合法的傍受アーキテクチャ

合法的傍受（LI）機能は、法執行機関（LEA）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。サーベイランスは、エッジ ルータを通過する Voice over Internet Protocol（VoIP）またはデータ トラフィックを傍受するため、盗聴を利用して実行されます。LEA は、ターゲットのサービス プロバイダーに盗聴を要求します。サービス プロバイダーには、IP セッションを使用してその個人が送受信するデータ通信を傍受する責任があります。

このマニュアルでは、Cisco Service Independent Intercept アーキテクチャと PacketCable Lawful Intercept アーキテクチャを含む、LI アーキテクチャについて説明します。また、LI 機能の構成要素と、システムで LI 機能を設定するための手順についても説明します。

Cisco IOS XE リリース 2.5 以前は、PPP セッションはアカウンティング セッションに基づいてタップされました。回線 ID ベースのタッピングは、Cisco IOS XE リリース 2.5 で導入されました。

Cisco IOS XE リリース 2.6 では、ユーザ セッションはイーサネット（PPPoE）回線 ID タグを介する独自の PPP に基づいてタップされます。この回線 ID タグは、デバイスの PPPoE ユーザ セッションの固有のパラメータとして機能します。タップされたユーザ セッションは SNMP を使ってプロビジョニングされ、ユーザ セッションのデータ パケットおよび RADIUS 認証のデータ パケットはタップされます。

合法的傍受の前提条件

Cisco LI 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知っておく必要があるシステム管理者に制限されます。MIB にアクセスするには、ルータ上でレベル 15 のアクセス権がユーザに必要です。

メディエーション デバイスとの通信

ルータが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、次の構成要件が満たされている必要があります。

- 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、ドメイン ネーム システム（DNS）に登録されている必要があります。

DNS で、ルータの IP アドレスは、通常はルータ上の 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シンプル ネットワーク管理プロトコル（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認可パスワードを指定できます。パスワードの長さは、最低 8 文字である必要があります。

合法的傍受の制約事項

一般的な制約事項

ルータで LI を設定するためのコマンドライン インターフェイス（CLI）はありません。すべてのエラー メッセージは、メディエーション デバイスに SNMP 通知として送信されます。すべての傍受は、SNMPv3 だけを使用してプロビジョニングされます。

合法的傍受では SUP HA がサポートされません。SUP スイッチオーバーの後に LI 設定を再適用する必要があります。このイベント用に SNMP トラップが生成されます。

合法的傍受 MIB

合法的傍受について知る必要があるメディエーション デバイスとユーザだけに LI MIB へのアクセスが許可されます。

Cisco LI MIB は、その機密性から、LI 機能をサポートしているソフトウェア イメージだけで使用できます。これらの MIB には、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。

SNMP 通知

LI の SNMP 通知は、メディエーション デバイス上のユーザ データグラム プロトコル（UDP）ポート 161 に送信する必要があります。ポート 162（SNMP のデフォルト）ではありません。

合法的傍受に関する情報

合法的傍受の概要

LI は、司法当局（LEA）が、司法命令または行政命令の許可に従って、電子的監視を行うためのプロセスです。ますます多くの法律が採択され、規制が施行されるのに伴い、サービス プロバイダー（SP）やインターネット サービス プロバイダー（ISP）は、許可された電子監視を明示的にサポートするネットワークを実装する必要性に迫られています。LI の指令に従う必要がある SP または ISP の種類は、国によって大きく異なります。米国での LI への準拠は、Commission on Accreditation for Law Enforcement Agencies（CALEA）で規定されています。

シスコでは、LI に対し、PacketCable と Service Independent Intercept の 2 つのアーキテクチャをサポートしています。LI コンポーネントだけでは、該当する規制に準拠できません。LI コンポーネントは、SP および ISP が、LI 準拠のネットワークを構築するために使用可能なツールを提供します。

Cisco Service Independent Intercept アーキテクチャ

『Cisco Service Independent Intercept Architecture Version 3.0』では、Cisco BTS 10200 Softswitch コール エージェント バージョン 5.0 を非 PacketCable ネットワークで使用した、VoIP ネットワーク向けの LI の実装について説明しています。Packet Cable Event Message 仕様バージョン 1.5-I01 は、コール識別情報と、コールの内容に対する Cisco Tap MIB バージョン 2.0 を提供するために使用されます。

