CHAPTER 2

LI 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 LI を実行したり、傍受に関連する情報にアクセスしたりできないように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

LI 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。

- Secure Shell（SSH; セキュア シェル）をサポートするイメージを実行していること。たとえば、イメージ s72033-adventerprisek9-mz です。SSH をサポートしないイメージでは LI はサポートされません。
- Catalyst 6500 シリーズ スイッチには、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、Catalyst 6500 シリーズ スイッチ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。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で、LI をグローバルに設定できます。
- Supervisor Engine 720 または Supervisor Engine 720-10GE（PFC3A、PFC3B、PFC3BXL、PFC3C、PFC3CXL をサポート）を搭載した Catalyst 6500 シリーズで、LI はサポートされます。
- Catalyst 6500 シリーズ スイッチと Mediation Device（MD; メディエーション デバイス）の時刻が同期されていること。Catalyst 6500 シリーズ スイッチと MD の両方で Network Time Protocol（NTP）を使用することを推奨します。
- （任意）Catalyst 6500 シリーズ スイッチが MD 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。ループバック インターフェイスを使用しない場合は、Catalyst 6500 シリーズ スイッチの複数の物理インターフェイスを使用して MD を設定し、ネットワーク障害に対処する必要があります。

セキュリティに関する考慮事項

Catalyst 6500 シリーズ スイッチに LI 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。

- LI の SNMP 通知は、MD 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。手順については、「LI の SNMP 通知のイネーブル化」（p.2-8）を参照してください。
- LI MIB にアクセスできるユーザは、Catalyst 6500 シリーズ スイッチ上の LI 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 LI 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、LI MIB にアクセスできません。
- SNMP-VACM-MIB を使用して、LI 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
  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約事項」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約事項

これ以降では、LI に関する一般的な制約事項と設定時の注意事項、Catalyst 6500 シリーズ スイッチに固有の注意事項、および加入者単位の注意事項について説明します。

- ネットワーク管理者が LI を配置するノードに、Optimized ACL Logging（OAL）、VLAN Access Control List（ACL; アクセス コントロール リスト）キャプチャ、Intrusion Detection System（IDS; 侵入検知システム）を設定することはできません。ノードに LI を配置すると、OAL、VACL キャプチャ、IDS の動作が予測不能になります。
- Catalyst 6500 シリーズ スイッチのパフォーマンスを維持するため、LI はアクティブ コールの 0.2% 以下に制限されています。たとえば、Catalyst 6500 シリーズ スイッチが 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。
- CISCO-IP-TAP-MIB は、Virtual Routing and Forwarding（VRF）の OID citapStreamVRF をサポートしていません。
- キャプチャされたトラフィックの速度は、ルート プロセッサの CPU 使用状況を保護するために 8,500 pps に制限されます。
- プロビジョニング時にはインターフェイス インデックスが使用され、LI を有効にするインデックスだけが選択されます。0 に設定するとすべてのインターフェイスで LI が有効になります。

設定時の一般的な注意事項

Catalyst 6500 シリーズ スイッチが MD と通信して LI を実行するには、次の設定要件を満たす必要があります。

- （任意）Catalyst 6500 シリーズ スイッチと 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）に登録できます。

  DNS では、Catalyst 6500 シリーズ スイッチの IP アドレスは通常、Catalyst 6500 シリーズ スイッチ上の FastEthernet0/0/0 インターフェイスのアドレスです。
- MD には Access Function（AF）が必要です。
- CISCO-TAP2-MIB ビューにアクセスできる SNMP（簡易ネットワーク管理プロトコル）ユーザ グループに MD を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。

  CISCO-TAP2-MIB のユーザとして MD を追加する場合は、MD の許可パスワードを指定する必要があります。パスワードは 8 文字以上の長さにします。

MIB の注意事項

LI のプロセスでは、次の Cisco MIB が使用されます。これらの MIB を LI MIB の SNMP ビューに含めることで、MD が、Catalyst 6500 シリーズ スイッチ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 LI 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 LI 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。
  - 次の 1 つまたはすべての機能が設定され正しく動作しており LI がイネーブルの場合、LI が優先され、機能は次のように動作します。

