Cisco 10000 シリーズ
ルータ合法的傍受コンフィギュレーション ガイド

May 2008

Text Part Number: OL-3426-05-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。
米国サイト掲載ドキュメントとの差異が生じる場合があるため、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。
また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

CONTENTS

はじめに

このマニュアルでは、Cisco 10000 シリーズ ルータでの Lawful Intercept（LI; 合法的傍受）機能の実装について説明します。

合法的傍受とは、Law Enforcement Agency（LEA; 法執行機関）が、裁判所の命令による権限に基づいて、個人に対して電子的監視を実行するプロセスです。この監視を支援するために、サービス プロバイダーは、サービス プロバイダーのルータを通過する時点でターゲットのトラフィックを傍受し、傍受したトラフィックのコピーを、ターゲットにわからないように LEA に送信します。

マニュアルの変更履歴

Cisco IOS リリース	Part Number	発行日	説明
Release 12.2(31)SB12	OL-3426-05	2008 年 5 月	MPL 機能に合法的傍受を追加
Release 12.2(31)SB2	OL-3426-04	2008 年 3 月	合法的傍受に関する制限事項の更新
Release 12.2(31)SB2	OL-3426-03	2006 年 11 月	新しい MIB サポート情報を追加
Release 12.2(28)SB2	OL-3426-02	2006 年 6 月	履歴テーブルと設定情報を追加
Release 12.3(7)XI	OL-3426-01	2004	初版リリース

対象読者

このマニュアルは、合法的傍受をサポートするようルータを設定する必要があるシステム管理者を対象にしています。また、このマニュアルは、合法的傍受と併用する管理アプリケーションを開発しているアプリケーション開発者にも役立ちます。

マニュアルの構成

このマニュアルは、次の章で構成されています。

- 第 1 章「合法的傍受の概要」では、合法的傍受およびその実装に関する背景情報について説明します。また、合法的傍受に使用する CISCO-TAP2-MIB についても説明します。MIB（管理情報ベース）を使用すると、SNMP（簡易ネットワーク管理プロトコル）を使用してルータを制御できます。
- 第 2 章「合法的傍受のサポートの設定」では、ルータで合法的傍受をサポートするための設定手順について説明します。
- 索引

表記法

このマニュアルでは、コマンドの記述に、次の表記法を使用しています。

太字	コマンド、ユーザ入力、およびキーワードは、**太字**で示しています。
イタリック体	ユーザが値を指定する引数および新規の用語は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{ x | y | z }	必ずどれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。

例では、次の表記法を使用しています。

`screen` フォント	システムが表示する端末セッションおよび情報は、`screen` フォントで示しています。
太字の **`screen`** フォント	ユーザが入力しなければならない情報は、**太字**の **`screen`** フォントで示しています。
< >	パスワードのように出力されない文字は、かぎカッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。

注意および警告は、次の表記法を使用しています。

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

マニュアルの入手方法および Service Request ツールの使用

マニュアルの入手方法、Service Request ツールの使用方法、追加情報の収集方法については、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。ここには、シスコの新規および改訂版の技術マニュアルの一覧も掲載されています。次の URL にアクセスしてください。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』の Really Simple Syndication（RSS）フィードを登録すると、コンテンツがデスクトップに直接配信され、リーダー アプリケーションで閲覧できます。RSS フィードは無料のサービスです。現在、シスコでは RSS バージョン 2.0 をサポートしています。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。

Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register/

CHAPTER 1

合法的傍受の概要

この章では、Lawful Intercept（LI; 合法的傍受）に関する次の情報について説明します。

注意 このマニュアルでは、合法的傍受の実装に関する法律上の義務については扱っていません。サービス プロバイダーは、自社のネットワークが、適用される合法的傍受の法規制に準拠していることを確認する責任があります。専門家に相談して、法律上の義務について確認することを推奨します。

合法的傍受の概要

合法的傍受とは、Law Enforcement Agency（LEA; 法執行機関）が、裁判所または行政の命令による権限に基づいて、個人（ターゲット）に対して電子的監視を実行するプロセスです。合法的傍受のプロセスを容易にするために、特定の法規制により、Service Provider（SP; サービス プロバイダー）および Internet Service Provider（ISP; インターネット サービス プロバイダー）は、自社のネットワーク上で認可された電子的監視を明示的にサポートするよう義務づけられています。