『Cisco Service Independent Intercept Architecture Version 2.0』では、Cisco BTS 10200 Softswitch コール エージェント バージョン 4.4 および 4.5 を非 PacketCable ネットワークで使用した、VoIP ネットワーク向けの LI の実装について説明しています。PacketCable ネットワークではありませんが、PacketCable Event Messages Specification バージョン I08 は、コール識別情報と、コール内容に対する Cisco Tap MIB のバージョン 1.0 またはバージョン 2.0 を提供するために引き続き使用されています。『*Cisco Service Independent Intercept Architecture Version 2.0*』では、IP アドレスとセッション ID の両方でデータを傍受するための追加機能について説明しています。これは、どちらも Cisco Tap MIB（CISCO-TAP2-MIB）のバージョン 2.0 でサポートされています。

『Cisco Service Independent Intercept Architecture Version 1.0』では、Cisco BTS 10200 Softswitch コール エージェント バージョン 3.5 および 4.1 を非 PacketCable ネットワークで使用した、VoIP

ネットワーク向けの LI の実装について説明しています。PacketCable ネットワークではありませんが、PacketCable Event Message Specification バージョン I03 は、コール識別情報と、コール内容に対する Cisco Tap MIB（CISCO-TAP-MIB）のバージョン 1.0 を提供するために引き続き使用されています。IP アドレスによる単純なデータの傍受についても説明されています。

PacketCable 合法的傍受アーキテクチャ

『*PacketCable Lawful Intercept Architecture for BTS Version 5.0*』では、PacketCable Event Messages Specification バージョン 1.5-I01 に準拠した PacketCable ネットワークで、Cisco BTS 10200 Softswitch コール エージェント バージョン 5.0 を使用した、VoIP 向けの LI の実装について説明しています。

『*PacketCable Lawful Intercept Architecture for BTS Versions 4.4 and 4.5*』では、Cisco BTS 10200 Softswitch コール エージェント バージョン 4.4 および 4.5 を、PacketCable Event Messages Specification バージョン I08 に準拠した PacketCable ネットワークで使用した、VoIP 向けの LI の実装について説明しています。

『 PacketCable Lawful Intercept Architecture for BTS Versions 3.5 and 4.1 』では、Cisco Broadband Telephony Softswitch (BTS) 10200 Softswitch コール エージェント バージョン 3.5 および 4.1 を、PacketCable Event Message Specification バージョン I03 に準拠した PacketCable ネットワークで使用した、Voice over IP（VoIP）向けの LI の実装について説明しています。

『*PacketCable Control Point Discovery Interface Specification* 』では、指定された IP アドレスのコントロールポイントを発見するために使用可能な IP ベースのプロトコルが定義されています。コントロール ポイントとは、Quality of Service（QoS）操作、LI コンテンツ タッピング操作、その他の操作を実行可能な場所です。

CISCO ASR 1000 シリーズ ルータ

Cisco ASR 1000 シリーズ アグリゲーション サービス ルータは、通常および広帯域（加入者ごと）の 2 種類の LI をサポートしています。広帯域の盗聴は、アクセス サブインターフェイスおよびトンネル インターフェイス上で実行します。通常の盗聴は、アクセス サブインターフェイス、トンネル インターフェイス、および物理インターフェイス上で実行します。内部インターフェイス上では盗聴は不要であり、実行されません。ルータは、ターゲット 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、実行する盗聴の種類を決定します。

Cisco ASR 1000 シリーズ ルータ上の LI は、次の 1 つ以上のフィールドの組み合わせに基づいてトラフィックを傍受できます。

- 宛先 IP アドレスとマスク（IPv4 または IPv6 アドレス）
- 宛先ポートまたは宛先ポートの範囲
- 送信元 IP アドレスとマスク（IPv4 または IPv6 アドレス）
- 送信元ポートまたは送信元ポート範囲
- プロトコル ID

- Type of Service（TOS）
- ルータ内で *vrf-tableid* 値に変換される Virtual Routing and Forwarding（VRF）名
- 加入者（ユーザ）接続 ID

Cisco ASR 1000 シリーズ ルータ上の LI の実装は、SNMP3 を使用してプロビジョニングされ、次の機能がサポートされています。

- RADIUS セッションは傍受し、次のいずれかの方法で実行できます。
  - アクセス許可パケットを介した傍受では、セッションの開始時に傍受が開始されるようにできます。
  - CoA 要求パケットによる傍受では、ルータがセッション中に傍受を開始または停止することができます。
- 通信内容の傍受。ルータは、傍受した各パケットを複製し、パケットのコピーを UDP ヘッダーでカプセル化されたパケットに（設定された CCCid とともに）格納します。ルータは、カプセル化したパケットを LI メディエーション デバイスに送信します。複数の合法的傍受が同じデータ フローに対して設定されている場合でも、パケットの 1 つのコピーだけメディエーション デバイスに送信されます。必要に応じて、メディエーション デバイスは各 LEA に対しパケットを複製できます。
- IPv4、IPv4 マルチキャスト、IPv6、および IPv6 マルチキャストフローの傍受。

