合法的傍受

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

合法的傍受の前提条件

- セキュア シェル（SSH）、たとえば、s72033-adventerprisek9-mz をサポートする実行イメージを実行している必要があります。合法的傍受は SSH をサポートしないイメージではサポートされません。
- 最高アクセス レベル（レベル 15）でスイッチにログインしている必要があります。レベル 15 のアクセス権でログインするには、**enable** コマンドを入力し、スイッチに対して定義された最高レベルのパスワードを指定します。
- コマンドライン インターフェイス（CLI）では、コマンドをグローバル コンフィギュレーション モードで発行する必要があります。すべてのインターフェイスまたは特定のインターフェイスの合法的傍受をグローバルに設定できます。
- スイッチの時刻とメディエーション デバイスの時刻は同期する必要があります。スイッチとメディエーション デバイスの両方でネットワーク タイム プロトコル（NTP）を使用します。
- （任意）スイッチがメディエーション デバイスとの通信に使用するインターフェイスについて、ループバック インターフェイスを使用すると役立つ場合があります。ループバック インターフェイスを使用しない場合、スイッチ上の複数の物理インターフェイスで、ネットワーク障害を処理するために、メディエーション デバイスを設定する必要があります。

合法的傍受の制約事項

一般的な設定の制約事項

- VSS モードは合法的傍受をサポートしていません。
- ネットワーク管理者が、ノードに合法的傍受が展開されることを期待する場合、最適化された ACL ロギング（OAL）、VLAN アクセス コントロール リスト（VACL）キャプチャ、または侵入検知システム（IDS）をそのノードに設定しないでください。ノードに合法的傍受を展開すると、OAL、VACL キャプチャおよび IDS で予期しない動作が発生します。
- スイッチのパフォーマンスを維持するために、合法的傍受はアクティブ コールの 0.2 % 以下に制限されます。たとえば、スイッチが 4000 コールを処理している場合、それらのコールのうち 8 つのセッションを傍受できます。
- CISCO-IP-TAP-MIB は仮想ルーティングおよび転送（VRF）の OID citapStreamVRF をサポートしません。
- キャプチャされたトラフィックは、ルート プロセッサ上の CPU 使用率を保護するためにレート制限されています。レート制限は 8500 pps です。
- インターフェイス インデックスは、プロビジョニング中に合法的傍受をイネーブルにするインデックスを選択するためだけに使用されます。0 に設定すると、合法的傍受がすべてのインターフェイスに適用されます。
- （任意）スイッチとメディエーション デバイスの両方のドメイン名が、ドメイン ネーム システム（DNS）に登録されていることがあります。
- メディエーション デバイスには、アクセス ファンクション（AF）が必要です。
- メディエーション デバイスを、CISCO-TAP2-MIB ビューにアクセスできる SNMP ユーザ グループに追加する必要があります。グループに追加するユーザとして、メディエーション デバイスのユーザ名を指定します。

  メディエーション デバイスを CISCO-TAP2-MIB ユーザとして追加するときに、メディエーション デバイスの許可パスワードを指定する必要があります。パスワードの長さは、最低 8 文字である必要があります。
- 1 つのインターフェイスを合法的傍受処理専用にします。たとえば、QoS またはルーティングなどのプロセッサ集約的タスクを実行するインターフェイスを設定することはできません。
- IPv4 ユニキャスト トラフィックだけでサポートされます。また、傍受されるトラフィックでは、トラフィックが入力インターフェイスと出力インターフェイスの両方で IPv4 である必要があります。たとえば、合法的傍受では出力側が MPLS で入力側が IPv4 の場合、トラフィックを傍受できません。
- IPv4 マルチキャスト、IPv6 ユニキャスト、および IPv6 マルチキャスト フローはサポートされません。
- レイヤ 2 インターフェイスではサポートされません。ただし、合法的傍受は、レイヤ 2 インターフェイスを通して伝達される VLAN 上のトラフィックを傍受できます。
- 他のパケット内でカプセル化されるパケット（たとえば、トンネリング パケットまたは Q-in-Q パケット）に対してはサポートされていません。
- Q-in-Q パケットではサポートされません。合法的傍受のレイヤ 2 タップのサポートはありません。

