合法的傍受の実装

合法的傍受とは、傍受対象の通信の合法的な傍受と監視です。回線交換とパケットのモードのネットワーク行う電子機器を用いて情報収集し、司法当局を支援することが世界中のサービスプロバイダーに合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。

デフォルトでは、合法的傍受は Cisco IOS XR ソフトウェアに含まれていません。**ncs560-li-1.0.0.0-r66136I.x86_64.rpm** をインストールしてアクティブ化することによって、別途インストールする必要があります。

合法的傍受パッケージのアクティブ化と非アクティブ化の詳細については、「合法的傍受（LI）パッケージのインストール （5 ページ）」の項を参照してください。

合法的傍受の実装について

シスコの合法的傍受は、RFC3924 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、ルータから仲介デバイス（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 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。
- IPv4 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

合法的傍受の実装に関する前提条件

合法的傍受の実装には、次の前提条件を満たす必要があります。

- ルータは、合法的傍受操作でコンテンツ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。

  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。

- **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（ループバック インターフェイスが望ましい）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。
- 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、傍受する 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。
- 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

合法的傍受には次の制限が適用されます。

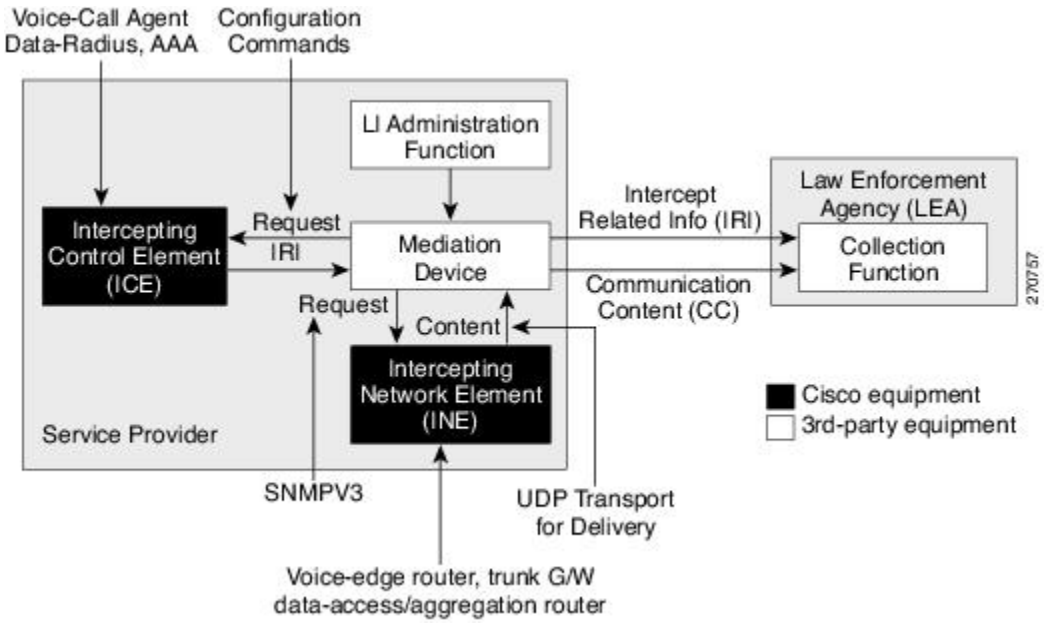
- 合法的傍受は、16 個の一意の送信元 IP アドレスのプールを tunnel-ip と共有します。GRE tunnel-ip と MD（cTap2MediationSrcInterface フィールド）を組み合わせた構成では、16 を超える一意の送信元 IP を生成してはいけません。MD を設定するときに、値 0 が cTap2MediationSrcInterface フィールドに渡されると、送信元 IP アドレスに解決されることに注意してください。その送信元 IP アドレスは、MD 宛先への出力 IP です。
- 合法的傍受は、純粋な IP over Ethernet パケットと照合するためにのみサポートされます。
- IPv4 では 250 の MD および 500 のタップのみがサポートされます。
- 複数の MD への単一タップはサポートされていません。
- ルートプロセッサのリロードまたはフェールオーバー後に、MD とタップの設定を再プロビジョニングする必要があります。
- IPv4 MD のみがサポートされています。
- MD へのパスには解決された ARP が必要です。その他のトラフィックまたはプロトコルで ARP をトリガーします。
- MD のネクストホップには解決された ARP が必要です。その他のトラフィックまたはプロトコルで ARP をトリガーします。
- 合法的傍受は GRE トンネル機能と交差することはありません。ただし、同じプールからハードウェアリソース（16 個の一意の出力 IP アドレス）が割り当てられる場合は除きます。通常、LI パケットの出力インターフェイスは転送アルゴリズムによって決まります。この一意のアドレスプールからのリソースは必要ありません。ただし、合法的傍受の設定で、合法的傍受パケットが特定のインターフェイス（MD 設定の cTap2MediationSrcInterface フィールド）を経由して出力する必要がある場合は、パケットがそのインターフェイスを通過するように転送モジュールを設定する必要があります。この場合、リソースは一意のアドレスプールから割り当てる必要があります。GRE ですべてのリソースが使用されている場合、LI は機能しません。
- 合法的傍受の統計情報はサポートされていません。
- 元のパケットをフラグメント化することはできますが、LI パケットをフラグメント化することはできません。MD への出力インターフェイスの MTU は、キャプチャされたパケットのサイズをサポートするのに十分な大きさである必要があります。
- 合法的傍受は、ルータで次の機能をサポートしていません。
  - IPv4 および IPv6 マルチキャスト タッピング
  - IPv6 MD カプセル化
  - インターフェイス別タッピング