    ・OAL — 機能しません。

    ・VACL キャプチャ — 正しく機能しません。

    ・IDS — 正しく機能しません。

    機能を有効にするには、LI を無効にするか設定解除します。

－ 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、LI 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。

設定時の注意事項および制約事項

次に、Catalyst 6500 シリーズ スイッチの LI 設定時の注意事項を示します。この注意事項は、すべての非アクセス（加入者）サブインターフェイス上での LI のプロセスに適用されます。

- Supervisor Engine 720 または Supervisor Engine 720-10GE（PFC3A、PFC3B、PFC3BXL、PFC3C、PFC3CXL をサポート）が必要です。

（注） 1 つのインターフェイスを LI のプロセス専用にすることを推奨します。たとえば、そのインターフェイスでプロセッサを集中的に使用するタスク（QoS やルーティングなど）を実行しないように設定します。

- 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、出力側が MPLS で、入力側が IPv4 の場合は、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 インターフェイス上ではサポートされません。ただし、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。
- 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）はサポートされません。
- Q-in-Q パケットはサポートされません。LI ではレイヤ 2 傍受はサポートされません。
- 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）はサポートされません。
- 入力方向では、（レート制限または ACL **deny** ステートメントなどにより）あとになって廃棄されるパケットであっても、Catalyst 6500 シリーズ スイッチはパケットを傍受し複製します。出力方向では、パケットが（ACL などにより）廃棄されると複製されません。
- LI ACL は、インターエイス内部で入力と出力の両方向に適用されます。
- 特定のユーザからのトラフィックを傍受するには、通常それぞれの方向のフローが設定されます。
- 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、LI 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 LEA 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、Catalyst 6500 シリーズ スイッチは 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。
- Catalyst 6500 シリーズ スイッチ上の LI 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

LI 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 LI MIB は、LI 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。

LI MIB へのアクセスの制限

LI MIB へのアクセスは、MD および LI 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 LI 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 LI ユーザ グループにユーザを追加して、MIB および LI 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、Catalyst 6500 シリーズ スイッチで LI を実行できません。

（注）　シスコの LI MIB ビューへのアクセスは、Catalyst 6500 シリーズ スイッチ上の LI 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、Catalyst 6500 シリーズ スイッチ上でレベル 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、Catalyst 6500 シリーズ スイッチに 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

LI MIB を含む、制限付き SNMP ビューの作成

シスコの LI 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用して、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.2-7）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　Catalyst 6500 シリーズ スイッチに 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.2-6）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 LI に必要です。

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

ステップ 3　SNMP ビューに次の MIB の 1 つまたは両方を追加して、IPv4 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
```

ステップ 4　LI 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、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 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、Catalyst 6500 シリーズ スイッチで LI を実行できません。LI MIB ビューへのアクセスは、Catalyst 6500 シリーズ スイッチ上の LI 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 LI MIB にアクセスして、SNMP **set** および **get** 要求を発行し、Catalyst 6500 シリーズ スイッチ上で LI を設定および実行することができるようになります。

MD に SNMP 通知を送信するための Catalyst 6500 シリーズ スイッチの設定方法については、「LI の SNMP 通知のイネーブル化」（p.2-8）を参照してください。

設定例

次に、MD が LI MIB に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 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. 該当する LI 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、および通知のアクセス権限を持つユーザ グループ（tapGrp）を作成します。
3. このユーザ グループに MD（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）Catalyst 6500 シリーズ スイッチに管理用の 24 文字の SNMP エンジン ID（123400000000000000000000 など）を割り当てます。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。

LI の SNMP 通知のイネーブル化

SNMP は、LI 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。

MD に LI 通知を送信するように Catalyst 6500 シリーズ 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
```

- LI 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、Catalyst 6500 シリーズ スイッチが 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）、およびシステムの再起動を知らせます。

表 2-1 に、LI イベントで生成される SNMP 通知を示します。

表 2-1　LI イベントの SNMP 通知

通知	意味
cTap2MIBActive	Catalyst 6500 シリーズ 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	LI 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

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。

LI 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。LI 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。