TAP-MIB は、IP 用のシスコの傍受機能を管理し、CISCO-TAP2-MIB とともに IP トラフィックの傍受に使用されます。
- ユーザ データグラム プロトコル（UDP）の MD へのカプセル化
- 傍受されたパケットの MD への複製および転送
- 受信パケットに設定された任意の規則に基づいた Voice-over IP（VoIP）コール傍受。
- LI がイネーブルになっているコール エージェントによる Voice-over IP（VoIP）の傍受
- IP アドレスに基づいたデータ セッションのコール傍受

VoIP コールのプロビジョニング

VoIP の合法的傍受のプロビジョニングは、次の方法で行われます。

- ユーザが SNMPv3 を通じて定義しているセキュリティと認証が実行されます。
- MD は SNMPv3 を使用して、合法的傍受情報のプロビジョニングを行います。
- ネットワーク管理は標準 MIB を通じて行われます。

コールの傍受

VoIP コールは、次の方法で傍受されます。

- MD はコンフィギュレーション コマンドを使用して、コール制御エンティティに傍受を設定します。
- コール制御エンティティは、ターゲットの傍受に関する情報を MD に送信します。
- MD は SNMPv3 を通じて、コンテンツ IAP ルータまたはトランク ゲートウェイにコール内容の傍受要求を開始します。
- コンテンツ IAP ルータまたはトランク ゲートウェイはコール内容を傍受し複製して、Packet Cable Electronic Surveillance UDP 形式で MD に送信します。 特に、IP ヘッダーの最初のバイトから始まる元のパケットには、TAP2-MIB において MD から提供される 4 バイトの CCCID がパケットの前に付与されます。 次に、このパケットは宛先アドレスおよびMDのポートとともに UDP フレームに入れられます。
- 複製された VoIP パケットが MD に送信されると、MD は一般的な規格でコピーを司法当局が所有する収集機能に転送します。

データ セッションのプロビジョニング

データ セッション用のプロビジョニングは、VoIP コールの合法的傍受の際と同様の方法で行われます。 （VoIP コールのプロビジョニング, （4 ページ）を参照してください）。

データの傍受

データは、次の方法で傍受されます。

- 合法的傍受がイネーブルになっている認証サーバまたはアカウンティング サーバが利用できない場合は、ネットワーク内でターゲットの存在を検出するためにスニファ デバイスを使用できます。
  - MD はコンフィギュレーション コマンドを使用して、スニファに傍受を設定します。
  - スニファ デバイスは、ターゲットの傍受に関する情報を MD に送信します。
- MD は SNMPv3 を使用して、コンテンツ IAP ルータに通信内容の傍受要求を開始します。
- コンテンツ IAP ルータは通信内容を傍受し複製して、UDP 形式で MD に送信します。

