合法的傍受の設定

合法的傍受の前提条件

- セキュアシェル（SSH）をサポートする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。
- ログインしているスイッチは、最高のアクセスレベル（L15）である必要があります。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。
- ネットワークに接続されているスイッチとメディエーションデバイス（サードパーティベンダーが提供）の時刻を同期する必要があります。また、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）を設定します。
- （オプション）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

- インターセプトまたはタップは、SNMP のみを使用して構成できます。また、インターフェイス固有の傍受の設定は許可されていません。

- 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。
- 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。Only IPv4 ユニキャストトラフィックのみがサポートされています。
- 合法的傍受は、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。
- 合法的傍受は、トンネルパケットや Q-in-Q パケットなど、他のパケット内にカプセル化されたパケットではサポートされていません。
- 合法的傍受は、レイヤ 2 タップではサポートされていません。
- 合法的傍受は、ネットワークアドレス変換（NAT）や TCP 再帰など、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ではサポートされていません。

合法的傍受に関する情報

合法的傍受の概要

合法的傍受は、法執行機関が、司法（裁判所）または行政命令によって承認された個人（ターゲット）に対して電子監視を実行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およびインターネットサービス プロバイダーに対して、認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。法執行機関は、個人との間のデータ通信を傍受する責任があるターゲットのサービスプロバイダーに盗聴の要求を配信します。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、どのエッジデバイスがターゲットのトラフィック（データ通信）を処理するかを決定します。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デバイス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 citapStreamprotocol オブジェクトの定義に従って 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。
- デバイス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。
- レイヤ 3 物理インターフェイスまたはスイッチ仮想インターフェイス（SVI）をサポートします。
- 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ー以外のユーザーから秘匿します。管理者は、特権ユーザー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、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。デバイス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でデバイスを通過します。

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。

設定時の注意事項

- 合法的傍受をノードに展開するには、ノードで最適化された ACL ロギング、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、最適化された ACL ロギング、VACL キャプチャ、および IDS で予測できない動作が発生します。
- メディエーションデバイスをプロビジョニングするときに、渡されるインターフェイスインデックスがゼロの場合、スイッチはメディエーションデバイスに到達するために可能な限り最適なインターフェイスを選択します。インターフェイスインデックスが別の値に設定されている場合、スイッチはそのインターフェイスインデックスを使用してメディエーションデバイスに到達します。
- （任意）デバイス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 ユーザー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も指定する必要があります。
- デバイスは、たとえばレート制限やアクセスコントロールリスト（ACL）の拒否ステートメントが原因でパケットが後でドロップされた場合でも、パケットを傍受および複製します。
- 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。
- 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 リミッタによって廃棄されるパケットは、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。
- 複数の法執行機関が単一の仲介デバイスを使用し、これらの各機関が同じターゲットで盗聴を実行している場合、デバイスは単一のパケットを仲介デバイスに送信します。法執行機関ごと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

合法的傍受に使用されるネットワーク コンポーネント

このセクションでは、合法的傍受に使用されるネットワークコンポーネントについて説明します。

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ー名、システム IP アドレスなど）または、VoIP 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）サーバーなどのデバイス。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：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、デバイス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、ユーザー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） 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、国固有の要件に応じて情報を必要な形式に変換し、法執行機関に転送します。

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に接続して、ターゲットのユーザー名やシステムの IP アドレスなどのインターセプト関連情報（IRI）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デバイスを識別した後、管理機能は SNMPv3 の取得および設定要求をデバイスの管理情報ベース（MIB）に送信して、合法的傍受を設定およびアクティブ化します。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、デバイスは次のことを行います。
    1. 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。
    2. 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接続先に転送します。
    3. 傍受されたトラフィックを 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を傍受して複製するプロセスでは、トラフィックストリームに検出可能な遅延は追加されません。

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） デバイスが司法命令で許可されていないトラフィックを傍受した場合、メディエーションデバイスは過剰なトラフィックを除外し、司法命令で許可されたトラフィックのみを LEA に送信します。

5. 合法的傍受が期限切れになると、デバイス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。

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。Cisco IOS MIB Locator ページにアクセスするには、次の場所に移動します。

http://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index。

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、トラフィックがデバイス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、デバイス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：デバイスで合法的傍受を現在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、デバイス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を提供します。たとえば、デバイスのアドレス、傍受されたトラフィックを送信するためのインターフェイス、傍受されたトラフィックの送信に使用するプロトコルなどです。
- 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、対応する MIB を参照してください。

CISCO-TAP2-MIB 処理

管理機能（メディエーションデバイスで実行）によって、SNMPv3 セットが発行され、デバイスの CISCO-TAP2-MIB に要求を取得し、合法的傍受を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 エントリを作成して、デバイス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。デバイスは、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、デバイスを通過する 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デバイス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 の場合、2 つのストリームが作成されます。1 つはターゲットからの RTP パケット用で、もう 1 つは RTP ストリームの設定に使用される SDP 情報で指定された特定の送信元および宛先 IP アドレスとポートを使用してターゲットにする RTP パケット用です。

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デバイス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：通常およびブロードバンドを含む両方のタイプの合法的傍受に必要です。
- CISCO-IP-TAP-MIB：レイヤ3（IPv4）ストリームのワイヤータップに必要です。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。

    これらの機能は、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 はそれ自体でトラフィックをキャプチャすることはできませんが、合法的傍受によって傍受されたトラフィックをキャプチャします。

