Cisco 7600 合法的傍受コンフィギュレーション ガイド

Cisco IOS Software Release 12.2SRC
December 2007

Text Part Number: OL-12352-02-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、Lawful Intercept（LI; 合法的傍受）機能を Cisco 7600 シリーズ ルータに実装する方法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サーベイランスを実行するプロセスのことです。サービス プロバイダーはこのサーベイランスを援助するために、ターゲットのトラフィックがサービス プロバイダーのルータを通過する際に傍受を行い、傍受したトラフィックのコピーをターゲットに知られることなく LEA に送信します。

マニュアルの変更履歴

表 1 に、このマニュアルに加えられた技術的な変更内容を示します。

表 1　　マニュアルの変更履歴

Cisco IOS リリース	Part Number	日付	変更点
リリース 12.2SRC	OL-12352-02	2007 年 12 月	VRF 単位の LI 機能およびその使用上のガイドラインのほか、SIP-400 Accelerated Lawful Intercept（ALI）に関する情報を追加
リリース 12.2SRB	OL-12352-02-J	2007 年 2 月	最初のリリース

対象読者

このマニュアルは、合法的傍受をサポートするためにルータを設定する必要のあるシステム管理者を対象にしています。また、合法的傍受と併用する管理アプリケーションを開発す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

このマニュアルの内容は、次のとおりです。

- 第 1 章「合法的傍受の概要」では、合法的傍受とその実装に関する背景情報について説明します。また、合法的傍受に使用される CISCO-TAP2-MIB と CISCO-IP-TAP-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。

表記法

このマニュアルのコマンドの説明では、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しい用語は、*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。

注釈および注意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、テクニカル サポート、およびセキュリティ ガイドライン

マニュアルの入手方法、サポート、マニュアルに関するフィードバックの提供、セキュリティ ガイドライン、および推奨するエイリアスと一般的なシスコのマニュアルに関する情報については、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧が示されています。この情報には、次の URL からアクセスしてください。

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

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）の情報について説明します。内容は次のとおりです。

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 プロバイダーには、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）に対して電子的サーベイランスを実行するプロセスのことです。合法的傍受のプロセスを容易にするため、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、認可された電子的サーベイランスを自社のネットワーク上で明示的にサポートすることが定められています。

このサーベイランスを実行するには、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通信傍受の要請を行います。サービス プロバイダーは個人に送受信され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。サービス プロバイダーは、ターゲットのトラフィックがこのルータを通過する際に傍受を行い、傍受したトラフィックのコピーをターゲットに知られることなく、LEA に送信します。

合法的傍受機能は、米国内のサービス プロバイダーに求められる合法的傍受のサポート方法を定めた Communication 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の詳細については、シスコのアカウント担当者にお問い合わせください。

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、互いに知ることなく、同じターゲットに対して合法的傍受を実行できます。
- ルータの加入者サービスに影響を与えません。
- 通信傍受を入力と出力の両方向でサポートします。
- レイヤ 3 およびレイヤ 2 トラフィックの通信傍受をサポートします。
- 1 つの物理インターフェイスを共有する個々の加入者に対する通信傍受をサポートします。
- ターゲットは合法的傍受を検知できません。ネットワーク管理者も通話当事者も、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づきません。
- SNMPv3（簡易ネットワーク管理プロトコル Verison 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限できます。
- 合法的傍受に関する情報へのアクセスを、最高特権を持つユーザだけに限定できます。管理者は、特権ユーザが合法的傍受情報にアクセスできるように、アクセス権を設定する必要があります。
- 2 つのセキュリティ インターフェイスを使用して、傍受を実行できます。1 つは通信傍受を設定するインターフェイス、もう 1 つは傍受したトラフィックを LEA に送信するインターフェイスです。

CALEA for Voice

CALEA for Voice 機能により、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 7600 シリーズ ルータ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 プロバイダーのネットワークのエッジにあるルータを通過します。

認可された政府機関により通話が傍受の対象になると判断されると、CALEA for Voice 機能によりこの通話の IP パケットがコピーされて、詳しく分析するために、適切なモニタリング デバイスに送信されます。

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。

- MD
- IAP
- 収集機能

合法的傍受のプロセスについては、「合法的傍受のプロセス」（p.1-4）を参照してください。

MD

合法的傍受のほとんどのプロセスは、Mediation Device（MD; メディエーション デバイス）（サードパーティ ベンダー製）によって処理されます。MD 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知られることなく 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、MD は、傍受したトラフィックのコピーを LEA ごとに作成する必要があります。また、障害によって中断された合法的傍受を再開するのも MD の役割です。