- レイヤ 3 またはレイヤ 4 の書き換えの対象となるパケット（たとえば、ネットワーク アドレス変換（NAT）または TCP 反射式）に対してはサポートされていません。
- 入力方向では、後でパケットがドロップされる場合（たとえば、レート制限またはアクセス コントロール リスト（ACL）の **deny** ステートメントが原因で）、スイッチがパケットを傍受および複製します。出力方向では、パケットがドロップされる場合（たとえば、ACL による）、複製されません。
- 合法的傍受の ACL は、インターフェイスの入力および出力方向の両方に対して内部的に適用されます。
- 特定のユーザからのトラフィックを傍受するためには、一般的な構成は 2 つのフロー（各方向の 1 つずつ）から成ります。
- ハードウェア レート制限の対象のパケットは、合法的傍受で次のように処理されます。
  - レート リミッタによってドロップされるパケットは、傍受または処理されません。
  - レート リミッタを通過するパケットは、傍受および処理されます。
- 複数の LEA が 1 つのメディエーション デバイスを使用しており、それぞれが同じターゲットに対して傍受を実行している場合、スイッチは 1 つのパケットをメディエーション デバイスに送信します。各 LEA 用にパケットを複製するのは、メディエーション デバイスの役割です。
- 合法的傍受は、次の 1 つ以上のフィールドの組み合わせと一致する値の IPv4 パケットを傍受できます。
  - 宛先の IP アドレスとマスク
  - 宛先ポート範囲
  - 送信元 IP アドレスおよびマスク
  - 送信元ポート範囲
  - プロトコル ID

MIB ガイドライン

次の Cisco MIB が合法的傍受処理に使用されます。これらの MIB を合法的傍受 MIB の SNMP ビューに含めて、メディエーション デバイスがスイッチを通過するトラフィックに対する傍受を設定および実行できるようにします。

- CISCO-TAP2-MIB：両方のタイプの合法的傍受（通常およびブロードバンド）に必要です。
- CISCO-IP-TAP-MIB：レイヤ 3（IPv4）ストリームの傍受に必要です。通常およびブロードバンドの両方の合法的傍受でサポートされます。
- CISCO-IP-TAB-MIB では、次の機能に関して制限があります。
  - 次の機能の 1 つまたはすべてが設定され、機能しており、かつ合法的傍受がイネーブルの場合、合法的傍受が優先され、機能は次のように動作します。
    - 最適化された ACL ロギング（OAL）：機能しません。
    - VLAN アクセス コントロール リスト（VACL）キャプチャ：適切に動作しません。
    - 侵入検知システム（IDS）：適切に動作しません。

    この機能は、合法的傍受をディセーブルにした後または設定解除した後に開始されます。
  - IDS ではトラフィックを自分でキャプチャできませんが、合法的傍受によって傍受されたトラフィックだけはキャプチャします。

合法的傍受に関する情報

注意　このガイドは、合法的傍受の実装の法的義務に対応するものではありません。サービス プロバイダーには、そのネットワークが、適用される合法的傍受の法令および規制に適合することを保証する責任があります。法的な助言を求め、果たすべき義務を明確にすることを推奨します。

合法的傍受の概要

合法的傍受は、裁判所または行政機関による命令を根拠として、司法当局（LEA）が個人（ターゲット）に対して電子監視を実施できるようにするプロセスです。合法的傍受プロセスを容易にするために、特定の法律および規制によって、サービス プロバイダー（SP）およびインターネット サービス プロバイダー（ISP）に対して、許可された電子監視を明示的にサポートするようにネットワークを実装することが定められています。

監視は、音声、データ、およびマルチサービス ネットワークによる従来のテレコミュニケーションおよびインターネット サービスに対する傍受を使用して実行されます。LEA は、ターゲットのサービス プロバイダーに傍受を要求します。サービス プロバイダーには、その個人が送受信するデータ通信を傍受する責任があります。サービス プロバイダーは、ターゲットの IP アドレスを使用して、ターゲットのトラフィック（データ通信）を処理しているエッジ スイッチを判別します。次に、サービス プロバイダーは、ターゲットのトラフィックがスイッチを通過するときにそれを傍受し、傍受したトラフィックのコピーをターゲットに気付かれずに LEA に送信します。

合法的傍受機能は、米国内のサービス プロバイダーによる合法的傍受のサポート方法を定めた Communications Assistance for Law Enforcement Act（CALEA）をサポートしています。現在、合法的傍受は次の規格によって定義されています。