VRF 対応 LI

VRF 対応 LI は、特定のバーチャル プライベート ネットワーク（VPN）での IPv4 データの LI 盗聴をプロビジョニングする機能です。この機能により、LEA は、その VPN 内のターゲット データを合法的に傍受できます。VRF ベースの LI タップを受けるのは、その VPN 内の IPv4 データのみです。

VRF 対応の LI は、次の種類のトラフィックに対して使用できます。

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

VPN ベースの IPv4 タップをプロビジョニングするために、LI 管理機能（メディエーション デバイスで動作します）は、CISCO-IP-TAP-MIB を使用して、ターゲットの VPN が使用している 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のに使用します。

ルータは、傍受するトラフィックと、傍受したパケットを送信するメディエーションデバイスを、VRF 名（および送信元および宛先アドレス、送信元および宛先ポート、およびプロトコル）に基づいて決定します。

（注） Cisco-IP-TAP-MIB を使用する場合、VRF 名がストリーム エントリで指定されていない場合、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。

合法的傍受 MIB

Cisco LI MIB は、その機密性から、LI 機能をサポートしているソフトウェア イメージだけで使用できます。これらの MIB には、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

合法的傍受について知る必要があるメディエーション デバイスとユーザだけに LI MIB へのアクセスを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. Cisco LI 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. ユーザをシスコ LI ユーザ グループに追加し、合法的傍受に関連する MIB および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。

詳細は、「合法的傍受 MIB の制限付き SNMP ビューの作成」を参照してください。

（注） Cisco LI 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知っておく必要があるシステム管理者に制限されます。MIB にアクセスするには、ルータ上でレベル 15 のアクセス権がユーザに必要です。

RADIUS ベースの合法的傍受

RADIUS ベースの合法的傍受ソリューションを使用すると、傍受要求は RADIUS サーバからネットワーク アクセス サーバ（NAS ）またはレイヤ 2 トンネル プロトコル アクセス コンセントレータ（LAC）に（アクセス許可パケットまたは認可変更（CoA）要求パケットを介して）送信されるようになります。PPP または L2TP セッションとやり取りされるすべてのトラフィック データは、仲介デバイスに渡されます。RADIUS ベースの合法的傍受のもう 1 つの利点は、ソリューションの同期です。すべてのターゲット トラフィックを傍受するように、タップはアクセス許可パケットで設定されます。

傍受要求は、SNMPv3 メッセージによって仲介デバイスで開始されるため、特定の IP アドレスから送受信されるすべてのトラフィック データは仲介デバイスに渡されます。IP アドレスに基づいた傍受は、IPアドレスがセッションに割り当てられるまでセッションがタップされるのを防ぎます。

RADIUSベースの合法的傍受機能は、次のモードの合法的傍受にハイ アベイラビリティ（HA）サポートを提供します。

- 新しいセッションのアクセス許可ベースの LI
- 既存のセッションの CoA ベースの LI

RADIUSベースのLI HAは、RADIUSベースのプロビジョニングのみをサポートします。SNMPベースのプロビジョニングはサポートされません。

傍受の動作

傍受要求がアクセス許可パケット内で動作するしくみ

傍受ターゲットが接続の確立を開始するとき、アクセス要求パケットはRADIUSサーバに送信されます。RADIUS サーバは、4 つの RADIUS 属性を含むアクセス許可パケットで応答します。

NAS または LAC は値 1 の LI-Action 属性を受け取り、新しいセッションの開始時に NAS または LAC でトラフィック データを複製できるようにします。また、属性、MD IP アドレス、およびMDポート番号を通して指定された仲介デバイスに複製されたデータを転送できるようにします。

（注） NASまたはLACが新しいセッションのトラフィック データの傍受を開始することができなければ、セッションは確立されません。

アカウンティングが（**aaa accounting network** コマンドおよび **aaa accounting send stop-record authentication failure** コマンドを介して）イネーブル化されると、アカウンティング停止パケットは、Acct-Termination-Cause 属性（49）が 15 に設定されて送信される必要があります。つまり、サービスは利用できないということです。