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。IAP には、次の 2 種類があります。

- Identification（ID）IAP ― 傍受に必要な Intercept-Related Information（IRI; 傍受関連情報）（ターゲットのユーザ名、システム IP アドレスなど）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。サービス プロバイダーは、IRI の情報により、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）を特定します。
- コンテント IAP ― ターゲットのトラフィックが通過する、Cisco 7600 シリーズ ルータなどのデバイス。IAP には次の機能があります。
  - 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。ルータは、宛先にトラフィックの転送を続けて、通信傍受が検知されないようにします。
  - 傍受したトラフィックのコピーを作成し、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）パケットにカプセル化し、このパケットをターゲットに知られることなく MD に転送します。

（注） コンテント IAP は、MD に、傍受したトラフィックのコピーを 1 つ送信します。複数の LEA が同じターゲットを傍受している場合、MD は、傍受したトラフィックのコピーを LEA ごとに作成する必要があります。

収集機能

収集機能は、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の格納と処理を行うプログラムです。このプログラムは、LEA にある機器上で動作します。

合法的傍受のプロセス

LEA は、裁判所からサーベイランスを実行する命令または令状を取得したあと、ターゲットが加入しているサービス プロバイダーにサーベイランスを要請します。サービス プロバイダーの担当者は、MD で管理機能を実行して、（裁判所の命令に従い）ターゲットの電子トラフィックを特定の期間モニタリングするために合法的傍受の設定を行います。

傍受を設定したあとは、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、合法的傍受の設定を行って実行します。合法的傍受では、次の一連の処理が行われます。

1. 管理機能は ID IPA と通信し、ターゲットのユーザ名やシステム 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）を特定します。
2. ターゲットのトラフィックを処理するルータが特定されると、管理機能により、そのルータの MIB に対して **get** および **set** 要求が発行され、合法的傍受が設定されてアクティブになります。合法的傍受の MIB には、CISCO-TAP2-MIB、CISCO-IP-TAP-MIB、CISCO-802-TAP-MIB、および CISCO-USER-CONNECTION-TAP-MIB（加入者単位の傍受がサポートされている場合）が含まれます。
3. 合法的傍受の間に、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が作成され、元のトラフィックはそのまま宛先に転送されるので、ターゲットに気付かれることはありません。
   c. 傍受したトラフィックを UDP パケットにカプセル化し、このパケットをターゲットに知られることなく MD 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処理によって、トラフィック ストリームに検知可能な遅れが生じることはありません。

4. MD は、この傍受したトラフィックを要求された形式に変換し、LEA で稼働している収集機能に送信します。傍受したトラフィックは、ここで格納され、処理が行われます。

（注） 裁判所の命令で許可されていないトラフィックをルータが傍受した場合は、MD により不要なトラフィックがフィルタリングされ、裁判所の命令で許可されたトラフィックのみが LEA に送信されます。

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。

合法的傍受の MIB

合法的傍受を実行するために、ルータは次の MIB を使用します。これらの MIB については、次のセクションで説明します。

- CISCO-TAP2-MIB — 合法的傍受の処理に使用します。
- CISCO-IP-TAP-MIB — レイヤ 3（IPv4）トラフィックの傍受に使用します。
- CISCO-802-TAP-MIB — レイヤ 2 トラフィックの傍受に使用します。
- CISCO-USER-CONNECTION-TAP-MIB — 個々の加入者のトラフィックの傍受に使用します。

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。MD 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、合法的傍受の設定を行って実行します。この MIB は、合法的傍受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 には、ルータ上で実行される合法的傍受の情報を提供するための複数のテーブルが含まれています。

- cTap2MediationTable — 現時点で、ルータ上で合法的傍受を実行している各 MD に関する情報が含まれています。テーブルの各エントリには、ルータが MD 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）が含まれています。
- cTap2StreamTable — 傍受するトラフィックを特定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 ストリームを特定するための、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され、コピーされて、対応する MD 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および傍受対象であっても傍受されなかった廃棄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に関する SNMP 通知も含まれています。MIB オブジェクトの詳細な説明については、MIB を参照してください。