- Telephone Industry Association（TIA）仕様 J-STD-025
- Packet Cable Electronic Surveillance Specification（PKT-SP-ESP-101-991229）

シスコの合法的傍受ソリューションの詳細については、シスコの代理店にご連絡ください。

（注）　合法的傍受機能は、音声と日付の傍受を含む CISCO-IP-TAB-MIB のオブジェクト citapStreamprotocol の定義に従って IPv4 プロトコルの傍受をサポートします。

合法的傍受の利点

- 複数の LEA が相互に知られることなく同じターゲットに対して合法的傍受を実行できます。
- スイッチ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 1 およびレイヤ 3 トラフィックの傍受をサポートします。レイヤ 2 トラフィックは、VLAN 上の IP トラフィックとしてサポートされます。
- 単一の物理インターフェイスを共有する個々の加入者の傍受をサポートします。
- ターゲットに気付かれません。ネットワーク管理者も通話者もパケットがコピーされていることや通話が傍受されていることに気付きません。
- 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。
- 傍受を実行するための 2 つの保護されたインターフェイスがあります。1 つは傍受の設定用、もう 1 つは傍受したトラフィックの LEA への送信用です。

ボイスのための CALEA

音声用の法執行のための通信援助法（CALEA）によって、Voice over IP（VoIP）で伝送される音声会話の合法的傍受が認められています。スイッチは音声ゲートウェイ デバイスではありませんが、VoIP パケットはサービス プロバイダー ネットワークのエッジにあるスイッチを通過します。

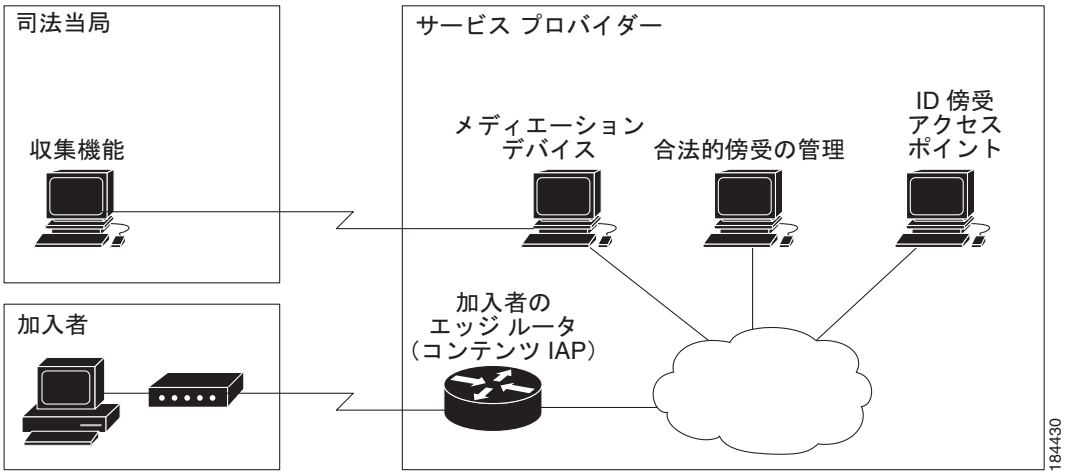
ある通話に注意を要すると認定された政府機関が判断した場合、ボイスのための CALEA は、会話を構成する IP パケットをコピーし、詳細な分析に適したモニタリング デバイスに重複パケットを送信します。

合法的傍受に使用されるネットワーク コンポーネント

- メディエーション デバイス
- 合法的傍受の管理
- 傍受アクセス ポイント
- コンテンツの傍受アクセス ポイント

合法的傍受処理については、「合法的傍受処理」（P.79-7）を参照してください。

図 79-1　　合法的傍受の概要



メディエーション デバイス

メディエーション デバイス（サードパーティ ベンダーから提供される）は、合法的傍受処理のほとんどを処理します。メディエーション デバイスは次の処理を行います。

- 合法的傍受の設定およびプロビジョニングに使用されるインターフェイスを提供します。
- 他のネットワーク デバイスに対して、合法的傍受を設定および実行する要求を生成します。
- 傍受したトラフィックを LEA が要求する形式（国によって異なる）に変換し、傍受したトラフィックのコピーをターゲットに気付かれずに LEA に送信します。