傍受要求が CoA 要求パケット内で動作するしくみ

セッションが傍受ターゲットに対して確立された後、次のタスクに CoA 要求パケットを使用できます。

- 既存のセッションの傍受の開始。LI-Action の属性は 1 に設定されます。
- 既存のセッションの傍受の停止。LI-Action の属性は 0 に設定されます。
- ダミーの傍受要求の発行。LI-Action の属性は 2 に設定されます。NAS または LAC は、どのセッションの傍受も実行することはできません。代わりに、CoA要求パケットで指定されている Acct-Session-Id 属性値に基づいてセッションを検索します。セッションが存在す

ると、NASまたはLACはRADIUSサーバへCoAの確認応答（ACK）を送信します。セッションがなければ、NASまたはLACは「セッションが見つかりません」のエラー メッセージを発行します。

各ケースでRADIUSサーバは、特定の属性とAcct-Session-Id属性のCoA要求パケットを送信する必要があります。これらの属性はそれぞれ、パケットである必要があります。

Acct-Session-Id属性は傍受されるセッションを識別します。Acct-Session-Id属性は、アクセス要求パケットまたはアカウンティング停止パケットから取得できます。

セッションがタップされセッションが終了すると、タップが停止します。アクセス許可が開始タップを示すか、CoA要求がセッションを開始するように送信されることを示さない限り、加入者のログが戻るときにセッションは開始されません。

（注） CoA要求パケットの頻度は、10分ごとに1つの要求のレートを超えることはありません。

Service Independent Intercept（SII）

シスコでは、サービスプロバイダーカスタマーの合法的傍受のサポート要件に対応するため、Service Independent Intercept（SII）アーキテクチャを開発しました。SIIアーキテクチャは、コンテンツの傍受アクセスポイント（IAP）として機能するシスコ機器とメディエーションデバイス間に、明確に定義されたオープン インターフェイスを提供します。SIIアーキテクチャのモジュラ特性により、サービスプロバイダーは、特定のネットワーク要件と警察当局の収集機能へのインターフェイスに対する地域的な標準ベースの要件とを満たす最適なメディエーション デバイスを選択できます。

メディエーションデバイスはSNMPv3を使用してコール接続（CC）IAPを指示し、CCを複製してメディエーション デバイスにコンテンツを送信します。CC IAPは、エッジルータまたは音声のトランキング ゲートウェイのいずれか、およびエッジ ルータまたはデータのアクセスサーバのいずれかにできます。

セキュリティを強化し、SNMPv3脆弱性を緩和するには、次のタスクが必要です。

信頼できるホストへのアクセス制限（暗号化なし）

SNMPv3は、セキュリティ モデルとセキュリティ レベルの両方をサポートします。セキュリティモデルは、ユーザおよびユーザに属するグループに合わせて設定される認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせによって、SNMPパケットを処理するときに適用されるセキュリティ メカニズムが決定されます。

さらに、名前付きアクセス リストのSNMPサポート機能により、いくつかのSNMPコマンドに、標準の名前付きアクセス コントロール リスト（ACL）へのサポートが追加されます。

新しいSNMPグループ、またはSNMPユーザーをSNMPビューにマップするテーブルを設定するには、グローバル コンフィギュレーション モードで**snmp-server group**コマンドを使用します。

```
access-list my-list permit ip host 10.10.10.1
snmp-server group my-group v3 auth access my-list
```

この例では、**my-list** という名前のアクセス リストは 10.10.10.1 以降の SNMP トラフィックのみ許可します。次にこのアクセス リストは、**my-group** という名前の SNMP グループに適用されます。

合法的傍受をするトラフィックの暗号化および信頼できるホストへのアクセス制限

ルータ（コンテンツインターセプトアクセスポイント（IAP））と仲介デバイス（MD）間で傍受されたトラフィックを暗号化することを強く推奨します。

次のように設定する必要があります。

- ルータの暗号化およびMDの暗号化クライアント、またはトラフィックを複合化するためMD に関連付けられたルータを設定します。
- 信頼できるホストへのアクセスを制限します。
- VPN クライアントを設定します。

ルータの暗号化の設定

最初に、認証、許可、およびアカウンティング（AAA）パラメータを設定します。次に、パラメータを設定する例を示します。

```
aaa authentication login userauthen local
username <username> password 0 <password>
```