- 傍受されたデータ セッションは、サポートされている合法的傍受の提供規格を使用して、MD から司法当局の収集機能へ送信されます。

MD について

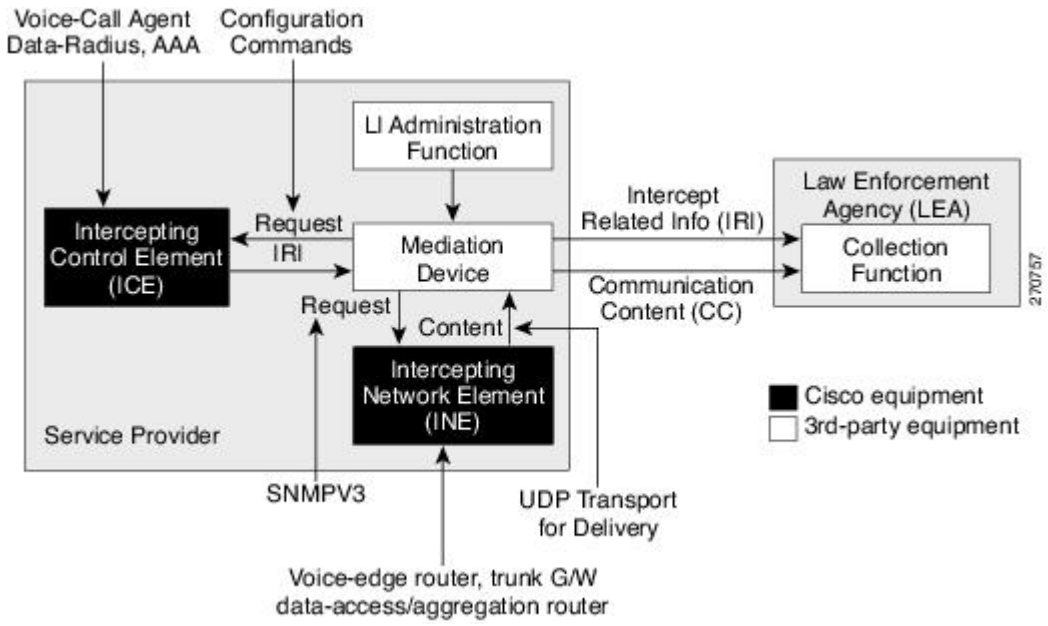
MD は次の作業を実行します。

- 認可された時間に傍受をアクティブにし、認可された期間が経過したときには傍受を削除する。
- 以下を確認するために、定期的にネットワーク内の要素を監査する。
  - 認可された傍受のみが存在していること。
  - 認可された傍受がすべて存在していること。

合法的傍受トポロジ

次の図は、音声傍受およびデータ傍受の合法的傍受トポロジにおける、傍受アクセス ポイントおよびインターフェイスを示しています。

図 *1*：音声傍受およびデータ傍受の合法的傍受トポロジ



スケールまたはパフォーマンスの改善

合法的傍受の拡張性およびパフォーマンスに関して、Cisco ASR 9000 Series Router に新たに導入された拡張機能は次のとおりです。

- IPv4の合法的傍受タップの上限は IPv4 ごとに 1000 タップ。
- IPv6の合法的傍受タップの上限は IPv6 ごとに 1000 タップ。
- 傍受レートは次のとおり。
  - ASR9000-SIP-700 ラインカードの場合、ネットワーク プロセッサ（NP）ごとに 50 Mbps。
  - ギガビット イーサネット ラインカードの場合、100 Mbps。
  - モジュラ Weapon-X ラインカードの場合、500 Mbps。
  - 100GE ラインカードの場合、1000 Mbps。
- 最大 512 個の MD をサポート。

IPv6 パケットの傍受

ここでは、Cisco ASR 9000 Series Router でサポートされている IPv6 パケットの傍受の詳細について説明します。

合法的傍受フィルタ

タップの分類に使用されるフィルタは次のとおりです。

- IP アドレス タイプ
- 宛先アドレス
- 宛先マスク
- 送信元アドレス
- 送信元マスク
- ToS（タイプ オブ サービス）および ToS マスク
- プロトコル
- 範囲指定の宛先ポート
- 範囲指定の送信元ポート
- VRF（VPN ルーティングおよび転送）
- フロー ID

フロー ID に基づいた IPv6 パケットの傍受

IPv6 パケットのフィルタ条件をさらに拡張するために、フロー ID に基づく IPv6 パケット傍受のサポートが Cisco ASR 9000 Series Router に追加されました。 すべての IPv6 パケットは、次の「IPv6