この監視を実行するには、音声、データ、およびマルチサービス ネットワークの従来の通信サービスおよびインターネット サービス上で、通信傍受を行います。LEA は、ターゲットのサービス プロバイダーに対して傍受要求を配信します。サービス プロバイダーは、個人間の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 アドレスまたはセッションから、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 ルータを判別します。さらに、サービス プロバイダーは、このルータを通過する時点でターゲットのトラフィックを傍受し、傍受したトラフィックのコピーを、ターゲットにわからないように LEA に送信します。

合法的傍受機能は、米国内のサービス プロバイダーに対して要求される合法的傍受の支援方法を定めた Communications Assistance for Law Enforcement Act（CALEA）に準拠しています。現在、合法的傍受は、次の標準規格により定義されています。

- 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に関する詳細は、シスコのアカウント担当者にお問い合わせください。

合法的傍受の機能履歴

Cisco IOS リリース	説明
Release 12.2(31)SB12	MLP 向け合法的傍受機能が PRE2 および PRE3 向け Cisco 10000 シリーズ ルータに追加されました。
Release 12.3(7)XI	この機能が、Cisco IOS Release 12.3(7)XI に統合され、PRE2 対応の Cisco 10000 シリーズ ルータに実装されました。
Release 12.2(28)SB	機能拡張により、RADIUS ベースの合法的傍受サポートが追加され、CISCO-TAP-MIB が CISCO-TAP2-MIB に変更されました。
Release 12.2(31)SB2	CISCO-USER-CONNECTION- TAP-MIB を含めるように機能が拡張されました。

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、同じターゲットに対して合法的傍受を実行できます。
- ルータ上の加入者サービスに影響を及ぼしません。
- ターゲットは合法的傍受を探知できません。
- LEA は、サービス プロバイダーに知られずに、合法的傍受を実行できます。
- SNMPv3（簡易ネットワーク管理プロトコル Version 3）、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、合法的傍受の情報およびコンポーネントへのアクセスを制御できます。
- 合法的傍受に関する情報を、この情報にアクセスできる最高権限を持つユーザ以外には隠すことができます。管理者は、特権レベルのユーザのアクセス権限を、合法的傍受情報にアクセスできるよう設定する必要があります。

- 2 つのセキュア インターフェイスを使用して、傍受を実行できます。ひとつは通信傍受を設定するインターフェイスで、もうひとつは傍受したトラフィックをメディエーション デバイスに送信するインターフェイスです。
- Cisco 10000 シリーズでは、次の PPPo*X* セッションで通信傍受がサポートされます。
  - PPPoA
  - PPPoE
  - PPPoEoA
  - PPPoEoVLAN
  - PPPoEoQinQ
- Cisco 10000 シリーズ ルータの IPv4 合法的傍受では、次の MLP バンドル インターフェイスのトラフィックがサポートされます。
  - MLP over Serial
  - MLP over Single VC ATM
  - MLP over Multi VC ATM
  - MLP over FR_
- Cisco IOS Release 12.2(31)SB2 以上のリリースでは、ルータは、ルータに設定された Routed Bridged Encapsulation（RBE; ルーテッド ブリッジ エンカプセレーション）を使用した合法的傍受をサポートします（RFC 1483）。

レイヤ 2 およびレイヤ 3 傍受を使用した代行受信

合法的傍受機能では、次に示すレイヤ 2 およびレイヤ 3 傍受がサポートされます。

- レイヤ 2 傍受 ― レイヤ 3 の内容に関係なく、セッションで送受信されるすべてのトラフィックを代行受信するセッションベースの傍受。レイヤ 2 傍受は、SNMP バージョン 3 プロビジョニングおよび RADIUS ベースの合法的傍受によって設定され、CISCO-TAP2-MIB および CISCO-USER- CONNECTION-TAP-MIB が使用されます。
- レイヤ 3 傍受 ― SNMPv3 プロビジョニングを使ってアクセス可能な IP レイヤで代行受信します。レイヤ 3 傍受では、CISCO-TAP2-MIB および CISCO-IP-TAP-MIB が使用されます。

レイヤ 2 およびレイヤ 3 傍受の詳細については、表 2-2（p.2-7）を参照してください。

SNMPv3 プロビジョニングの合法的傍受要求の開始

SNMPv3 プロビジョニングの合法的傍受要求は、SNMPv3 メッセージを使用して、メディエーション デバイスにより開始されます。IP アドレスまたはセッションで送受信されるトラフィック データはすべて、メディエーション デバイスに転送されます。SNMPv3 プロビジョニングでは、次の合法的傍受 MIB が使用されます。