次の例は、内部データベースを使用しています。ただし、認証を実行するように、外部認証サーバを指定できます。

AAA パラメータを設定した後、Internet Security Association and Key Management Protocol（ISAKMP）ポリシーとクリプト マップを設定します。次の例では、フェーズ 1（Internet Key Exchange（IKE））の暗号化プロトコルとして事前共有キー、Diffie-Hellman（DH）グループ 2 および AES 256 を使用します。クリプト マップはダイナミック マップと呼ばれ、VPN グループはLI グループと呼ばれます。アクセス リスト 108 によって、ルータに許可されるトラフィックが定義されます（この状況で ip プールは 10.1.1.254 を介した 10.1.1.1 です）。

```
crypto isakmp policy 1
encr aes 256
authentication pre-share
group 2
!
crypto isakmp client configuration group LI-group
key <password>
dns 10.10.10.10
wins 10.10.10.20
domain cisco.com
pool ippool
acl 108
!
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
```

```
!
crypto dynamic-map dynmap 10
set transform-set myset
!
!
crypto map clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list groupauthor
crypto map clientmap client configuration address respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
!
interface GigabitEthernet0/3
ip address <IP address of LI-enabled router> 255.255.255.0
crypto map clientmap
!
!
ip local pool ippool 10.1.1.1 10.1.1.254
!
!
access-list 108 permit ip  10.1.1.0 0.0.0.255 host 10.0.24.4 <IP address of LI-enabled
router>
```

信頼できるホストへのアクセス制限（暗号化あり）

次の例は、VPN クライアントの IP プール（10.1.1.0/24）のみを許可する ACL の作成方法と、SNMPv3 グループへのその ACL の割り当て方法を示しています。

```
access-list my-list permit ip 10.1.1.0 0.0.0.255
snmp-server group my-group v3 auth access my-list
```

VPN クライアントの設定

```
See the
 Installing the VPN Client
 document to download and configure the Cisco VPN Client for Solaris. See the
Cisco VPN Client installation instructions
 document to download and configure the Cisco VPN Client for other operating systems.
```

合法的傍受の設定方法

ルータで合法的傍受をプロビジョニングするための直接のユーザ コマンドはありませんが、LI MIB へのアクセスの有効化、SNMP 通知の設定、LI RADIUS セッション機能のイネーブル化など、いくつかの設定作業を実行する必要があります。ここでは、必要なタスクの実行方法について説明します。

合法的傍受 MIB の制限付き SNMP ビューの作成

ユーザを作成して、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

- 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 モードで実行する必要があります。
- デバイスで SNMPv3 が設定されている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa intercept**
4. **snmp-server view** *view-name MIB-name* **included**
5. **snmp-server view** *view-name MIB-name* **included**
6. **snmp-server view** *view-name MIB-name* **included**
7. **snmp-server group** *group-name* **v3 noauth read** *view-name* **write** *view-name*
8. **snmp-server user** *user-name group-name* **v3 auth md5** *auth-password*
9. **end**

手順の詳細

	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	**aaa intercept** 例： `Device(config)# aaa intercept`	デバイスで合法的傍受をイネーブルにします。 • このコマンドが削除されたときに許可のないユーザが傍受を停止できないように、このコマンドを高い管理セキュリティに関連付けます。 （注） **aaa intercept** コマンドは、IP セッションを使用した盗聴の設定に必要です。
ステップ 4	**snmp-server view** *view-name MIB-name* **included** 例： `Device(config)# snmp-server view exampleView 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。

	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 ciscoIpTapMIB included`	CISCO-IP-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 cisco802TapMIB included`	CISCO-802-TAP-MIB を SNMP ビューに追加します。
ステップ 7	**snmp-server group** *group-name* **v3 noauth read** *view-name* **write** *view-name* 例： `Device(config)# snmp-server group exampleGroup v3 noauth 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 8	**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 9	**end** 例： `Device(config)# end`	現在の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。

次の作業

これで、メディエーション デバイスは合法的傍受 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。ルータがメディエーション デバイスに SNMP 通知を送信するよう設定する方法については、「合法的傍受のための SNMP 通知のイネーブル化」を参照してください。

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ルータを設定するには、ここに示す手順を実行します。

始める前に

- 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 モードで実行する必要があります。
- ルータで SNMPv3 が設定されている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server host** *ip-address* **community-string udp-port** *port notification-type*
4. **snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart** *and* **snmp-server enable traps rf**
5. **end**

手順の詳細

	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 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** *and* **snmp-server enable traps rf**
	例：
	`Device(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart`
	`Device(config)# snmp-server enable traps rf`
		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ルータを設定します。
		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）、およびルータ再起動を示します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config)# end`	現在の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