ヘッダーフィールドの詳細」表で定義されている数値フィールドを構成するIPv6ヘッダーのフィールドに基づいて傍受されます。

（注） フィールド長またはペイロード長はパケットの傍受には使用されません。

表 *1*：*IPv6* ヘッダー フィールドの詳細

IPv6 フィールド名	フィールドの説明	フィールド長
バージョン	IPv6 バージョン番号。	4 ビット
トラフィック クラス	インターネット トラフィックにおける配信の優先度を示す値。	8 ビット
フロー ID（フロー ラベル）	一連のパケットに対して、送信元から宛先までの特別なルータ処理を指定するために使用されます。	20 ビット
ペイロード長	パケット内のデータ長を指定します。ゼロにクリアすると、オプションはホップバイホップのジャンボペイロードになります。	16 ビット（未割り当て）
次ヘッダー	次のカプセル化されたプロトコルを指定します。値は、IPv4 プロトコル フィールドで指定されている値と互換性があります。	8 ビット
ホップ リミット	各ルータがパケットを転送するたびに、ホップ リミットは1ずつ減少します。ホップリミットフィールドがゼロに達すると、パケットは廃棄されます。このフィールドは、本来時間ベースのホップリミットとして使用されることを目的としていたIPv4ヘッダーの TTL フィールドに代わるものです。	8 ビット（符号なし）
送信元アドレス	送信ノードの IPv6 アドレス。	16 バイト
宛先アドレス	宛先ノードの IPv6 アドレス。	16 バイト

フロー ID またはフロー ラベルは、トラフィック フローの区別に使用される、IPv6 パケット ヘッダー内の 20 ビットのフィールドです。 各フローには、一意のフロー ID が含まれています。 特定のフロー ID に一致するパケットを傍受するフィルタ条件は、タップ設定ファイルに定義されます。 傍受されたマップ済みのフロー ID は、ラインカードから MD 設定ファイル内で指定されている次のホップに送信されます。 傍受されたパケットは複製され、ラインカードから MD に送信されます。

VRF（6VPE）および 6PE パケットの傍受

ここでは、VRF 対応パケットおよび 6PE パケットの傍受について説明します。 この傍受の仕組みを説明する前に、6VPE ネットワークの基本的な知識について説明します。

MPLS VPN モデルは真のピア VPN モデルです。 このモデルは、プロバイダーのコンテンツ IAP ルータで一意の VPN ルート転送（VRF）テーブルを各カスタマーの VPN に割り当てることで、トラフィックの分離を実行します。 そのため、VPN 内のユーザは外部のトラフィックを見ることができません。

Cisco ASR 9000 Series Router は、6VPE において、指定した VRF ID の IPv6 パケットの傍受をサポートしています。 VPN 上のトラフィックを区別するために、特定の VRF ID を含む VRF が定義されています。 特定の VRF ID をタップするフィルタ条件は、タップ内で指定されます。 IPv6 パケットは、インポジション（ip2mpls）およびディスポジション（mpls2ip）の両方のシナリオで、VRF コンテキストを使用して傍受されます。

6PE パケットは VPN 上で IPv6 パケットを伝送します。 パケットには VRF ID は含まれていません。 IP トラフィックのみが傍受されます。MPLS ベースの傍受はサポートされていません。 IPv6 トラフィックは、インポジション（ip2mpls）およびディスポジション（mpls2ip）の MPLS クラウドのコンテンツ IAP で傍受されます。

ip2tag パケットおよび tag2ip パケットに対しても、IPv6 パケットの傍受が実行されます。 ip2tag パケットは、プロバイダーのコンテンツ IAP ルータで IPv6 からタギングに変換されたパケット（IPv6 to MPLS）を指し、tag2ip パケットは、プロバイダーのコンテンツ IAP ルータでタギングから IPv6 に変換されたパケット（MPLS to IPv6）を指します。

傍受パケットでサポートされるカプセル化タイプ

タップをマッピングする傍受パケットは複製およびカプセル化され、MD に送信されます。 IPv4 パケットおよび IPv6 パケットは、UDP（ユーザ データグラム プロトコル）カプセル化を使用してカプセル化されます。 複製されたパケットは、コンテンツ配信プロトコルに UDP を使用して、MD に転送されます。 IPv4 MD カプセル化のみサポートされています。

傍受パケットには、新しい UDP ヘッダーと IPv4 ヘッダーが付与されます。 IPv4 ヘッダーの情報は MD 設定から取得されます。 IP ヘッダーおよび UDP ヘッダーとは別に、4 バイトのチャネル ID（CCCID）もパケットの UDP ヘッダーの後に挿入されます。 MD カプセル化を追加した後、パケット サイズが MTU を超過する場合、出力 LC CPU はパケットをフラグメント化します。 また、タップされたパケットがすべてにフラグメントである場合もあります。 各タップには、MD が 1 つだけ関連付けられています。 Cisco ASR 9000 Series Router は、複数 MD への複製パケットの転送をサポートしていません。