- CISCO-TAP2-MIB
- CISCO-IP-TAP-MIB
- CISCO-USER-CONNECTION-TAP-MIB

MLP 向け合法的傍受

Cisco 10000 シリーズ ルータは、ネットワークにおけるコンテンツ Intercept Access Point（IAP; 傍受アクセス ポイント）です。MLP 向け合法的傍受機能では、MLP バンドル インターフェイスを経由する加入者トラフィックの合法的傍受がサポートされます。MLP バンドルでの LI のサポートは、IPv4 トラフィック傍受のみに限られます。

RADIUS を使用した合法的傍受の要求

RADIUS ベースの合法的傍受ソリューションでは、RADIUS サーバから NAS または LAC に対して（Access-Accept パケットまたは CoA-Request パケット経由で）傍受要求を送信できます。PPP または L2TP セッションで送受信されるトラフィック データはすべて、メディエーション デバイスに転送されます。

RADIUS ベースの合法的傍受の利点は、ソリューションの同時性です。傍受は、Access-Accept パケットを使用して設定されるため、ターゲットのすべてのトラフィックが傍受されます。

CALEA for Voice を使用した会話の傍受

CALEA for Voice 機能により、Voice over IP（VoIP）上で行われている音声通話の合法的傍受が可能です。Cisco 10000 シリーズ ルータは音声ゲートウェイ装置ではありませんが、VoIP パケットは、サービス プロバイダーのネットワーク エッジにあるルータを通過します。CALEA for Voice は、完全な合法的傍受ソリューションに含まれるコンポーネントの 1 つで、外部モニタリングおよびサードパーティ製の管理デバイスで構成されます。

認可された政府機関により監視対象となる通話が検出されると、CALEA for Voice はこの会話の IP パケットをコピーし、さらに分析するために適切なモニタリング装置に複製したパケットを送信します。ネットワーク管理者も会話の当事者も、パケットがコピーされていること、または電話が傍聴されていることに気づきません。

（注） PRE2 では、CALEA for Voice は、レイヤ 3 傍受機能をサポートしており、32 の同時傍受、および探知されることなく 6.1 Mbps（すべてのトラフィック対象）の最高速度を実現します。

合法的傍受に使用するネットワーク コンポーネント

合法的傍受では、次のネットワーク コンポーネントを使用します。

- メディエーション デバイス（p.1-4）
- IAP（p.1-5）
- 収集プログラム（p.1-5）

合法的傍受のプロセスの詳細については、「合法的傍受のプロセス」（p.1-5）を参照してください。

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 ベンダー製）は、合法的傍受のほとんどのプロセスを管理します。メディエーション デバイスは、次の機能を実行します。

- 合法的傍受の設定およびプロビジョニングのための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、合法的傍受の設定と実行を要求します。
- 傍受したトラフィックを、LEA が要求する形式（国により異なる）に変換し、このトラフィックのコピーを、ターゲットに気づかれずに LEA に送信します。

（注） 複数の LEA が同じターゲットを傍受している場合、メディエーション デバイスは各 LEA に対して、傍受したトラフィックのコピーを作成します。また、障害により合法的傍受が中断された場合に、これを再開するのもメディエーション デバイスです。

IAP

Intercept Access Point（IAP）は、合法的傍受の情報を提供するデバイスです。次の 2 種類の IAP を使用できます。

- Identification（ID）IAP ― （ターゲットのユーザ名およびシステム IP アドレスなど）傍受した *Intercept Related Information*（IRI; 傍受関連情報）を提供する、Authentication, Authorization, Accounting（AAA; 認証、認可、アカウンティング）サーバなどのデバイスです。サービス プロバイダーは、IRI により、ターゲットのトラフィックが通過する コンテント IAP（ルータ）を判別します。
- コンテント IAP ― ターゲットのトラフィックが通過する、Cisco 10000 シリーズ ルータなどのデバイスです。コンテント IAP は、次の機能を実行します。
  - 裁判所の命令により指定された期間、ターゲットの送受信トラフィックを傍受します。通信傍受が探知されないように、ルータはトラフィックを宛先に転送し続けます。
  - 傍受したトラフィックのコピーを作成し、UDP パケットにカプセル化し、ターゲットに気づかれずにパケットをメディエーション デバイスに転送します。