ルータ上で SNMP 通知をディセーブルにするには、ここに示す手順を実行します。

（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。

手順の概要

1. **enable**
2. **configure terminal**
3. **no snmp-server enable traps**
4. **end**

手順の詳細

	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`	現在の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。

RADIUS セッション傍受のイネーブル化

メディエーションデバイスまたはタップをプロビジョニングするために使用可能なユーザCLIコマンドはありません。しかし、CISCO-TAP-MIB を通じて傍受をイネーブルにするには、account-session-id 値をメディエーションデバイスが使用できるようにシステムを設定する必要があります。ルータでRADIUSセッション傍受をイネーブルにするには、ここに示す手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa intercept**
4. **aaa authentication ppp default group radius**
5. **aaa accounting delay-start all**
6. **aaa accounting send stop-record authentication failure**
7. **aaa accounting network default start-stop group radius**
8. **radius-server attribute 44 include-in-access-req**
9. **radius-server host** *host-name*
10. **aaa server radius dynamic-author**
11. **client** *ip-address*
12. **domain** {**delimiter** *character*| **stripping [right-to-left]**}
13. **server-key** *word*
14. **port** *port-number*
15. **exit**
16. **end**

手順の詳細

	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	**aaa intercept** 例： `Device(config)# aaa intercept`	ルータで合法的傍受をイネーブルにします。 • このコマンドが削除されたときに許可のないユーザが傍受を停止できないように、このコマンドを高い管理セキュリティに関連付けます。

	コマンドまたはアクション	目的
ステップ 4	**aaa authentication ppp default group radius** 例： `Device(config)# aaa authentication ppp default group radius`	ポイントツーポイントプロトコル（PPP）を実行中のシリアル インターフェイス上で使用する認証方式を指定します。 （注） このコマンドが必要なのは、タップ情報が RADIUS サーバにしかないためです。ローカルに設定した情報で認証できますが、ローカルに設定した情報ではタップを指定できません。
ステップ 5	**aaa accounting delay-start all** 例： `Device(config)# aaa accounting delay-start all`	アカウンティング開始レコードの生成を、ユーザの IP アドレスが確立されるまで遅らせます。**all** キーワードを指定することにより、遅延がすべての VRF ユーザーおよび非 VRF ユーザーに適用されます。 （注） このコマンドは、メディエーション デバイスがターゲットに割り当てられた IP アドレスを参照できるようにするために必要です。
ステップ 6	**aaa accounting send stop-record authentication failure** 例： `Device(config)# aaa accounting send stop-record authentication failure`	（任意）ログイン時またはセッションのネゴシエーション中に認証に失敗したユーザに対するアカウンティング停止レコードを生成します。 （注） 合法的傍受の動作 1 でタップが開始されない場合、停止レコードの Acct-Termination-Cause（属性 49）に 15（サービス使用不能）が設定されます。
ステップ 7	**aaa accounting network default start-stop group radius** 例： `Device(config)# aaa accounting network default start-stop group radius`	（任意）すべてのネットワーク関連のサービス要求に対するアカウンティングをイネーブルにします。 （注） このコマンドは、タップが開始されなかった理由を特定するためだけに必要です。
ステップ 8	**radius-server attribute 44 include-in-access-req** 例： `Device(config)# radius-server attribute 44 include-in-access-req`	（任意）ユーザ認証前のアクセス要求パケット（事前認証の要求を含む）中で、RADIUS 属性 44（アカウンティング セッション ID）を送信します。 （注） このコマンドは、Access-Request パケットから属性 44 を取得するために入力します。そうしない場合、属性 44 の値を特定するには、アカウンティング パケットが受信されるのを待つ必要があります。

	コマンドまたはアクション	目的
ステップ 9	**radius-server host** *host-name* 例： `Device(config)# radius-server host host1`	（任意）RADIUS サーバ ホストを指定します。
ステップ 10	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	デバイスを認証、許可、アカウンティング（AAA）サーバとして設定して外部ポリシー サーバとの通信を容易にし、ダイナミック認可ローカル サーバ コンフィギュレーション モードを開始します。 （注） セッションの開始時に常にタップが開始される場合、このコマンドはオプションです。CoA-Requests を使用して既存のセッションでタップを開始および停止する場合は、このコマンドは必須です。
ステップ 11	**client** *ip-address* 例： `Device(config-locsvr-da-radius)# client 10.0.0.2`	（任意）デバイスが CoA-Request パケットを受け付ける RADIUS クライアントを指定します。