（注） RTP や RTP-NOR などのカプセル化タイプはサポートされていません。

タップ別ドロップ カウンタのサポート

Cisco ASR 9000 Series Router ラインカードでは、インターフェイスとして SNMP サーバを提供し、MD パケットに転送された各タップとドロップ数をエクスポートします。 ポリサー処理により MD に転送される前にドロップされた傍受パケットは、すべてカウントおよびレポートされます。 ポリサー処理によりドロップされるパケットは、ドロップされるパケットの中で唯一タップ別ドロップ カウンタでカウントされます。 合法的傍受フィルタが変更された場合、パケット カウントは 0 にリセットされます。

（注） タップ別ドロップ カウンタのサポートは、ASR9000-SIP-700 ラインカードのみで利用できます。イーサネット ラインカードでは利用できません。

合法的傍受のハイ アベイラビリティ

合法的傍受のハイ アベイラビリティでは、タップ フローおよびプロビジョニングされた MD テーブルの継続的な運用を実現し、ルート プロセッサ フェールオーバー（RPFO）による情報の喪失を低減します。

ストリームの継続的な傍受を実現するには、RP フェールオーバーが検出された際に、MD が CISCO-TAP2-MIB、CISCO-IP-TAP-MIB、および CISCO-USER-CONNECTION-TAP-MIB に関連するすべての行を再プロビジョニングし、RP および MD にまたがるデータベース ビューを同期する必要があります。

（注） 合法的傍受のハイ アベイラビリティは、リリース 4.2.0 以降ではデフォルトでイネーブルになっています。

RP フェールオーバー中のタップおよび MD テーブルの維持

MD はあらゆるタイミングで SNMP 設定プロセスを通じて、タップの喪失を検出する役割を果たします。

RPFO が完了すると、MD はストリーム テーブルのすべてのエントリ、MD テーブル、および IP タップにフェールオーバー前と同じ値を再プロビジョニングする必要があります。 エントリが時間どおりに再プロビジョニングされる限り、既存のタップは喪失されずにフローを継続します。

citapStreamEntry、cTap2StreamEntry、cTap2MediationEntry MIB オブジェクトでの SNMP 操作の動作に関連して、MD テーブルおよびタップ テーブルの再プロビジョニングには次の制約事項があります。

- RPFO 後に、再プロビジョニングされていないテーブルの行は SNMP GET 操作の結果として NO_SUCH_INSTANCE 値を返します。

- テーブルの行全体が RPFO 前と完全に同じ値で、かつ rowStatus を CreateAndGo にして、1 回の設定ステップで作成される必要があります。 cTap2MediationTimeout オブジェクトのみは例外で、有効な未来時刻を反映する必要があります。

リプレイ タイマー

リプレイ タイマーは、MD が既存のタップ フローを維持しながらタップ エントリを再プロビジョニングするための十分な時間を確保する内部タイムアウトです。 RPFO が実行されると、このタイマーはアクティブな RP でリセットされ、開始されます。 リプレイ タイマーは、ルータ内の LI エントリ数の係数で、最小値は 10 分です。

リプレイ タイムアウト後、再プロビジョニングされていないタップでは傍受が停止します。

（注） ハイ アベイラビリティが必須でない場合、MD はフェールオーバー後にエントリがエージング アウトするまで待機します。 MD はリプレイ タイマーが満了するまでエントリを変更できません。 MD でタップをそのまま再インストールしてその後に変更を加えるか、エントリがエージング アウトするまで MD を待機させることができます。

ルータでの合法的傍受の SNMP v3 アクセスの設定方法

合法的傍受をイネーブルにする目的で管理プレーン保護（MPP）および SNMP を設定するには、次の手順を示されている順番で実行します。

合法的傍受のディセーブル化

合法的傍受は、この機能がサポートされているルータでは、デフォルトでイネーブルになっています。

- LI をディセーブルにするには、グローバル コンフィギュレーション モードで **lawful-intercept disable** コマンドを入力します。
- この機能を再度イネーブルにするには、このコマンドの **no** 形式を使用します。