（注） コンテント IAP は、メディエーション デバイスに、傍受したトラフィックのコピーを送信します。複数の LEA が同じターゲットを傍受している場合、メディエーション デバイスは各 LEA に対して、傍受したトラフィックのコピーを作成します。

収集プログラム

収集プログラムは、LEA の機器で稼働するソフトウェア プログラムです。これは、サービス プロバイダーによって傍受されたトラフィックを保存および処理するプログラムです。

合法的傍受のプロセス

裁判所から監視の実行に対する命令または保証を取得すると、LEA はターゲットのサービス プロバイダーに監視要求を配信します。サービス プロバイダーの担当者は、メディエーション デバイス上で管理機能を実行し、（裁判所の命令により定義された）特定の期間、ターゲットの電子トラフィックをモニタリングする合法的傍受を設定します。

傍受の設定後は、ユーザが介入する必要はありません。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、次のイベント シーケンスが発生します。

1. 管理機能が ID IAP と通信し、ターゲットのユーザ名およびシステム IP アドレスなどの *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ト IAP（ルータ）を判別します。
2. ターゲットのトラフィックを処理するルータが識別されると、管理機能はルータの MIB に対して SNMPv3 の **get** および **set** 要求を発行し、合法的傍受を設定して、起動します。ルータの MIB には、CISCO-TAP2-MIB および CISCO-IP-TAP-MIB、および CISCO-USER-CONNECTION-TAP-MIB が含まれます。
3. 合法的傍受の実行中、ルータは次の機能を実行します。
   a. 着信および発信トラフィックを調べ、合法的傍受要求の条件に一致するすべての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、ターゲットに疑われないようにコピー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、ターゲットに気づかれずに、パケットをメディエーション 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り、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要求された形式に変換し、LEA で実行される収集機能に転送します。ここで、傍受したトラフィックが保管および処理されます。

   ルータが裁判所命令により許可されていないトラフィックを傍受した場合には、メディエーション デバイスにより不要なトラフィックがフィルタリングされ、裁判所命令により許可されたトラフィックだけが LEA に送信されます。

（注） 複数の合法的傍受が行われている場合、パケット カウントは個々のデータ ストリームではなく、メディエーション デバイスのエントリに基づきます。たとえば、合法的傍受により 2 つのストリームが傍受され、ストリームごとに 1000 パケットが送信されるとします。メディエーション デバイスは 2000 パケットを受信し、ストリームごとのパケット カウントは 2000 になります。非ハードウェア傍受パケットが Route Processor（RP; ルート プロセッサ）でルーティングされる場合、パケット カウントはストリームによって決まります。

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

CISCO-TAP2-MIB

CISCO-TAP2-MIB には、ルータ上の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、トラフィックがルータ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。この MIB は、合法的傍受機能をサポートするシスコのソフトウェア イメージにバンドルされています。

CISCO-TAP2-MIB の内容

CISCO-TAP2-MIB には、ルータで実行する合法的傍受の情報を提供する、いくつかのテーブルが含まれています。

- cTap2MediationTable ― 現在、ルータ上で合法的傍受を実行している各メディエーション デバイスの情報が含まれています。テーブルの各エントリは、ルータがメディエーション デバイスと通信するための情報（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転送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識別するための情報が含まれています。テーブルの各エントリには、合法的傍受のターゲットに関連するトラフィック ストリームを識別する、フィルタへのポインタが含まれています。フィルタと一致したトラフィックが傍受され、コピーされて、対応するメディエーション デバイスのアプリケーション（cTap2MediationContentId）に送信されます。

  このテーブルには、傍受したパケット数、傍受すべきなのに傍受しなかったドロップ パケット数のカウントも含まれています。
- cTap2DebugTable ― 合法的傍受のエラーに関するトラブルシューティング用のデバッグ情報が含まれています。

この MIB には、合法的傍受イベントに関するいくつかの SNMP 通知も含まれています。MIB オブジェクトの詳細な説明は、MIB を参照してください。

CISCO-TAP2-MIB のプロセス

（メディエーション デバイス上で実行される）管理機能により、ルータの CISCO-TAP2-MIB に SNMPv3 の **set** および **get** 要求が発行され、合法的傍受を設定および開始します。管理機能は、次の動作を実行します。