- タグ付きパケット タッピング
- 複数の MD への単一タップの複製
- L2 フローのタッピング
- RTP のカプセル化
- 同じインターフェイス上の合法的傍受と SPAN

合法的傍受トポロジ

次の図に、音声とデータの両方の傍受のための、合法的傍受トポロジでの傍受アクセス ポイントとインターフェイスを示します。

図 *1:* 音声とデータの両方の傍受のための合法的傍受トポロジ



（注）

- ルータは、コンテンツ傍受アクセスポイント（IAP）ルータ、または合法的傍受オペレーションにおける傍受ネットワーク要素（INE）として使用されます。
- 傍受制御要素（ICE）は、シスコ機器またはサードパーティ機器のいずれかになります。

合法的傍受の利点

合法的傍受には、次の利点があります。

- 複数の LEA が相互に知られることなく同じルータに対して合法的傍受を実行できます。
- ルータでの加入者サービスには影響しません。
- 入力と出力の両方向の傍受をサポートします。
- レイヤ 3 トラフィックの傍受をサポートしています。
- ターゲットに気付かれません。
- 簡易ネットワーク管理プロトコルバージョン 3（SNMPv3）および View-based Access Control Model（SNMP-VACM-MIB）や User-based Security Model（SNMP-USM-MIB）などのセキュリティ機能を使用して、合法的傍受情報およびコンポーネントへのアクセスを制限します。
- 合法的傍受に関する情報を、最高特権を持つユーザ以外のユーザから秘匿します。管理者は、特権ユーザが法的傍受情報にアクセスできるアクセス権を設定する必要があります。

合法的傍受（LI）パッケージのインストール

LI はデフォルトで Cisco IOS XR イメージの一部ではないため、別途インストールする必要があります。

LI パッケージのインストールとアクティブ化

コミットされたソフトウェアパッケージを確認するには、EXEC モードで **show install committed** コマンドを使用します。

合法的傍受（LI）パッケージをインストールするには、**ncs560-li-1.0.0.0-r66136I.x86_64.rpm** をインストールしてアクティブ化する必要があります。

設定

```
Router# install add source
tftp://223.255.254.252/auto/tftp-sjc-users/username/ncs560-li-1.0.0.0-r66136I.x86_64.rpm
Router# install activate ncs560-li-1.0.0.0-r66136I.x86_64.rpm
Router# install commit
```

確認

```
Router# show install active
Node 0/RP0/CPU0 [RP]
  Boot Partition: xr_lv0
 Active Packages: 2
        ncs560-xr-6.6.1.36I version=6.6.1.36I [Boot image]
```

```
        ncs560-li-1.0.0.0-r66136I.x86_64.rpm

Node 0/0/CPU0 [LC]
  Boot Partition: xr_lcp_lv0
  Active Packages: 2
        ncs560-xr-6.6.1.36I version=6.6.1.36I [Boot image]
        ncs560-li-1.0.0.0-r66136I.x86_64.rpm
```

LI RPM の非アクティブ化

合法的傍受パッケージをアンインストールするには、次の手順に示すように、**ncs560-li-1.0.0.0-r66136I.x86_64.rpm** を非アクティブにします。

設定

```
Router# install deactivate ncs560-li-1.0.0.0-r66136I.x86_64.rpm
Router# install commit
Router# install remove ncs560-li-1.0.0.0-r66136I.x86_64.rpm
Router# show install committed
```

合法的傍受のための SNMPv3 アクセスを設定する方法

合法的傍受を有効化する目的で SNMPv3 を設定するには、次の手順を実行します。

SNMP ベースの合法的傍受のディセーブル化

合法的傍受は、**ncs560-li-1.0.0.0-r66136I.x86_64.rpm** をインストールしてアクティブにした後、ルータでデフォルトで有効になります。

- 合法的傍受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。
- 再び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。

SNMP ベースの合法的傍受のディセーブル化：例

```
Router# configure
Router(config)# lawful-intercept disable
```

（注） **ncs560-li-1.0.0.0-r66136I.x86_64.rpm** をインストールしてアクティブ化した後でのみ、**lawful-intercept disable** コマンドをルータで使用できます。

すべての SNMP ベースのタップは、合法的傍受がディセーブルのときはドロップします。

インバンド管理プレーン保護機能の設定

別のプロトコルを使用するように MPP を設定していない場合、合法的傍受用途で SNMP サーバにメディエーション デバイスとの通信を許可するように MPP 機能も設定されていないことを確認します。このような場合、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 コマンドがルータで許可されるように、MPP が明確にインバンド インターフェイスとして設定される必要があります。

