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。