（注）　複数の LEA が同じターゲットに対して傍受を実行している場合、メディエーション デバイスは LEA ごとに傍受したトラフィックのコピーを作成する必要があります。メディエーション デバイスには、障害のために中断された合法的傍受を再開する役割もあります。

合法的傍受の管理

合法的傍受の管理（LIA）は、合法的傍受に認証インターフェイスや盗聴要求および管理を提供します。

傍受アクセス ポイント

傍受アクセス ポイント（IAP）は、合法的傍受に情報を提供するデバイスです。次の 2 つのタイプの IAP があります。

- Identification（ID）IAP : 傍受のための傍受関連情報（IRI）（ターゲットのユーザ名、システム IP アドレスなど）または、Voice over IP のコール エージェントを提供する認証、許可、アカウンティング（AAA）サーバなどのデバイス。IRI は、ターゲットのトラフィックが通過するコンテンツ IAP（スイッチ）をサービス プロバイダーが判別する場合に有用です。
- コンテンツ IAP : スイッチなどのターゲットのトラフィックが通過するデバイス。コンテンツ IAP は次の処理を行います。

- 司法命令で指定された期間、ターゲットが送受信するトラフィックを傍受します。傍受が気付かれないように、スイッチは宛先へのトラフィックの転送を継続します。
- 傍受したトラフィックのコピーを作成し、ユーザ データグラム プロトコル（UDP）パケットにカプセル化し、ターゲットに気付かれずにメディエーション デバイスにパケットを転送します。IP オプション ヘッダーはサポートされません。

（注）　コンテンツ IAP は、傍受したトラフィックの単一のコピーをメディエーション デバイスに送信します。複数の LEA が同じターゲットに対して傍受を実行している場合、メディエーション デバイスは LEA ごとに傍受したトラフィックのコピーを作成する必要があります。

コンテンツの傍受アクセス ポイント

コンテンツ IAP は、関連するデータ ストリームを傍受し、コンテンツを複製し、その後メディエーション デバイスに複製されたコンテンツを送信します。メディエーション デバイスは ID IAP およびコンテンツ IAP からデータを受信し、国別の要件に応じて必要な形式に情報を変換し、司法当局（LEA）に転送します。

合法的傍受処理

監視を実行する司法命令または令状を取得したあと、LEA はターゲットのサービス プロバイダーに監視を要求します。サービス プロバイダーの担当者は、メディエーション デバイスで実行される管理機能を使用して合法的傍受を設定し、ターゲットの電子トラフィックを（司法命令で定義された）特定の期間モニタリングします。

傍受を設定したあとは、ユーザの介入は必要ありません。管理機能が他のネットワーク デバイスと通信し、合法的傍受を設定および実行します。合法的傍受では、次の一連のイベントが発生します。

1. 管理機能は、ID IAP と通信して傍受関連情報（IRI）（ターゲットのユーザ名、システムの IP アドレスなど）を取得し、ターゲットのトラフィックが通過するコンテンツ IAP（スイッチ）を判別します。
2. ターゲットのトラフィックを処理するスイッチを特定したあと、管理機能は SNMPv3 の **get** および **set** 要求をスイッチの管理情報ベース（MIB）に送信し、合法的傍受を設定および有効化します。CISCO-TAP2-MIB は、加入者単位の傍受を提供する、サポートされた合法的傍受 MIB です。
3. 合法的傍受中に、スイッチは次の処理を行います。
   a. 着信および発信トラフィックを調べ、合法的傍受要求の指定と一致するトラフィックを傍受します。
   b. 傍受したトラフィックのコピーを作成し、ターゲットが疑いを持たないように元のトラフィックを宛先に転送します。
   c. 傍受したトラフィックを UDP パケットにカプセル化し、そのパケットをターゲットに気付かれずにメディエーション デバイスに転送します。

（注）　ターゲットのトラフィックの傍受および複製のプロセスによって、トラフィック ストリームに検出可能な遅延が発生することはありません。

4. メディエーション デバイスは、傍受したトラフィックを必要な形式に変換し、LEA で実行される収集機能に送信します。傍受したトラフィックはここに格納されて処理されます。