ステップ 12	**domain** {**delimiter** *character*| **stripping [right-to-left]**}
	例：
	`Device(config-locsvr-da-radius)# domain stripping right-to-left`
	例：
	`Device(config-locsvr-da-radius)# domain delimiter @`
		（任意）RADIUS アプリケーションについてユーザ名のドメイン オプションを設定します。
		• **delimiter** キーワードで、ドメインデリミタを指定します。次のいずれかのオプションを文字引数に指定できます：**@**、**/**、**$**、**%**、****、**#**または **-**
		• **stripping** キーワードは、着信のユーザー名と、**@** ドメインデリミタの左側にある名前を比較します。
		• The **right-to-left** キーワードは、右から左方向に見て最初のデリミタで文字列を終了します。

ステップ 13	**server-key** *word* 例： `Device(config-locsvr-da-radius)# server-key samplekey`	（任意）デバイスと RADIUS クライアントの間で共有する RADIUS キーを設定します。
ステップ 14	**port** *port-number* 例：	（任意）デバイスが CoA-Request パケットを受け付ける RADIUS クライアントを指定します。

	コマンドまたはアクション	目的
	`Device(config-locsvr-da-radius)# port 1600`	
ステップ 15	**exit** 例： `Device(config-locsvr-da-radius)# exit`	ダイナミック認可ローカル サーバー コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 16	**end** 例： `Device(config)# end`	現在の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。

回線 ID ベースのタッピングの設定

ルータのユーザ セッションのデータ パケットと RADIUS 認証のデータ パケットの回線 ID ベースのタッピングを設定するには、このセクションの手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **subscriber access pppoe unique-key circuit-id**
4. **end**
5. **show pppoe session all**
6. **show idmgr session key circuit-id** *circuit-id*

手順の詳細

	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	**subscriber access pppoe unique-key circuit-id** 例： `Device(config)#subscriber access pppoe unique-key circuit-id`	PPPoE のユーザ セッションの一意の回線 ID タグがルータでタップされるように指定します。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config)# end`	現在の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。
ステップ 5	**show pppoe session all** 例： `Device# show pppoe session all`	次の手順でユーザ セッションの検証に使用される、PPPoE セッションの回線 ID タグを表示します。

ステップ 6	**show idmgr session key circuit-id** *circuit-id*
	例：
	`Device# show idmgr session key circuit-id Ethernet4/0.100:PPPoE-Tag-1`
	例：
	例：
	`session-handle = AA000007`
	例：
	`aaa-unique-id = 0000000E`
	例：
	`circuit-id-tag = Ethernet4/0.100:PPPoE-Tag-1`
	例：
	`interface = nas-port:0.0.0.0:0/1/1/100`
	例：
	`authen-status = authen`
	例：
	`username = user1@cisco.com`
	例：
	`addr = 106.1.1.3`
	例：
	`session-guid = 650101020000000E`
	例：
		一意の回線 ID タグを指定して、ID Manager（IDMGR）データベースのユーザ セッション情報を確認します。

	コマンドまたはアクション	目的

	`The session hdl AA000007 in the record is valid`
	例：
	`The session hdl AA000007 in the record is valid`
	例：
	`No service record found`	

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、4 つの LI MIB（CISCO-TAP2-MIB、CISCO-IP-TAP-MIB、CISCO-802-TAP-MIB、CISCO-USER-CONNECTION-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。

```
aaa intercept
snmp-server view tapV ciscoTap2MIB included
snmp-server view tapV ciscoIpTapMIB included
snmp-server view tapV cisco802TapMIB included
snmp-server view tapV ciscoUserConnectionTapMIB included
snmp-server group tapGrp v3 noauth read tapV write tapV notify tapV
snmp-server user MDuser tapGrp v3 auth md5 MDpasswd
snmp-server engineID local 1234
```