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。
- 合法的傍受 MIB にアクセスできるユーザーは、メディエーションデバイス、およびデバイス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 （1 ページ）」および「合法的傍受の前提条件 （1 ページ）」で提供される情報も参照することをお勧めします。

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ーグループにユーザーを追加して、合法的傍受に関連する情報（ある場合）とともに、MIB にアクセスできるユーザーを定義します。このグループのユーザーとして、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、デバイス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、およびデバイス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、デバイス上でレベル 15 のアクセス権がユーザーに必要です。

合法的傍受の設定方法

合法的傍受 MIB の制限付き SNMP ビューの作成

ユーザーを作成して、シスコの合法的傍受 MIB を含む SNMP ビューに割り当てるには、ここに示す手順を実行します。

始める前に

- デバイスで SNMPv3 が設定されている必要があります。

（注） コマンドは、レベル 15 のアクセス権で、グローバル コンフィギュレーション モードで実行します。

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 モードを有効にします。パスワードを入力します（要求された場合）。
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	**snmp-server view** *view-name MIB-name* **included** 例： `Device(config)# snmp-server view exampleView ciscoTap2MIB included`	CISCO-TAP2-MIB を含む SNMP ビューを作成します（ここで、*exampleView* は、MIB に対して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。
ステップ 4	**snmp-server view** *view-name MIB-name* **included** 例： `Device(config)# snmp-server view exampleView ciscoIpTapMIB included`	CISCO-IP-TAP-MIB を SNMP ビューに追加します。

	コマンドまたはアクション	目的
ステップ 5	**snmp-server view** *view-name MIB-name* **included** 例： `Device(config)# snmp-server view exampleView cisco802TapMIB included`	CISCO-802-TAP-MIB を SNMP ビューに追加します。
ステップ 6	**snmp-server view** *view-name MIB-name* **included** 例： `Device(config)# snmp-server view exampleView ciscoUserConnectionTapMIB included`	CISCO-USER-CONNECTION-TAP-MIB を SNMP ビューに追加します。
ステップ 7	**snmp-server view** *view-name MIB-name* **included** 例： `Device(config)# snmp-server view exampleView ciscoMobilityTapMIB included`	CISCO-MOBILITY-TAP-MIB を SNMP ビューに追加します。
ステップ 8	**snmp-server group** *group-name* **v3 auth read** *view-name* **write** *view-name* 例： `Device(config)# snmp-server group exampleGroup v3 auth read exampleView write exampleView`	LI MIB ビューにアクセス可能な SNMP ユーザ グループを作成し、グループのビューに対するアクセス権を定義します。
ステップ 9	**snmp-server user** *user-name group-name* **v3 auth md5** *auth-password* 例： `Device(config)# snmp-server user exampleUser exampleGroup v3 auth md5 examplePassword`	指定したユーザ グループにユーザを追加します。
ステップ 10	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

合法的傍受のための SNMP 通知のイネーブル化

SNMP は、合法的傍受イベントについての通知を自動的に生成します。合法的傍受通知をメディエーションデバイスに送信するようにデバイスを設定するには、ここに示す手順を実行します。

始める前に

- SNMPv3 がデバイスで設定されている必要があります。

（注） コマンドは、レベル 15 のアクセス権で、グローバル コンフィギュレーション モードで実行します。

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 モードを有効にします。 • パスワードを入力します（要求された場合）。
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	**snmp-server host** *ip-address* **community-string udp-port** *port notification-type* 例： `Device(config)# snmp-server host 10.2.2.1 community-string udp-port 161 udp`	メディエーション デバイスの IP アドレスと、通知要求とともに送信されるパスワードに似たコミュニティ ストリングを指定します。 • 合法的傍受では、**udp-port** は 162（SNMP のデフォルト）ではなく 161 とする必要があります。
ステップ 4	**snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart** 例： `Device(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart`	RFC 1157 通知をメディエーションデバイスに送信するようにデバイスを設定します。 • 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）、およびデバイス再起動を示します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SNMP 通知のディセーブル

デバイスで SNMP 通知を無効にするには、このセクションに記載されている手順を実行します。

（注） 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。

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 モードを有効にします。パスワードを入力します（要求された場合）。
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	**no snmp-server enable traps** 例： `Device(config)# no snmp-server enable traps`	システムで使用可能なすべての SNMP 通知タイプをディセーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

合法的傍受の設定例

例：メディエーション デバイス アクセスの合法的傍受 MIB の有効化

次に、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例を示します。この例では、3 つの LI MIB（CISCO-TAP2-MIB、CISCO-IP-TAP-MIB、CISCO-802-TAP-MIB）を含む SNMP ビュー（tapV）を作成します。また、tapV ビュー内の MIB に読み込み、書き込み、通知アクセス可能なユーザ グループも作成します。

```
Device> enable
Device# configure terminal
Device(config)# snmp-server view tapV ciscoTap2MIB included
Device(config)# snmp-server view tapV ciscoIpTapMIB included
Device(config)# snmp-server view tapV cisco802TapMIB included
Device(config)# snmp-server group tapGrp v3 auth read tapV write tapV notify tapV
Device(config)# snmp-server user MDuser tapGrp v3 auth md5 MDpasswd
Device(config)# snmp-server engineID local 1234
Device(config)# end
```

合法的傍受の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Gibraltar 16.11.1	合法的傍受	合法的傍受機能は、法執行機関の要件を満たす際にサービスプロバイダーをサポートし、管轄または行政命令によって承認されている電子サーベイランスを提供します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。