（注）　司法命令で許可されていないトラフィックをスイッチが傍受した場合、メディエーション デバイスは余分なトラフィックをフィルタで除外し、司法命令で許可されたトラフィックだけを LEA に送信します。

5. 合法的傍受の期間が終了すると、スイッチはターゲットのトラフィックの傍受を停止します。

合法的傍受 MIB

- CISCO-TAP2-MIB：合法的傍受処理に使用されます。
- CISCO-IP-TAP-MIB：レイヤ 3（IPv4）トラフィックを傍受する場合に使用されます。

CISCO-TAP2-MIB

CISCO-TAP2-MIB には合法的傍受を制御する SNMP 管理オブジェクトが含まれています。メディエーション デバイスはこの MIB を使用して、トラフィックがスイッチを通過するターゲットに対して合法的傍受を設定および実行します。

CISCO-TAP2-MIB には、スイッチで実行される合法的傍受に情報を提供する複数のテーブルが含まれています。

- cTap2MediationTable：スイッチで現在、合法的傍受を実行している各メディエーション デバイスに関する情報が含まれています。各テーブル エントリは、スイッチがメディエーション デバイスと通信するために使用する情報（デバイスのアドレス、傍受したトラフィックを送信するインターフェイス、傍受したトラフィックの送信に使用するプロトコルなど）を提供します。
- cTap2StreamTable：傍受するトラフィックを特定するために使用する情報が含まれています。各テーブル エントリには、合法的傍受のターゲットに関連するトラフィック ストリームを特定するために使用するフィルタへのポインタが含まれています。フィルタに一致するトラフィックが傍受およびコピーされて、対応するメディエーション デバイス アプリケーション（cTap2MediationContentId）に送信されます。

  cTap2StreamTable テーブルには、傍受されたパケット数のカウント、および傍受する必要があったが傍受されずにドロップされたパケットのカウントも含まれています。
- cTap2DebugTable：合法的傍受のエラーをトラブルシューティングするためのデバッグ情報が含まれています。

CISCO-TAP2-MIB には、合法的傍受イベントの複数の SNMP 通知も含まれています。MIB オブジェクトの詳細については、MIB 自体を参照してください。

CISCO-TAP2-MIB 処理

（メディエーション デバイスで実行される）管理機能によって、SNMPv3 の **set** および **get** 要求がスイッチの CISCO-TAP2-MIB に対して発行され、合法的傍受が設定および開始されます。このために、管理機能によって次の処理が実行されます。

1. cTap2MediationTable のエントリを作成し、スイッチが傍受を実行するメディエーション デバイスと通信する方法を定義します。

（注）　cTap2MediationNewIndex オブジェクトによって、メディエーション テーブル エントリの一意のインデックスが提供されます。

2. cTap2StreamTable にエントリを作成し、傍受するトラフィック ストリームを特定します。
3. cTap2StreamInterceptEnable を true(1) に設定し、傍受を開始します。スイッチは、傍受期間（cTap2MediationTimeout）が終了するまでストリーム内のトラフィックを傍受します。

CISCO-IP-TAP-MIB

CISCO-IP-TAP-MIB には、スイッチを通過する IPv4 トラフィック ストリームでの合法的傍受を設定および実行するための SNMP 管理オブジェクトが含まれています。この MIB は、CISCO-TAP2-MIB の拡張です。

CISCO-IP-TAP-MIB を使用して、次の 1 つ以上のフィールドの組み合わせと一致する値の IPv4 パケットを傍受するようにスイッチでの合法的傍受を設定できます。

- 宛先の IP アドレスとマスク
- 宛先ポート範囲
- 送信元 IP アドレスおよびマスク
- 送信元ポート範囲
- プロトコル ID

CISCO-IP-TAP-MIB 処理

データが傍受されると、2 つのストリームが作成されます。1 つ目のストリームは、ターゲット IP アドレスから他の IP アドレスに任意のポートを使用して送信されるパケット用です。2 つ目のストリームは、他のアドレスからターゲット IP アドレスに任意のポートを使用してルーティングされるパケットに対して作成されます。VoIP では、2 つのストリームが作成されます。1 つ目はターゲットからの RTP パケット用であり、2 つ目はターゲットへの RTP パケット用です。これらのパケットは、特定の送信元および宛先 IP アドレス、および RTP ストリームを設定するために使用される SDP 情報に指定されたポートを使用します。