1. cTap2MediationTable のエントリを作成し、ルータと、傍受を実行するメディエーション デバイスとの通信方法を定義します。

   （注） cTap2MediationNewIndex オブジェクトにより、メディエーション テーブル エントリに固有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 ストリームを識別します。
3. cTap2StreamInterceptEnable を true(1) に設定して、傍受を開始します。ルータは、傍受の設定時間が終了するまで（cTapMediationTimeout）、ストリーム内のトラフィックを傍受します。

CISCO-TAP2-MIB の拡張 MIB

CISCO-TAP2-MIB には、次の拡張 MIB が含まれます。

- CISCO-IP-TAP-MIB ― IP アドレスに基づいて傍受します。
- CISCO-USER-CONNECTION-TAP-MIB ― RADIUS ベースのユーザ接続傍受

関連情報

合法的傍受に関するその他の情報については、シスコのアカウント担当者にお問い合わせください。

CHAPTER 2

合法的傍受のサポートの設定

この章では、Lawful Intercept（LI; 合法的傍受）の設定方法について説明します。未許可ユーザが、合法的傍受を実行できないように、または傍受の関連情報にアクセスできないようにすることが必要です。

この章の内容は、次のとおりです。

合法的傍受の前提条件

合法的傍受のサポートを設定するには、次の前提条件を満たす必要があります。

- 最高レベルのアクセス権限（レベル 15）でルータにログインする必要があります。レベル 15 のアクセス権限でログインするには、**enable** コマンドを入力して、ルータに定義されている最上位パスワードを指定します。
- CLI（コマンドライン インターフェイス）のグローバル コンフィギュレーション モードでコマンドを入力する必要があります。
- （任意）ルータがメディエーション デバイスと通信するインターフェイスに、ループバック インターフェイスを使用すると役立つことがあります。

セキュリティの考慮事項

ルータに合法的傍受を設定する際は、次のセキュリティ事項に留意してください。

- 合法的傍受の SNMP 通知は、メディエーション デバイスの UDP ポート 162（SNMP のデフォルト）ではなく、ポート 161 に送信する必要があります。詳細は、「合法的傍受の SNMP 通知のイネーブル化」（p.2-7）を参照してください。
- Lawful Intercept MIB へのアクセスを許可するユーザは、メディエーション デバイスと、ルータ上の合法的傍受について認識している必要のあるシステム管理者だけにします。これらのユーザには、Lawful Intercept MIB にアクセスするための authPriv または authNoPriv アクセス権限を設定する必要もあります。NoAuthNoPriv アクセス権限が設定されたユーザは、Lawful Intercept MIB にアクセスできません。
- SNMP-VACM-MIB を使用して、Lawful Intercept 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 ビューは、次の MIB が除外されています。
- CISCO-TAP2-MIB
  CISCO-IP-TAP-MIB
  CISCO-USER-CONNECTION-TAP-MIB
  SNMP-COMMUNITY-MIB
  SNMP-USM-MIB
  SNMP-VACM-MIB

詳細については、「制限および制約事項」（p.2-3）および「合法的傍受の前提条件」（p.2-2）を参照してください。

制限および制約事項

- ルータでは、RADIUS ベースの合法的傍受用の L2TP LNS セッションはサポートされません。
- ルータのパフォーマンスを保持するために、合法的傍受はアクティブ コールの 0.2% 未満に制限されています。たとえば、ルータが 4000 コールを処理している場合、傍受できるのは 8 コールまでです。
- Cisco IOS Release 12.2(31)SB では、PRE2 および PRE3 上で CISCO-IP-TAP-MIB の citapStreamVRF OID を使用する Virtual Routing and Forwarding（VRF）対応 IP 傍受がサポートされます。
- PRE1 では、合法的傍受はサポートされません。
- 音声およびデータの傍受は、Cisco IOS Release 12.2(7)XI 以上のリリースでサポートされます。
- マルチキャスト パケットの傍受はレイヤ 3 傍受を使用します。ただし、対象となる ID が MAC アドレスの場合は傍受されません。
- Cisco IOS Release 12.2(28)SB では、PXF によってレイヤ 2 傍受が処理され、RP によってレイヤ 3 傍受が処理されます。
- Cisco IOS Release 12.2(31)SB では、PXF によって PRE2 および PRE3 の両方のレイヤ 3 傍受が処理されます。