CISCO-TAP2-MIB のプロセス

管理機能（MD 上で実行）により、ルータの CISCO-TAP2-MIB に対し SNMPv3 の **set** および **get** 要求が発行され、合法的傍受が設定および開始されます。具体的には、次の処理が行われます。

1. cTap2MediationTable のエントリを作成し、ルータおよび傍受を実行する MD との通信方法を定義します。

   （注） cTap2MediationNewIndex オブジェクトは、メディエーション テーブル エントリの固有のインデックスです。

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) に設定して、傍受を開始します。ルータは、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、ルータを通過する IPv4 トラフィック ストリームに対して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 の拡張版です。

CISCO-802-TAP-MIB

CISCO-802-TAP-MIB には、ルータを通過する IEEE 802 データ ストリームに対して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。

CISCO-USER-CONNECTION-TAP-MIB

CISCO-USER-CONNECTION-TAP-MIB には、ルータ上の個々のユーザ接続（セッション）に対して通信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 には、ユーザ接続に関する情報が含まれています。各接続は、一意のセッション ID で識別されます。

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。不正ユーザが合法的傍受を実行できないようにしたり、傍受に関連する情報にアクセスできないようにしたりする必要があります。

この章の内容は、次のとおりです。

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。

- ルータには、最高レベルのアクセス権（レベル 15）でログインする必要があります。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、ルータに定義されている最高レベルの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）を使用して、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 Mediation Device（MD; 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、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。

セキュリティに関する考慮事項

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を考慮してください。

- 合法的傍受の SNMP（簡易ネットワーク管理プロトコル）通知は、MD の User Datagram Protocol（UDP; ユーザ データグラム プロトコル）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。手順については、「合法的傍受の SNMP 通知のイネーブル化」（p.2-12）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、ルータ上の合法的傍受について知る必要性のあるシステム管理者と MD に制限する必要があります。これらのユーザには、authPriv または authNoPriv アクセス権限を付与して合法的傍受 MIB にアクセスできるようにする必要があります。NoAuthNoPriv アクセス権を所有するユーザは、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 が除外されています。

  CISCO-TAP2-MIB
  CISCO-IP-TAP-MIB
  CISCO-802-TAP-MIB
  CISCO-USER-CONNECTION-TAP-MIB
  SNMP-COMMUNITY-MIB
  SNMP-USM-MIB
  SNMP-VACM-MIB

その他の考慮事項については、「設定時の注意事項および制限事項」を参照してください。また、「前提条件」（p.2-2）も参照してください。

設定時の注意事項および制限事項

ここからは、合法的傍受に関する一般的な制限事項と設定時の注意事項、Cisco 7600 に固有の注意事項、および加入者単位の注意事項について説明します。

- ルータのパフォーマンスを維持するため、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、これらのうち 8 コールを傍受できます。

（注） リリース 12.2(33)SRC 以上のリリースでは、Route Processor Lawful Interface（RPLI）機能は最大 50 コールをサポートし、Accelerated Lawful Intercept（ALI）機能は最大 500 コールをサポートします。

- CISCO-IP-TAP-MIB は、Virtual Routing and Forwarding（VRF）の OID citapStreamVRF をサポートします。

（注） リリース 12.2(33)SRC 以上のリリースでは、VRF 単位の合法的傍受で citapStreamVRF をサポートします。

- Cisco 7600 ルートでは、「レギュラー」と「ブロードバンド」（加入者単位）の 2 つのタイプの合法的傍受をサポートします。ブロードバンドの通信傍受は、アクセス サブインターフェイス上で実行され、レギュラーの通信傍受は、その他すべてのインターフェイス タイプ上で実行されます。ルータは、ターゲットのトラフィックが使用しているインターフェイスに基づいて、通信傍受のタイプを決定します。

設定時の一般的な注意事項

ルータが MD 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 MD 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、ルータ上の FastEthernet0/0/0 インターフェイスのアドレスです。

- MD には、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。
- MD 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。このグループに追加するユーザの名前には、MD のユーザ名を指定します。

  MD を CISCO-TAP2-MIB のユーザとして追加する場合は、必要に応じて MD の許可パスワードを指定できます。パスワードは 8 文字以上の長さにします。

MIB の注意事項

合法的傍受のプロセスでは、次の Cisco MIB が使用されます。これらの MIB を合法的傍受 MIB の SNMP ビューに含めることで、MD が、ルータを通過するトラフィックに対して通信傍受を設定および実行できるようにする必要があります。