合法的傍受サポートの設定方法

セキュリティに関する注意事項

- 合法的傍受の SNMP 通知は、メディエーション デバイス ポート上の UDP ポート 161（SNMP のデフォルトのポート 162 ではなく）に送信されます。手順については、「合法的傍受のための SNMP 通知のイネーブル化」（P.79-12）を参照してください。
- 合法的傍受 MIB にアクセスできるユーザは、メディエーション デバイス、およびスイッチでの合法的傍受について知る必要があるシステム管理者だけにします。また、これらのユーザには、合法的傍受 MIB にアクセスするための authPriv または authNoPriv アクセス権が必要です。NoAuthNoPriv アクセス権を持つユーザは、合法的傍受 MIB にアクセスできません。

- SNMP-VACM-MIB を使用して合法的傍受 MIB を含むビューを作成することはできません。
- デフォルトの SNMP ビューでは次の MIB は除外されています。

  CISCO-TAP2-MIB
  CISCO-IP-TAP-MIB
  SNMP-COMMUNITY-MIB
  SNMP-USM-MIB
  SNMP-VACM-MIB

「合法的傍受の制約事項」（P.79-2）と「合法的傍受の前提条件」（P.79-1）も参照してください。

合法的傍受 MIB へのアクセス

機密に関係するため、シスコの合法的傍受 MIB は合法的傍受機能をサポートするソフトウェア イメージだけで使用できます。これらの MIB には、Network Management Software MIBs Support ページ（http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml）からはアクセスできません。

合法的傍受 MIB へのアクセスの制限

合法的傍受 MIB へのアクセスは、メディエーション デバイスおよび合法的傍受について知る必要があるユーザだけに許可する必要があります。これらの MIB へのアクセスを制限するには、次の作業を実行する必要があります。

1. シスコの合法的傍受 MIB を含むビューを作成します。
2. このビューへの読み取りおよび書き込みアクセス権を持つ SNMP ユーザ グループを作成します。このユーザ グループに割り当てられたユーザだけが、MIB の情報にアクセスできます。
3. シスコの合法的傍受ユーザ グループにユーザを追加して、MIB および合法的傍受に関する情報にアクセスできるユーザを定義します。このグループのユーザとして、メディエーション デバイスを追加してください。追加しないと、スイッチで合法的傍受を実行できません。

（注）　シスコの合法的傍受 MIB ビューへのアクセスは、メディエーション デバイス、およびスイッチでの合法的傍受について知る必要があるシステム管理者だけに制限する必要があります。MIB にアクセスするには、スイッチ上でレベル 15 のアクセス権がユーザに必要です。

SNMPv3 の設定

次の手順を実行するには、スイッチで SNMPv3 が設定されている必要があります。次の資料を参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/configuration/15-sy/snmp-15-sy-book.html

合法的傍受 MIB の制限付き SNMP ビューの作成

シスコの合法的傍受 MIB を含む SNMP ビューを作成し、ユーザを割り当てるには、グローバル コンフィギュレーション モードでレベル 15 のアクセス権を使用して、CLI で次の手順を実行します。コマンドの例については、「設定例」（P.79-11）を参照してください。

（注）　次の手順のコマンド構文には、各作業の実行に必要なキーワードだけが示されています。コマンド構文の詳細については、前の項（「SNMPv3 の設定」）に記載されているマニュアルを参照してください。

ステップ 1　スイッチで SNMPv3 が設定されていることを確認します。手順については、「SNMPv3 の設定」（P.79-10）に記載されているマニュアルを参照してください。

ステップ 2　CISCO-TAP2-MIB を含む SNMP ビューを作成します（*view_name* は、MIB 用に作成するビューの名前です）。この MIB は、通常とブロードバンドの両方の合法的傍受に必要です。

```
Router(config)# snmp-server view view_name ciscoTap2MIB included
```

ステップ 3　次の MIB の 1 つまたは両方を SNMP ビューに追加して、IPv4 ストリームに対する傍受のサポートを設定します（*view_name* は、ステップ 2 で作成したビューの名前です）。

```
Router(config)# snmp-server view view_name ciscoIpTapMIB included
```