表 2-1 に、Cisco IOS ソフトウェアの合法的傍受機能の説明を示します。

表 2-1　合法的傍受の実装

Cisco IOS リリース	傍受の種類	傍受のキャパシティ	PRE	MIB	RP/PXF[1]
Release 12.3(7)XI	レイヤ 3 SNMPv3	すべてのアクティブな傍受で合計 6.4 Mbps	PRE2	CISCO-TAP-MIB	RP
Release 12.2(28)SB	レイヤ 2 RADIUS	4095 同時傍受	PRE2	CISCO-TAP2-MIB	PXF
	レイヤ 3 SNMPv3	すべてのアクティブな傍受で合計 6.4 Mbps	PRE2		RP
Release 12.2(31)SB	レイヤ 2 RADIUS	4095 同時傍受	PRE2、PRE3	CISCO-TAP2-MIB	PXF
	レイヤ 3 SNMPv3	4095 同時傍受	PRE2、PRE3		PXF

1. 傍受された各パケットは、RP または Parallel Express Forwarding（PXF）エンジンによって処理されます。

設定の注意事項

ルータで、メディエーション デバイスと通信して合法的傍受を実行するには、次の設定要件を満たす必要があります。

- ルータとメディエーション デバイスの両方のドメイン名が、Domain Name System（DNS; ドメイン ネーム システム）に登録されている必要があります。
- DNS では、ルータの IP アドレスは通常、ルータの FastEthernet0/0/0 インターフェイスのアドレスです。
- メディエーション デバイスに、Access Function（AF）および Access Function Provisioning Interface（AFPI）が設定されている必要があります。
- 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、必要に応じて、メディエーション デバイスの許可パスワードを設定できます。このパスワードは、8 文字以上の長さにする必要があります。

Lawful Intercept MIB へのアクセス

Cisco Lawful Intercept MIB は、機密事項に関わるものであるため、合法的傍受機能をサポートするソフトウェア イメージだけに提供されています。これらの MIB は、Network Management Software MIB 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。

Lawful Intercept MIB へのアクセスの制限

Lawful Intercept MIB へのアクセスを許可するのは、メディエーション デバイスと、合法的傍受について知っている必要のあるユーザだけにします。これらの MIB へのアクセスを制限するには、次の作業を行う必要があります。

1. Cisco Lawful Intercept 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たユーザだけが、MIB の情報にアクセスできます。
3. Cisco Lawful Intercept ユーザ グループにユーザを追加し、MIB および合法的傍受の関連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 デバイスを必ず追加してください。追加しないと、ルータで合法的傍受を実行できません。

（注） CISCO-TAP2-MIB および CISCO-IP-TAP-MIB ビューへのアクセスは、メディエーション デバイスと、ルータ上の合法的傍受を認識している必要のあるシステム管理者だけに制限してください。MIB にアクセスするには、ユーザはルータ上でレベル 15 のアクセス権限を所有している必要があります。

SNMPv3 の設定

次の手順を実行するには、ルータ上に SNMPv3 が設定されている必要があります。

- Lawful Intercept MIB を含む、制限付き SNMP ビューの作成（p.2-5）

SNMPv3 の設定方法、および以降の項目で説明するコマンドの詳細については、次のシスコ マニュアルを参照してください。

- 『*Cisco IOS Configuration Fundamentals Configuration Guide*』Part 3：System Management の「Configuring SNMP Support」のセクション。次の URL から入手できます。
  http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf014.html
- 『*Cisco IOS Network Management Command Reference*』の「SNMP Commands」のセクション。次の URL から入手できます。
  http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_book.html

Lawful Intercept MIB を含む、制限付き SNMP ビューの作成

Cisco Lawful Intercept MIB を含む SNMP ビューを作成してユーザを割り当てるには、レベル 15 のアクセス権限を使用し、CLI のグローバル コンフィギュレーション モードで次の作業を行います。この手順の完了すると、メディエーション デバイスは、Lawful Intercept MIB にアクセスし、SNMP の **set** および **get** 要求を発行して、ルータ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。

ステップ 1　ルータ上に SNMPv3 が設定されていることを確認します。詳細については、「SNMPv3 の設定」（p.2-5）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 および CISCO-IP-TAP-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）。

```
Router(config)# snmp-server view view_name cTap2MIB included
```