- CISCO-TAP2-MIB ― レギュラーとブロードバンドの両タイプの合法的傍受に必要です。
- CISCO-IP-TAP-MIB ― レイヤ 3（IPv4）ストリームに対する通信傍受に必要です。レギュラーおよびブロードバンドの合法的傍受に対応しています。

- CISCO-802-TAP-MIB ― レイヤ 2 ストリームに対する通信傍受に必要です。インターフェイス タッピング ブロードバンドの合法的傍受のみに対応しています。
- CISCO-IP-TAB-MIB には、次の機能に対する制限があります。
  - Optimized Access Control List（ACL; アクセス コントロール リスト）Logging（OAL）および VLAN Access Control List（VACL）キャプチャは機能しません。
  - IDS は単独でトラフィックをキャプチャすることはできず、合法的傍受により傍受されたトラフィックのみをキャプチャできます。

Cisco 7600 設定時の注意事項および制限事項

次に、Cisco 7600 シリーズ ルータ上のレギュラーの合法的傍受に対する設定時の注意事項のリストを示します。

- これらの注意事項は、すべての非アクセス（加入者）サブインターフェイスに対する合法的傍受のプロセスに適用されます。個々の加入者に対する通信傍受に適用される注意事項のリストについては、「ブロードバンド（加入者単位）設定時の注意事項と制限事項」（p.2-5）を参照してください。VPN トラフィックに対する通信傍受に適用される注意事項については、「VRF 単位の合法的傍受の設定時の注意事項および制限事項」（p.2-6）を参照してください。
- 合法的傍受には、Route Switch Processor 720（RSP720）、Supervisor Engine 720（Sup720）、または Supervisor Engine 32（Sup32）（PFC3A、PFC3B、PFC3BXL、PFC3C、および PFC3CXL をサポート）が必要です。Cisco IOS リリース 12.2SRC 以上のリリースでは、RSP720-10GE もサポートされています。

（注） 合法的傍受では、パケット転送レートに影響を与えずに、トラフィックを 6000 パケット / 秒（pps）のレートで傍受できます。この傍受レートは、すべてのアクティブな傍受数を含み、パケット長が 150 ～ 200 バイト長であることを前提としています。合法的傍受はプロセッサを多用するため、傍受レートが 6000 pps を超えると、パケット転送レートはわずかに減少します。

- 合法的傍受は、IPv4 ユニキャスト トラフィックのみをサポートします。また、傍受対象のトラフィックは、入力と出力の両方のインターフェイスで IPv4 である必要があります。たとえば、合法的傍受は Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）タグに基づいて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。
- 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 VLAN インターフェイスがレイヤ 3 インターフェイスで、トラフィックが VLAN インターフェイスによってルーティングされる場合に、レイヤ 2 インターフェイス上で動作する VLAN 上のトラフィックは傍受できます。
- 合法的傍受は、他のパケットでカプセル化されたパケット（トンネル パケットや Q-in-Q パケットなど）ではサポートされません。
- 合法的傍受は、レイヤ 3 またはレイヤ 4 での書き換えが行われるパケット（Network Address Translation［NAT; ネットワーク アドレス変換］や TCP リフレクシブ）ではサポートされません。
- 入出力方向では、あとになって（レート制限または ACL 拒否ステートメントなどにより）廃棄されるパケットであっても、ルータは最大廃棄パケット レート リミッタ設定（デフォルトは 100 pps）までパケットを傍受および複製します。
- ハードウェアのレート リミットの対象になるパケットは、合法的傍受で次のように処理されます。
  - ― レート リミットにより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 リミッタが通過させたパケットは、傍受および処理されます。

- 複数の Law Enforcement Agency（LEA; 法執行機関）が 1 つの MD を使用し、それぞれが同じターゲットに対する通信傍受を実行している場合、ルータは 1 つのパケットを MD に送信します。各 LEA にパケットを複製するのは MD の役割です。
- Cisco 7600 ルート上の合法的傍受は、次の 1 つまたは複数のフィールドの組み合わせに一致する値を持つ IPv4 パケットを傍受できます。
  - 宛先 IP アドレスおよびマスク
  - 宛先ポート範囲
  - 発信元 IP アドレスおよびマスク
  - 発信元ポート範囲
  - プロトコル ID
  - インターフェイス インデックス（プロビジョニングの際に、インデックスを選択して合法的傍受をオンにするためのみに使用。合法的傍受タップのターゲットの特定には使用されません）