（注） プロビジョニングされているアクティブなタップや MD が存在する場合は、LI をディセーブルにしないでください。 ディセーブルにした場合、ルータからすべてのタップと MD が削除されます。

インバンド管理プレーン保護機能の設定

以前にMPPを別のプロトコルと連携して動作するように設定していない場合は、合法的傍受の目的でMDと通信できるように、MPP機能を設定してSNMPサーバをイネーブルにする必要はありません。 このような場合だけ、明示的にMPPをインバンドインターフェイスとして設定し、指定したインターフェイスまたはすべてのインターフェイスを使用してSNMPコマンドをルータで受け付けられるようにする必要があります。

（注） 最近Cisco IOSからCisco IOS XRソフトウェアに移行し、任意のプロトコルに対してMPPを設定済みである場合は、この作業を実行する必要があります。

合法的傍受の目的で、ループバックインターフェイスをSNMPメッセージの宛先にする場合が多くあります。 このインターフェイス タイプを選択した場合は、インバンド管理設定にこのインターフェイス タイプを含める必要があります。

設定手順については、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の項を参照してください。 この手順のLIに関する例については、インバンド管理プレーン保護機能の設定：例, （15ページ）を参照してください。

インバンド管理インターフェイスの詳細な説明については、インバンド管理インターフェイスを参照してください。

VoIP およびデータ セッションを傍受するためのメディエーション デバイスのイネーブル化

次のSNMPサーバ設定作業では、MDによるVoIPまたはデータ セッションの傍受を許可することで、Cisco IOS XRソフトウェアを実行しているルータ上でCisco SII機能をイネーブルにします。

手順の概要

1. **configure**
2. **snmp-server view** *view-name* **ciscoTap2MIB included**
3. **snmp-server view** *view-name* **ciscoIpTapMIB included**
4. **snmp-server group** *group-name* **v3 auth read** *view-name* **write** *view-name* **notify** *view-name*
5. **snmp-server host** *ip-address* **traps version 3 priv** *username* **udp-port** *port-number*
6. **snmp-server user** *mduser-id groupname* **v3 auth md5** md-*password*
7. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**
8. show snmp users
9. show snmp group
10. show snmp view

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	**snmp-server view** *view-name* **ciscoTap2MIB included** 例： `RP/0//CPU0:router(config)# snmp-server view TapName ciscoTap2MIB included`	ビュー レコードを作成または変更し、CISCO-TAP2-MIB ファミリを含めます。
ステップ 3	**snmp-server view** *view-name* **ciscoIpTapMIB included** 例： `RP/0//CPU0:router(config)# snmp-server view TapName ciscoIpTapMIB included`	ビュー レコードを作成または変更し、CISCO-IP-TAP-MIB ファミリを含めます。
ステップ 4	**snmp-server group** *group-name* **v3 auth read** *view-name* **write** *view-name* **notify** *view-name*	新しい SNMP グループの設定、または SNMP ユーザを SNMP ビューにマップするテーブルの設定を行います。このグループは SNMP ビューの読み取り、書き込み、および通知権限を持っています。