ステップ 3　CISCO-TAP2-MIB および CISCO-IP-TAP-MIB ビューにアクセスできる SNMP ユーザ グループを作成し、このグループのビューへのアクセス権限を定義します。

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

ステップ 4　作成したユーザ グループにユーザを追加します（*username* はユーザ名、*groupname* はユーザ グループ名、*auth_password* は認証パスワードです）。

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

（注）　このユーザ グループに、メディエーション デバイスを必ず追加してください。追加しないと、ルータで合法的傍受を実行できません。CISCO-TAP2-MIB ビューへのアクセスは、メディエーション デバイスと、ルータ上の合法的傍受について認識している必要のあるシステム管理者だけに制限してください。

上述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含まれています。コマンド構文の詳細については、「SNMPv3 の設定」（p.2-5）に記載されているマニュアルを参照してください。

メディエーション デバイスに SNMP 通知を送信するためのルータの設定方法については、「合法的傍受の SNMP 通知のイネーブル化」（p.2-7）を参照してください。

設定例

次に、メディエーション デバイスが Lawful Intercept Tap MIB にアクセスできるように設定する例を示します。**snmp-server group** コマンドの形式は、PRE2 カード搭載のルータ用であることに注意してください。

```
Router(config)# snmp-server view tapV cTap2MIB included
Router(config)# snmp-server group tapGrp v3 noauth read tapV write tapV notify tapV
Router(config)# snmp-server user ss8user tapGrp v3 auth md5 ss8passwd
Router(config)# snmp-server engineID local engineid-string
```

1. 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を許可するユーザ グループ（tapGrp）を作成します。
3. このユーザ グループにメディエーション デバイス（ss8user）を追加し、パスワード（ss8passwd）を設定して、MD5 認証を指定します。
4. （任意）ルータに管理用の 24 文字の SNMP エンジン ID を割り当てます。特定のエンジン ID を指定しない場合、自動的に 1 つの エンジン ID が生成されます。エンジン ID を変更すると、SNMP ユーザのパスワードおよびコミュニティ ストリングに影響することに注意してください。

合法的傍受の SNMP 通知のイネーブル化

SNMP は、合法的傍受イベントの通知を自動的に生成します（表 2-2 を参照）。デフォルトで、cTap2MediationNotificationEnable オブジェクトが true(1) に設定されるからです。

ルータがメディエーション デバイスに対して合法的傍受通知を送信するように設定するには、レベル 15 のアクセス権限を使用して、CLI のグローバル コンフィギュレーション モードで、次のコマンドを入力します（*MD-ip-address* はメディエーション デバイスの IP アドレス、*community-string* は通知要求と一緒に送信するパスワードに似たコミュニティ ストリングです）。

```
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
```

- 合法的傍受の場合、**udp-port** は 162（SNMP のデフォルト）ではなく、161 に設定する必要があります。
- 2 番めのコマンドは、ルータがメディエーション デバイスに RFC 1157 通知を送信するように設定しています。これらの通知は、認証エラー、リンク ステータス（アップまたはダウン）、およびルータの再起動を示します。

表 2-2 に、合法的傍受イベント用に生成される MIB 通知を示します。

表 2-2　合法的傍受イベント用の SNMP 通知

通知	意味
cTap2MIBActive	ルータは、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（cTap2MediationTimout の時間切れなど）。
cTap2MediationDebug	cTap2MeditationTable エントリに関するイベントに、対処が必要です。
cTap2StreamDebug	cTap2StreamTable エントリに関するイベントに、対処が必要です。
cTap2Switchover	冗長設定のアクティブ Route Processor（RP; ルート プロセッサ）がスタンバイ モードに、スタンバイ RP がアクティブ RP に切り替わります。

SNMP 通知のディセーブル化

ルータの SNMP 通知は、次の手順でディセーブルに設定できます。

- すべての SNMP 通知をディセーブルにするには、**no snmp-server enable traps** コマンドを使用します。
- 合法的傍受の通知をディセーブルにするには、SNMPv3 を使用して、CISCO-TAP2-MIB オブジェクトの cTap2MediationNotificationEnable を false(2) に設定します。合法的傍受の通知を再びイネーブルにするには、SNMPv3 を使用して、このオブジェクトを true(1) にリセットします。

INDEX

か

け

こ

し

せ

つ

て

と

ひ

め

れ