ブロードバンド（加入者単位）設定時の注意事項と制限事項

ブロードバンドの合法的傍受では、個々の加入者に対する通信傍受をサポートします。次に、合法的傍受を設定して、個々の加入者の通信傍受をサポートするための注意事項を示します。

- ハードウェアおよびソフトウェア要件
  - Cisco IOS リリース 12.2SRB 以上
  - アクセス サブインターフェイスとして設定された個々の加入者をサポートする、ギガビット イーサネット（GE）Shared Port Adapter（SPA; 共有ポート アダプタ）搭載の Cisco 7600 SIP-400。合法的傍受は、2 ポートおよび 5 ポート GE SPA の任意の組み合わせを使用した、最大 10 の GE ポート上でサポートされます。

（注） また、アクセス サブインターフェイスとして設定されていない Cisco 7600 SIP-400 GE インターフェイス上でも、合法的傍受を実行できます。

- 加入者単位の通信傍受は、IPv4 および IEEE 802 の両方のストリームでサポートされます。両方のタイプのストリームに対応するには、合法的傍受 MIB ビューに CISCO-IP-TAP-MIB と CISCO-802-TAP-MIB を追加する必要があります。
- ルータのパケット転送レートに影響を与えることなく、最大 20 の傍受を一度に実行できます。また、最大 200 の傍受を同時に設定できますが、これらはディセーブル ステートになります。傍受レートがこのレートを超えると、合法的傍受はプロセッサを多用するため、パケット転送レートがわずかに減少します。
- 合法的傍受のプロセスは、出力方向でセキュリティ ACL と QoS（Quality Of Service）機能が加入者のトラフィックに適用されたあとで実行されます。したがって、合法的傍受は、これらの機能で廃棄されたトラフィックの複製は行いません。入力方向では、合法的傍受はセキュリティ ACL と QoS 機能が適用される前に実行されます。
- SSO と NonStop Fowarding（NFS）は、通信傍受ではサポートされません。アクティブおよびスタンバイ スーパーバイザ エンジン間でスイッチオーバーが発生すると、アクティブな通信傍受に関する情報は削除されます。
- 加入者通信傍受の統計情報は、Cisco 7600 SIP-400 により保持されます。
- 活性挿抜（online insertion and removal; OIR）の後、すべての通信傍受のカウンタがクリアされます。

VRF 単位の合法的傍受の設定時の注意事項および制限事項

VRF 単位の合法的傍受とは、特定の VPN の IPv4 データに対して合法的傍受の通信傍受をプロビジョニングすることです。これにより、LEA は特定の VPN 内のターゲット データを合法的に傍受できます。特定の VPN 内の IPv4 データだけが、VRF ベースの LI タップの対象になります。

（注） VRF 単位の合法的傍受は、Cisco IOS リリース 12.2SRC 以上のリリースで利用できます。

VRF 単位の LI は、次のタイプのトラフィックで利用できます。

- ip2ip
- ip2tag（IP から MPLS）
- tag2ip（MPLS から IP）

（注） MPLS は、リリース 12.2(33)SRC 以上のリリースでのみサポートされます。

VPN ベースの IPv4 タップをプロビジョニングするため、LI 管理機能（MD 上で実行）は CISCO-IP-TAP-MIB を使用して、ターゲット VPN が使用する VRF テーブルの名前を特定します。VRF 名は、タップを実行するために LI をイネーブルにする VPN インターフェイスを選択する際に使用されます。

ルータは、送信元および宛先のアドレス、送信元および宛先のポート、およびプロトコルのほか、VRF 名に基づいて傍受するトラフィックおよび傍受されたパケットを送信する MD を決定します。

（注） Cisco-IP-TAP-MIB を使用する場合、VRF 名がストリーム エントリに指定されていないと、デフォルトでグローバル IP ルーティング テーブルが使用されます。

要件および制限事項

通常の合法的傍受に適用される制限および制約事項は、VRF 単位の LI にも同様に適用されます。さらに、次の要件と制限事項が VRF 単位の LI に適用されます。

- 合法的傍受は、最大 1000 の VRF またはインターフェイスをサポートします。
- VPN ベースのタップに使用する VRF を判別するために、ルータは ACL Ternary Content Addressable Memory（TCAM）を使用して再循環を実行します。再循環を適用させるためには、次のハードウェア リソースが必要です。
  - 各 VRF に 2 つの内部 VLAN（1 つは入力トラフィック用、1 つは出力トラフィック用）
  - 隣接結果が LI の結果に競合する可能性がある入力機能がインターフェイスにある場合、VPN ベースのタップが実行されている各インターフェイスで内部 VLAN が必要になります。ACL TCAM 再循環を使用する機能のリストについては、次のセクションを参照してください。