	コマンドまたはアクション	目的
	例： `RP/0//CPU0:router(config)# snmp-server group TapGroup v3 auth read TapView write TapView notify TapView`	
ステップ 5	**snmp-server host** *ip-address* **traps version 3 priv** *username* **udp-port** *port-number* 例： `RP/0//CPU0:router(config)# snmp-server host 223.255.254.224 traps version 3 priv bgreen udp-port 2555`	SNMP トラップ通知、使用する SNMP のバージョン、通知のセキュリティ レベル、および通知の受信者（ホスト）を指定します。
ステップ 6	**snmp-server user** *mduser-id groupname* **v3 auth md5** md-*password* 例： `RP/0//CPU0:router(config)# snmp-server mduser-id TapGroup v3 auth md5 mdpassword`	MD パスワードと関連付ける v3 セキュリティ モデルと HMAC MD5 アルゴリズムを使用して、MD ユーザが SNMP グループに属するように設定します。 • *mduser-id* および *mdpassword* は MD に設定されている値と一致している必要があります。 あるいは、これらの値はルータで使用されている値と一致している必要があります。 • SNMPv3 セキュリティの最低基準を満たすには、パスワードの長さは 8 文字以上である必要があります。 • LI を利用する最低限のセキュリティ レベルは *auth* です。*noauth* では動作しません。 LI のセキュリティ レベルは MD のセキュリティ レベルとも一致している必要があります。 • ルータでは MD5 以外を選ぶこともできますが、MD 値は一致している必要があります。 ほとんどの MD では、MD5 がデフォルトになっているか、MD 5 のみをサポートしています。
ステップ 7	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`	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

	コマンドまたはアクション	目的
	または `RP/0/RSP0/CPU0:router(config)# commit`	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 8	show snmp users 例： `RP/0//CPU0:router# show snmp users`	SNMP ユーザ テーブルの各 SNMP ユーザ名に関する情報を表示します。
ステップ 9	show snmp group 例： `RP/0//CPU0:router# show snmp group`	ネットワークの各 SNMP グループの情報を表示します。
ステップ 10	show snmp view 例： `RP/0//CPU0:router# show snmp view`	関連付けられた MIB ビュー ファミリ名、ストレージ タイプ、ステータスなど、設定されたビューに関する情報を表示します。

インバンド管理プレーン機能のイネーブル化の設定例

次に、デフォルトでディセーブルになっているMPP機能を合法的傍受の目的でイネーブルにする方法の例を説明します。

インバンド管理プレーン保護機能の設定：例

次の手順を使用して、管理アクティビティをグローバルまたはインバンド ポート単位で明示的にイネーブルにする必要があります。 インバンド MPP をグローバルにイネーブルにするには、

interface コマンドで特定のインターフェイス タイプとインスタンス ID を使用するのではなく、**all** キーワードを使用します。

```
RP/0//CPU0:router# configure
RP/0//CPU0:router(config)# control-plane
RP/0//CPU0:router(config-ctrl)# management-plane
RP/0//CPU0:router(config-mpp)# inband
RP/0//CPU0:router(config-mpp-inband)# interface loopback0
RP/0//CPU0:router(config-mpp-inband-Loopback0)# allow snmp
RP/0//CPU0:router(config-mpp-inband-Loopback0)# commit
RP/0//CPU0:router(config-mpp-inband-Loopback0)# exit
RP/0//CPU0:router(config-mpp-inband)# exit
RP/0//CPU0:router(config-mpp)# exit
RP/0//CPU0:router(config-ctr)# exit
RP/0//CPU0:router(config)# exit
RP/0//CPU0:router# show mgmt-plane inband interface loopback0

Management Plane Protection - inband interface


interface - Loopback0
        snmp configured -
                All peers allowed
RP/0//CPU0:router(config)# commit
```

参考資料

ここでは、合法的傍受の実装に関連する参考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
合法的傍受コマンド	『*Cisco ASR 9000 Series Aggregation Services Router System Security Command Reference*』
SNMP の実装	『*Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide*』
SNMP サーバ コマンド	『*Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference*』

標準

標準	タイトル
サードパーティ機器と容易に通信してサービス プロバイダーの合法的傍受の要件を満たすシンプルな実装を目的に設計されたモジュール式のオープン アーキテクチャ。	RFC, （17 ページ）の RFC-3924 を参照してください。

標準	タイトル
ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコル。伝送制御プロトコル/インターネット プロトコル（TCP/IP）プロトコル スイートの一部。	『Simple Network Management Protocol Version 3 (SNMPv3)』

MIB

MIB	MIB リンク
• CISCO-TAP2-MIB バージョン 2 • CISCO-IP-TAP-MIB	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
RFC-3924	『Cisco Architecture for Lawful Intercept in IP Networks』

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、このページからログインして詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html