（注） Cisco IOS から Cisco IOS XR ソフトウェアに最近移行し、MPP を所定のプロトコルに設定した場合でも、このタスクを必ず実行します。

合法的傍受では、多くの場合にループバック インターフェイスが SNMP メッセージに適しています。このインターフェイス タイプを選択した場合、インバンド管理設定にこれを含める必要があります。

例：インバンド管理プレーン保護機能の設定

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。

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。

```
router# configure
router(config)# control-plane
router(config-ctrl)# management-plane
router(config-mpp)# inband
router(config-mpp-inband)# interface loopback0
router(config-mpp-inband-Loopback0)# allow snmp
router(config-mpp-inband-Loopback0)# commit
router(config-mpp-inband-Loopback0)# exit
router(config-mpp-inband)# exit
router(config-mpp)# exit
router(config-ctr)# exit
router(config)# exit
router# show mgmt-plane inband interface loopback0
Management Plane Protection - inband interface
interface - Loopback0
        snmp configured -
All peers allowed
router(config)# commit
```

合法的傍受 SNMP サーバ設定の有効化

次の SNMP サーバ設定作業では、MD によるデータ 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 LI 機能をイネーブルにします。

設定

```
router(config)# snmp-server engineID local 00:00:00:09:00:00:00:a1:61:6c:20:56
router(config)# snmp-server host 1.75.55.1 traps version 3 priv user-name udp-port 4444
router(config)# snmp-server user user-name li-group v3 auth md5 clear lab priv des56
clear lab
router(config)# snmp-server view li-view ciscoTap2MIB included
router(config)# snmp-server view li-view ciscoIpTapMIB included
router(config)# snmp-server view li-view snmp included
router(config)# snmp-server view li-view ifMIB included
router(config)# snmp-server view li-view 1.3.6.1.6.3.1.1.4.1 included
router(config)# snmp-server group li-group v3 auth read li-view write li-view notify
li-view
```

（注） LI RPM を無効にしている間は、SNMP 設定を削除する必要があります。

合法的傍受に関する追加情報

傍受モード

合法的傍受は、**グローバル LI** モードで動作します。

このモードでは、タップはすべてのライン カードで入力方向に取り付けられます。合法的傍受は、QoS ピアリングが有効になっているライン カードで利用できます。グローバル タップを使用すると、入力点に関係なく、ターゲットのトラフィックを傍受できます。インターフェイス フィールドにワイルド カードを持つタップだけがサポートされています。

データの傍受

データは、次の方法で傍受されます。

- 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、IPv4 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。

スケールまたはパフォーマンスの値

ルータは、合法的傍受に対し次のスケーラビリティおよびパフォーマンスの値をサポートしています。

- IPv4、IPv6、または IPv4 と IPv6 の組み合わせでは、合法的傍受のタップ制限は最大 500 タップまでです。
- ポート範囲がタップで使用されている場合、スケールは減少します。
- IPv6 エントリは、IPv4 エントリのメモリを 2 倍消費します。したがって、IPv6 のスケールは IPv4 のスケールの半分に縮小されます。
- 最大 250 の IPv4 MD がサポートされます。
- 傍受率は、ラインカード NPU あたり 1 Gbps のベスト エフォートです。

IPv4 および IPv6 パケットの傍受

ここでは、ルータでサポートされる IPv4 および 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

タップの分類では、次のフィルタがサポートされています。

- 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
- L4 Protocol
- 範囲の宛先ポート
- 範囲の送信元ポート
- VRF（ルーティングおよび転送）

（注） フロー ID およびインターフェイスフィルタはサポートされていません。

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 および IPv6 パケットは、IPv4 UDP 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。

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。ルータは、同じ複製パケットを複数の MD に転送すること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。

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 および CISCO-IP-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。

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

任意の時点で、MDS は SNMP の設定プロセスによってタップの損失を検出する責任があります。

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。エントリが適時に再プロビジョニングされている限り、既存のタップは損失なく流れ続けます。

次の制限は、MD の再プロビジョニングと、citapStreamEntry、cTap2StreamEntry の cTap2MediationEntry MIB オブジェクトの SNMP 操作の動作に関連するタップ テーブルに適用されます。

- RPFO 後、再プロビジョニングされていないテーブルの行には、SNMP Get 操作の結果として、NO_SUCH_INSTANCE 値が返されます。
- 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。例外は、有効な将来の時刻を反映する cTap2MediationTimeout オブジェクトのみです。

リプレイ タイマー

再送タイマーは、既存のタップ フローを維持する間、再プロビジョニングのタップ エントリに対する MDS で十分な時間を提供する内部タイム アウトです。RPFO タスクが行われるときに、ACTIVE RP でリセットされて開始されます。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。

リプレイのタイムアウト後、傍受は再プロビジョニングされていないタップで停止します。

（注） ハイ アベイラビリティが必要ない場合、フェールオーバー後に MD はエントリがエージングアウトするのを待機します。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。タップを現状のまま再インストールして変更する、またはエージングアウトするのを待機できます。