（注） 上記の内部 VLAN は各ルータで利用できる内部 VLAN の合計（4096）から取得されます。これは、ルータが一度に実行できる VPN ベースの LI タップの数を制限します。

- VPN に所属するインターフェイスが VRF 単位の LI に設定されている場合、Policy-Based Routing（PBR; ポリシー ベース ルーティング）、または隣接結果を使用する入力 Web Cache Communication Protocol（WCCP）ACL TCAM エントリは LI 再循環の隣接に設定されます。隣接結果が書き換えられる間、トラフィック フローが一時的に中断する可能性があります。
- 再循環によって、VPN ベースの LI タップがルータによって廃棄されるトラフィックを傍受することになる場合もあります。
- VPN ベースのタップが同じ VPN に所属する入出力インターフェイスのペアで実行される場合、インターフェイスを通過する IP-to-IP トラフィックが 2 回傍受されます。これにより、MD に重複パケットが送信されます。

他の機能との相互作用

VRF 単位の LI はリダイレクション隣接結果を使用して入力 ACL 結果を判別するため、隣接結果を同様に使用する他の機能と競合する可能性があります。次の IP ACL 機能が現在、再循環隣接結果を使用しています。

- DHCP スヌーピング
- IP 再循環
- PBR
- Reverse Path Forwarding（RPF）
- Server Load Balancing（SLB）
- WCCP

合法的傍受サービス モジュールとしての Cisco 7600 SIP-400 の使用

Cisco 7600 SIP-400 は、Cisco 7600 シリーズ ルータのルート プロセッサで実行される同じ LI 機能を実装するのに使用できます。シャーシに SIP-400 が搭載されていると、パケットの傍受プロセスがルート プロセッサから SIP-400 にオフロードされ、ルート プロセッサが LI パケットを検索しなくなります。

この機能は、LI プロセスに使用できる SIP-400 モジュールのリストを指定することによって実装されます。合法的傍受が開始すると、リストの最初の SIP-400 が使用されます。現在アクティブのモジュールが非アクティブになると、使用する新しいアクティブ モジュールを検索するために、リストが再スキャンされます。アクティブな SIP-400 モジュールが存在しないと、ルート プロセッサが LI 機能を引き継ぎます。リストに表示された SIP-400 が再度アクティブになると、LI 機能が自動的に SIP-400 に戻ります。

設定時の注意事項および制約事項

次に、Cisco 7600 SIP-400 を合法的傍受装置として使用する場合に関連する注意事項と制限事項を示します。

- LI をイネーブルにするためのルータ プロビジョニングは、従来通り SNMPv3 を通じて行われています。
- SIP-400 は、インターフェイスがインストールされている場合とインストールされていない場合があります。
  - インターフェイスが SIP-400 にインストールされている場合、LI 機能によって生成された他のトラフィックが、SIP-400 を流れるトラフィックに影響する可能性があります。
  - インターフェイスがインストールされていない場合、SIP-400 は LI サービス モジュールとしてのみ動作します。
  - シャーシに 2 つ以上の SIP-400 が搭載されている場合、サービス モジュールとして設定できるのは 1 つの SIP-400 だけです。
- SIP-400 の活性挿抜の実行中に、SIP-400 がシャーシに再度取り付けられるまでルート プロセッサが LI トラフィックを処理します。
- 傍受されたパケットは、ハイ プライオリティ パケットとして扱われます。
- SIP-400 は、最大 500 タップをサポートします。
- SIP-400 はコンテンツ配信プロトコルとしてのみ UDP をサポートします。
- ルーテッド パケット（IPv4 ユニキャストおよびマルチキャスト トラフィック）のみがサポートされています。IPv6 パケットの傍受は、サポートされていません。
- VLAN ベースの傍受は、サポートされていません。

SIP-400 の選択

合法的傍受モジュールとして使用する SIP-400 のリストを選択するには、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実行します。

	コマンド	目的
ステップ 1	`Router# 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 2	`Router(config)# li-slot slot-list` *slot1, slot2, ...* **rate** *value*	LI 装置として使用する SIP-400 モジュールの場所を選択します。 **rate** *value* の有効な範囲は、1000 ～ 1000000 pps です。
ステップ 3	`Router(config)# show li slot`	使用するすべての SIP-400 モジュールの場所を確認します。