例：RADIUS セッションの合法的傍受のイネーブル化

次に、イーサネットの PPP connection over Ethernet（PPPoE）リンクを使用したネットワーク アクセス サーバ（NAS）デバイスとして機能するルータ上で、RADIUS ベースの合法的傍受ソリューションを設定する例を示します。

```
aaa new-model
!
aaa intercept
!
aaa group server radius SG
server 10.0.56.17 auth-port 1645 acct-port 1646
!
aaa authentication login LOGIN group SG
aaa authentication ppp default group SG
aaa authorization network default group SG
aaa accounting send stop-record authentication failure
aaa accounting network default start-stop group SG
```

```
!
aaa server radius dynamic-author
client 10.0.56.17 server-key cisco
!
vpdn enable
!
bba-group pppoe PPPoE-TERMINATE
virtual-template 1
!
interface Loopback0
ip address 10.1.1.2 255.255.255.0
!
interface GigabitEthernet4/1/0
description To RADIUS server
ip address 10.0.56.20 255.255.255.0
duplex auto
!
interface GigabitEthernet4/1/2
description To network
ip address 10.1.1.1 255.255.255.0
duplex auto
!
interface GigabitEthernet5/0/0
description To subscriber
no ip address
!
interface GigabitEthernet5/0/0.10
encapsulation dot1q 10
protocol pppoe group PPPoE-TERMINATE
!
interface Virtual-Template1
ip unnumbered Loopback0
ppp authentication chap
!
radius-server attribute 44 include-in-access-req
radius-server attribute nas-port format d
radius-server host 10.0.56.17 auth-port 1645 acct-port 1646
radius-server key cisco
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
SNMP サポートの設定	*SNMP* サポートの設定
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
PacketCable™ コントロール ポイント検出インターフェイス仕様	『*PacketCable™ Control Point Discovery Interface Specification*』（PKT-SP-CPD-I02-061013）

MIB

MIB	MIB のリンク
• CISCO-TAP2-MIB • CISCO-IP-TAP-MIB • CISCO-802-TAP-MIB • CISCO-USER-CONNECTION-TAP-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC-2865	『*Remote Authentication Dial In User Service (RADIUS)*』
RFC-3576	*Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*
RFC-3924	『*Cisco Architecture for Lawful Intercept in IP Networks*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

合法的傍受に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1* : 合法的傍受に関する機能情報

機能名	リリース	機能情報
合法的傍受	Cisco IOS XE Release 2.4 Cisco IOS XE Release 3.15S	合法的傍受（LI）機能を利用すると、サービス プロバイダーは、エッジ ルータを通過する Voice-over-Internet（VoIP）トラフィックまたはデータ トラフィックを傍受できる機能を提供するという、司法当局による要求を満たすことができます。 Cisco IOS XE Release 2.4 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 Cisco IOS XE リリース 3.15S で、Cisco ASR 1000 シリーズアグリゲーション サービス ルータのトンネル インターフェイスに合法的傍受機能が導入されました。
VRF 対応の LI（合法的傍受）	Cisco IOS XE Release 2.4	VRF 対応 LI は、特定のバーチャル プライベート ネットワーク（VPN）での IPv4 データの LI 盗聴をプロビジョニングする機能です。 Cisco IOS XE Release 2.4 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。
RADIUS ベースの合法的傍受	Cisco IOS XE Release 2.4 Cisco IOS XE Release 3.5S	合法的傍受の実装は SNMP3 を使用してプロビジョニングされ、RADIUS セッションの傍受をサポートします。 Cisco IOS XE Release 2.4 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 Cisco IOS XE リリース 3.5 では、ハイ アベイラビリティのサポートが RADIUS ベースの合法的傍受用に追加されました。
合法的傍受の PPP セッションの回線 ID ベースのタッピング	Cisco IOS XE Release 2.5	Cisco IOS XE リリース 2.5 では、PPP セッションの回線 ID ベースのタッピングが導入されました。回線 ID ベースのタッピングは、ユーザ セッションがアクティブになった後、タップがプロビジョニングされる場合にのみ動作します。このインスタンスでは、ユーザセッションは回線 ID タグで一意に識別されることを前提としています。

機能名	リリース	機能情報
合法的傍受の回線 ID ベースのタッピング	Cisco IOS XE Release 2.6	Cisco IOS XE リリース 2.6 では、PPP セッションの回線 ID ベースのタッピングの事前プロビジョニングが導入されました。ユーザ セッションがアクティブになる前にタップがプロビジョニングされる場合、タップはユーザ セッションがアクティブになればいつでも有効になります。また、対応する RADIUS 認証とアカウンティング パケットもタップされます。このインスタンスでは、ユーザ セッションは回線 ID タグで一意に識別されることを前提としています。
非合法的傍受（Non-LI）のイメージ	Cisco IOS XE Release 3.10S	Cisco IOS XE リリース 3.10S では、この機能は Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 非合法的傍受のイメージは、Cisco IOS XE リリース 3.10S 以降で使用可能で、合法的傍受サブシステムは含まれません。

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。