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。