合法的傍受 MIB へのアクセス

機密情報の扱いに関わることから、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 イメージの形でのみ提供されています。これらの MIB 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、MD および合法的傍受について知る必要性のあるユーザのみに許可されます。これらの MIB へのアクセスを制限するには、次の作業を行います。

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書きアクセス権限を持つ 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のみが 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連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、必ず MD を追加してください。これを行わないと、ルータ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、ルータ上の合法的傍受について知る必要性のあるシステム管理者と MD に制限する必要があります。MIB にアクセスするには、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、ルータに SNMPv3 が設定されている必要があります。SNMPv3 の設定方法および以降のセクションで説明するコマンドの詳細情報については、次のシスコの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」。次の URL から入手できます。
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf014.htm
- 『*Cisco IOS Configuration Fundamentals and Network Management Command Reference*』。次の URL から入手できます。
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/fun_r/cfr_1g11.htm

合法的傍受 MIB を含む、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 ビューを作成して、ユーザを割り当てるには、CLI のグローバル コンフィギュレーション モードでレベル 15 のアクセス権限を使って、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.2-11）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のみが示されています。コマンド構文の詳細については、前のセクション（「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　ルータに 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.2-9）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、レギュラー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 と 802 ストリームに対する通信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）。

```
Router(config)# snmp-server view view_name ciscoIpTapMIB included
Router(config)# snmp-server view view_name ciscoTap802MIB included
```

ステップ 4　（任意）個々の加入者に対する通信傍受のサポートを設定するには、次の MIB を SNMP ビューに追加します。

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

ステップ 5　合法的傍受 MIB にアクセスできる SNMP ユーザ グループ（*groupname*）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 6　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、および *auth_password* は認証パスワード）。

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

（注） この SNMP ユーザ グループに、必ず MD を追加してください。これを行わないと、ルータで合法的傍受を実行できません。シスコの合法的傍受 MIB ビューへのアクセスは、ルータ上の合法的傍受について知る必要性のあるシステム管理者と MD に制限する必要があります。

これで MD は合法的傍受 MIB にアクセスして、SNMP **set** および **get** 要求を発行し、ルータ上に合法的傍受を設定および実行することができるようになります。

SNMP 通知を MD に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.2-12）を参照してください。

設定例

次に、MD が合法的傍受 MIB をアクセスできるように設定する例を示します。

```
Router(config)# snmp-server view tapV ciscoTap2MIB included
Router(config)# snmp-server view tapV ciscoIpTapMIB included
Router(config)# snmp-server view tapV ciscoTap802MIB included
Router(config)# snmp-server view tapV ciscoTapConnectionMIB 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 1234
```

1. 適切な合法的傍受 MIB（CISCO-TAP2-MIB、CISCO-IP-TAP-MIB、CISCO-802-TAP-MIB、および CISCO-USER-CONNECTION-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、および通知のアクセス権限を持つユーザ グループ（tagGrp）を作成します。
3. このユーザ グループに MD（ss8user1）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（123400000000000000000000 など）。指定しない場合は、エンジン ID が自動的に生成されます。上記の例の最後の行にあるように、エンジン ID の後続のゼロは省略できます。

（注） 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 ストリングにも影響します。

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 2-1 を参照）。これは、cTap2MediationNotificationEnable オブジェクトが、デフォルトで true(1) に設定されているためです。

合法的傍受通知を MD に送信するようにルータを設定するには、グローバル コンフィギュレーション モードでレベル 15 のアクセス権限を使って、次の CLI コマンドを発行します（*MD-ip-address* は MD の IP アドレス。*community-string* は通知要求と一緒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）。

```
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、**upd-port** は 162（SNMP のデフォルト）ではなく、161 に設定します。
- 2 番めのコマンドでは、ルータが RFC 1157 規定の通知を MD に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知らせます。

表 2-1 に、合法的傍受イベントで生成される SNMP 通知を示します。

表 2-1　合法的傍受イベントの 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（cTap2MediationTimeout の時間切れなど）。
cTap2MediationDebug	cTap2MediationTable エントリに関するイベントには、対処が必要です。
cTap2StreamDebug	cTap2StreamTable エントリに関するイベントには、対処が必要です。

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) に戻します。

INDEX