ステップ 4　合法的傍受 MIB ビューにアクセスできる SNMP ユーザ グループ（*groupname*）を作成し、ビューに対するこのグループのアクセス権を定義します。

```
Router(config)# snmp-server group groupname v3 noauth read view_name write view_name
```

ステップ 5　作成したユーザ グループにユーザを追加します（*username* はユーザ、*groupname* はユーザ グループ、*auth_password* は認証パスワード）。

```
Router(config)# snmp-server user username groupname v3 auth md5 auth_password
```

（注）　SNMP ユーザ グループにメディエーション デバイスを追加してください。追加しないと、スイッチで合法的傍受を実行できません。合法的傍受 MIB ビューへのアクセスは、メディエーション デバイス、およびルータでの合法的傍受について知る必要があるシステム管理者だけに制限する必要があります。

これで、メディエーション デバイスは合法的傍受 MIB にアクセスして、SNMP の **set** および **get** 要求を発行し、スイッチ上で合法的傍受を設定および実行できるようになります。

SNMP 通知をメディエーション デバイスに送信するためのスイッチの設定方法については、「合法的傍受のための SNMP 通知のイネーブル化」（P.79-12）を参照してください。

設定例

次のコマンドは、メディエーション デバイスが合法的傍受 MIB にアクセスできるようにする方法の例です。

```
Router(config)# snmp-server view tapV ciscoTap2MIB included
Router(config)# snmp-server view tapV ciscoIpTapMIB included
```

1. 適切な合法的傍受 MIB（CISCO-TAP2-MIB および CISCO-IP-TAP-MIB）を含むビュー（tapV）を作成します。
2. tapV ビューの MIB への読み取り、書き込み、および通知アクセス権を持つユーザ グループ（tapGrp）を作成します。
3. メディエーション デバイス（ss8user）をユーザ グループに追加し、パスワード（ss8passwd）を使用して MD5 認証を指定します。

4. （任意）管理用に 24 文字の SNMP エンジン ID（123400000000000000000000 など）をスイッチに割り当てます。エンジン ID を指定しない場合は、自動的に生成されます。上記の例の最後の行に示されているように、エンジン ID の後ろのゼロは省略できることに注意してください。

（注） エンジン ID を変更すると、SNMP ユーザ パスワードおよびコミュニティ ストリングに影響します。

合法的傍受のための SNMP 通知のイネーブル化

SNMP では、合法的傍受イベントの通知が自動的に生成されます（表 79-1 を参照）。これは、cTap2MediationNotificationEnable オブジェクトのデフォルト値が true(1) であるためです。

メディエーション デバイスに合法的傍受通知を送信するようにスイッチを設定するには、グローバル コンフィギュレーション モードでレベル 15 のアクセス権を使用して、次の CLI コマンドを発行します（*MD-ip-address* はメディエーション デバイスの IP アドレス、*community-string* は通知要求とともに送信するパスワードに似たコミュニティ ストリング）。

```
Router(config)# snmp-server host MD-ip-address community-string udp-port 161 snmp
Router(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart
warmstart
```

- 合法的傍受では、**udp-port** は 161 である必要があります。162（SNMP のデフォルト）ではありません。
- 2 つ目のコマンドは、メディエーション デバイスに RFC 1157 通知を送信するようにスイッチを設定します。これらの通知は、認証の失敗、リンク ステータス（アップまたはダウン）、およびスイッチ再起動を示します。

表 79-1　合法的傍受イベントの SNMP 通知

通知	意味
cTap2MIBActive	スイッチは、CISCO-TAP2-MIB に設定されたトラフィック ストリームのパケットを傍受する準備ができています。
cTap2MediationTimedOut	合法的傍受が終了しました（cTap2MediationTimeout の期限切れのためなど）。
cTap2MediationDebug	cTap2MediationTable のエントリに関するイベントの場合、介入が必要になります。
cTap2StreamDebug	cTap2StreamTable のエントリに関するイベントの場合、介入が必要になります。

SNMP 通知のディセーブル

no snmp-server enable traps コマンドを入力して、SNMP 通知をディセーブルにできます。

合法的傍受通知をディセーブルにするには、SNMPv3 を使用して CISCO-TAP2-MIB オブジェクト cTap2MediationNotificationEnable を false(2) に設定します。SNMPv3 を通じて合法的傍受の通知を再度イネーブルにするには、オブジェクトに true（1）を再設定します。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する